Cybersecurity Education in High School: Exploring Cyber Assets, Cyber Value at Risk, and Authentic Assessment

Prashant Vajpayee
Dept. of Information Science
University of North Texas
Denton, TX
prashantvajpayee@my.unt.edu

Gahangir Hossain
Dept. of Information Science
University of North Texas
Denton, TX
Gahanjir.Hossain@unt.edu

Abstract*—In the realm of cybersecurity, a knowledge chasm exists among high school students. High school students face a significant gap in cybersecurity knowledge, essential for safeguarding the digital environment. This educational deficit renders them vulnerable to cyber threats, compromising personal and school-wide digital security. The global shortage of cybersecurity professionals exacerbates the issue, threatening future defenses against cyberattacks. This paper introduces Cyber Value-at-Risk (CVaR), a concept adapted from finance, to evaluate the risk to digital assets. It outlines a model using basic math and probability to assess and mitigate risks to these cyber assets, which include data, vulnerability, and potential negative impacts like financial or reputational loss at the time of cyber incident. The approach equates cyber assets to financial terms—assets, liabilities, and capital—to demonstrate how additional countermeasures can reduce cyber asset value. The paper emphasizes the importance of consistent cybersecurity practices, akin to the effects of compound interest, and aims to demystify cybersecurity for students using financial literacy and mathematical concepts. The paper uses the proposed method to calculate cyber risks for the prominent cyber-attacks such as Phishing, DDoS, Data breach, Ransomware, and IoT Vulnerabilities in the context of school. It further explains the value of problem based learning and provides an authentic assessment framework to establish a practical learning of cybersecurity concepts for high school students. Finally, it advocates for the integration of security measures in internet use, covering authentication, authorization, encryption, firewall, secure connections, and systems' upgrade to reduce cyber risks. With the rise of online education, gaming, social media, and digitalization, cyber awareness is crucial for high school students. The criticality of internet security is making cyber knowledge an urgent educational priority. Due to growing demand of IoT and artificial intelligence (AI), the paper suggests future research about explaining cyber risks to high school students using machine learning, human behavior, and system anomalies.

Keywords*—Cybersecurity, Cyber Value at Risk (CVaR), Probability, Financial literacy, Cyber Threats, Authentic Assessment

I. Introduction

The Internet has a positive influence on society, however, it introduces online risks such as cyberbullying, financial fraud, identify theft, cyber threats, and hacking. The cyber risk is attributed to a general lack of awareness and protective measures among users. Research indicates that the overall level of cybersecurity awareness is still not adequate. It is very important to educate young children about these dangers and equipping them with the knowledge to navigate cyberspace safely [1].

The increasing susceptibility of schools to cyber-attacks have become more frequent and varied in recent years. Sensitive information such as students' grades, disciplinary records, personal contact details, and even parents' data is at risk of exposure due to these security breaches. The consequences of such attacks are significant, necessitating immediate action to enhance cybersecurity measures. Cyberattacks often occur through compromised storage devices or infected hardware, and can also result from intentional or unintentional actions by system operators that lead to the disclosure or alteration of confidential student information [2].

The primary objective of this paper is to underscore the necessity of teaching modern learners about online risks and to discuss innovative strategies of teaching cybersecurity using basic financial and mathematical concepts for better correlation and effective learning outcomes.

Cyberattacks in schools are growing. The following figure 1 shows prominent cyber-attacks, which teachers' face [3]. The teachers, students, parents should aware about these attacks.

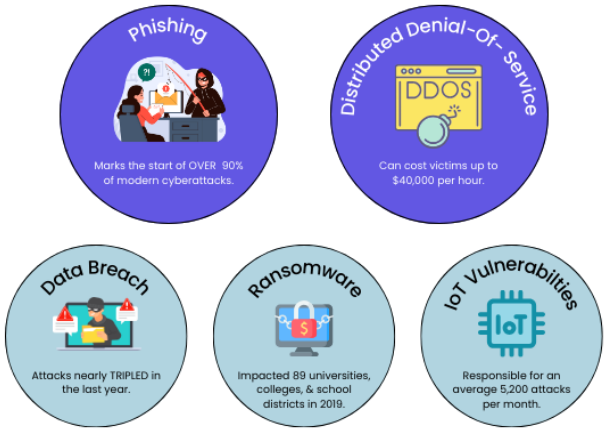

Fig. 1. Cybersecurity Threats Faced by Teachers

Human actions are the significant part of cyber issues and risk. The cyber-attacks and losses represented in the above figure clearly points out the need of proper cyber awareness among students to avoid cyber incidents. For the ease of learning the mathematical and financial terms have been used.

The gap has been examined between the demand for cybersecurity professionals and the current educational offerings. It finds that while there is a significant need for

skilled cybersecurity workers, higher education programs are too theoretical and lack practical as well as experiential learning opportunities like simulations and internships. The study suggests that the curriculum needs to incorporate more applied learning and technical writing, as well as improve cyber risk evaluation skills to better prepare students for the future workforce. Dawson (2020) proposes the development of a framework akin to the NICE Cybersecurity Workforce Framework, but tailored for an offensive security workforce. This would facilitate the cultivation of offensive security skills from as early as high school through to university education [4].

The study will discuss about the K-12 mathematical curriculum and associated financial component of that to propose an innovative approach of cyber learning in school environment to generate effective cyber awareness among students. The cyber asset, asset value, cyber value at risk (CVaR) concepts have been utilized to explain cyber risks associated with students actions. The paper suggests that early education on cybersecurity is essential to prepare children for the challenges of the digital world and meet the future demand of cybersecurity skill gap nationwide. It aims to investigate the critical need for awareness and to identify effective methods of learning as well as assessment using basic mathematics and financial concepts. It is important for students to develop a capability of computing risk for their cyber and internet activities. Analyzing the cyber risk based on the activity, applying mitigating steps, and restricting to repeat the same activity in future can be identified as practical learning for students, which will not only make school system secure but also develop efficient digital citizens to meet the future demand of skilled cybersecurity professionals.

II. Literature Review

A. Mathematical and Finance Knowledge in Schools

In a study it has been identified that a deeper understanding of AI algorithms requires math knowledge typically taught in high school. The curriculum adheres to the Common Core State Standards for Mathematics and includes subjects like pre-calculus, calculus, algebra, and geometry. The basic statistics and probability are taught throughout K-12 itself [5]. In another survey based study it has been identified that 46 states have established their own personal finance standards or have incorporated personal finance principles within the curriculum of various subjects in K-12 [6]. Another study explores the financial attitudes and behaviors of high school seniors, revealing their optimism about achieving or exceeding their parents' standard of living. The survey, conducted across seven high schools, assessed students' views on spending and education. Key findings show that students rely on independent thinking for money management, with part-time jobs as their main income source. Overall, the students displayed a confident outlook on their financial futures [7]. The contextual and hands on learning has become more significant. A study shows pivotal shift in computer science education (CSE) for K-12 schools over recent years. The study analyzed 47 peer-reviewed articles to understand trends, benefits, and challenges in the field. It focused on programming tools, educational contexts, and instructional methods. Findings indicate that CSE research is moving in a positive direction, with the potential to make learning enjoyable and effective. The study advocates for hands-on learning, where students engage in creating projects and problem-solving, to deepen understanding and navigate the nuances of both formal and informal educational settings [8]. The National Financial Institute (NFI) conducted a nationwide research on financial literacy of K-12. The findings were as follows [9].

- High school instruction in financial literacy becomes more specialized and advanced.
- Teachers from Business education and consumer sciences typically lead the way in teaching higher-level financial concepts. These include comprehensive money management strategies, the responsible use of credit, the intricacies of lending, understanding taxes, and the fundamentals of investing.
- Math teachers in high schools focuses to educate business and consumer sciences. The goal at this level is to equip students with a deeper understanding of financial literacy that they can carry into their adult lives.

The mathematical and financial curriculum of K-12 is significant to cover computational aspects of cyber security in terms of quantifying cyber risk when appropriate security measures are not followed by high school students. It will be easier to simulate cyber asset, cyber asset values, and explain cyber value at risk due to mathematical and financial background.

B. Gaps in Cybersecurity Practial Education in Schools

Based on literature review following gaps have been observed as part of K-12 cybersecurity.

- A key issue is the lack of uniform assessment methods to measure student progress in cybersecurity learning. Current evaluation techniques vary widely, including self-assessment, examination of student work, direct observation, and quizzes. This diversity makes it challenging to establish evidence-based best practices or to effectively assess and compare different cybersecurity teaching methods in K–12 educational settings [10].
- It's essential to emphasize hands-on experience and practical application in learning. In the field of cybersecurity, where practical skills are as important as theoretical knowledge, students often only learn the theory without having the opportunity to apply it. To truly master cybersecurity, students need ample opportunities to practice and implement their knowledge in real-life situations [11]. Moreover, research in this area should include a diverse range of perspectives to enrich understanding and approaches.
- Cybersecurity instruction needs to integrate more experiential learning activities. Engaging methods like gaming, simulated environments, and other interactive educational techniques can provide learners with authentic experiences in a controlled environment. These approaches are effective in equipping students with the necessary skills for real-world cybersecurity challenges [12].

Another study was conducted to do an extensive review with 24 academic article and 19 additional resources from 2013 to 2023 for K-12 cybersecurity education globally. The research underscores the need for a broad set of cybersecurity skills and competencies for K-12 students. The review points out the lack of clarity in terminology across interdisciplinary studies, a challenge exacerbated by cybersecurity's widespread relevance [13]. A notable gap in K-12 education is the focus on teaching students how to utilize different technologies without equally educating them about the potential risks associated with their use [14]. An innovative

way is required to explain cyber risks associated with regular academic activities associated with the students.

C. Need of Cybersecurity Education in High School

The escalation in internet usage underscores the urgent need for cybersecurity education, as evidenced by a study showing 93.8% of New Zealand's youths use internet, increasing their susceptibility to cyber-attacks. Survey results reveal a concerning deficit in cybersecurity awareness among students aged 8 to 21emphasizing the necessity of equipping them with knowledge and tools to defend against digital threats. [15].

The integration of technology in U.S. education necessitates early cybersecurity education for K-12 students to mitigate online risks such as cyberbullying and identity theft. This research underscores the pivotal role of educational institutions in imparting cyber literacy and revealing a gap in educators' preparedness to teach cybersecurity. It advocates for the inclusion of cyber ethics and safety in the K-12 curriculum to make this advance for addressing existing educational constraints and protecting students from cyber risks and threats [16, 17].

Kreider and Almalag (2019) introduced a comprehensive model to scrutinize the proficiency shortfall among cybersecurity experts, focusing on three key aspects: student pipelines development channels, educational content, and institutional capabilities [18]. The Global Information Security Workforce Study highlighted a critical shortage of qualified cybersecurity personnel within firms to effectively counter cyber offenses [19].

Global scholars and experts are dedicated to enhancing cybersecurity education, aiming to inspire high school students to explore cybersecurity careers, refine educational programs, and develop engaging cybersecurity learning experiences [20]. It will help to resolve global shortfall of cybersecurity talent. Integration with learning and educational motivation theories specifically cognitivism and social cognitive theory can generate positive impact in cybersecurity education [21, 22].

III. Methodology

It is very important for the students to understand finance and cybersecurity domain analogy for different terms to correlate the context for better understanding of use case and compute the cyber risk to analyze the overall impact. The following terms have been consolidated to understand the overall methodology.

A. Confedentialitiy, Integrity, and Availability (CIA)

Confidentiality is about restricting information as well as data and enabling access to only those who have proper authorization. Access levels are tailored based on the individual's necessity for the information. **Integrity** refers to the protection and security of data, ensuring that only legitimate users can alter encrypted data throughout its processing, transmission, and storage. **Availability** refers to the significance of systems and associated data availability. While securing and authenticating information is crucial, having availability of the data when needed, especially during urgent or critical situations, is essential for operations [23].

B. Cyber Asset, Asset Value, and Matrix

- **Cyber assets' classification:** Cyber assets are different from financial assets. Financial assets can be any financial product such as Home loan, shares, bonds, mutual funds, and CDs which has a monetary value associated. However, cyber assets can be categorized as tangible, intangible, and digital assets. In the contemporary digital era, digital assets have become an integral part of our daily existence, deeply ingrained within our digital culture. These assets encompass all forms of digital information, whether stored on computers, smartphones, various digital platforms, or cloud services. Historically, the term 'assets' was reserved for physical, tangible items like money, equipment, real estate, and livestock, as well as non-physical, intangible assets such as intellectual property, copy right, trademarks, trade secrets [24].
- **Asset Value:** Typically, the value of the cyber asset depends on the data associated with the asset. If the data is unstructured or unclassified, it is difficult to determine the value. However, if the data is classified as business critical, internal, and public, the value of cyber asset can be high, medium, and low respectively. Apart from classified data, the degree of effective enablement of CIA triad for a cyber asset is also a significant contributing factor to determine value of cyber asset.
- **Total Asset Value Metric:** The total asset value can be calculated based on product of data classification (DC), confidentiality (C), integrity (I), and availability (A) score. The following equation 1 displays the total asset value (TAV) formula for a cyber asset.

$$TAV_1 = C_1 * I_1 * A_1 * DC_1 \quad (1)$$

- Based on the above formula the following metric in Table I can be derived for a possible values of cyber assets considering various combinations of CIA scores and data classifications. In the below metric the high, medium, and low values have been indicated by numbers 1, 2, and 3 respectively [25]. Data classification reflects the type of data assets contains. Similarly CIA triad score provides information about the significance of confidentiality, integrity, and availability aspects of the asset.

TABLE I. ASST VALUE METRIC

Data Classification	**CIA Triad Score**			**Total Asset Value**
	Confidentiality	***Integrity***	***Availability***	
1	1	1	1	1
1	1	1	2	2
1	1	1	3	3
1	1	2	1	2
1	1	3	1	3
1	2	1	1	2
1	3	1	1	3
3	**3**	**3**	**3**	**27**

C. Cyber Value at Risk (CVaR)

Value at Risk (VaR) is a financial terms, which quantifies potential portfolio financial losses into a single numeric value, estimating the loss likely to be surpassed with a given probability over a set time. For instance the 95% VaR is $90K for one month indicates a 95% chances that portfolio losses will not exceed $90K

for next one month. VaR consolidates diverse risks for high-level decision-making and regulatory reporting [26]. Cyber Value at Risk (CVaR) has been originated from VaR which can provide information about cyber losses depending on the risk score of an asset. As VaR reflects losses in a given time, the CVaR anticipates cyber losses at the instant based on risk and asset value. For the ease of understanding, we can explain CVaR for single incident. The following equation 2 can be used for CVaR calculation.

$$R_1\,(Risk) = L_1(Liklihood) * IM_1(CIA\ Impact) \quad (2)$$

$$CVaR_1 = R_1 * TAV_1 \quad (3)$$

For calculation purpose we select a random row from Table II with the combination of Data Classification, Confidentiality score, Integrity score, and Availability score and Total asset value as 1, 3,1,1,3 respectively. The following steps will be used for CVaR calculation.

- The average CIA impact score can be (3+1+1)/3 = 5/3
- The probability of random coin flip for head or tail outcomes remain 1/2 i.e. P (H) = P (T) = 1/2. In the similar way, we can assume a cyber incident may occur or may not occur. Therefore for conceptual evaluation the probability or likelihood of a cyber incident remains 1/2.
- Total Risk $R_1 = \frac{5}{3} * \frac{1}{2} = \frac{5}{6}$
- $CVaR_1 = R_1 * TAV_1 = \frac{5}{6} * 3 = 2.5$ < Asset Value

TABLE II. CVAR EVALUATION

CVaR for DC =1	CIA Triad Score			Total Asset Value
	Confidentiality	*Integrity*	*Availability*	
8	2	2	2	8
40.5	3	3	3	27
0.5	1	1	1	1

The Table II explains the total CVaR value changes at 50% risk probability based on average CIA impact score. The scenarios in which CVaR is equal to TAV or greater than TAV are critical and require immediate attention. However, for scenarios CVaR less than TAV, the necessary control can be applied to minimize CIA impact and in turn reduce CVaR. The variation of the variables for a given cyber incident will help students to understand the associated risk and provide an opportunity to them to think for implementation of necessary controls along with Do's/Don'ts to avoid a cyber incident. On a different perspective following financial equations can also be used for analogy.

$$\text{Assets} = Libalities + Equity \quad (4)$$

$$\text{Cyber Asset Value} = Ctrl\ Cost + Business\ Value \quad (5)$$

The financial assets, liabilities, and equity has been considered with Cyber assets, control cost, and business value respectively in equations (3) and (4). For the ease of understanding CVaR can be explained using profit loss to high school students. For a given probability CVaR > TAV, CVaR = TAV, and CVaR < TAV reflects loss, break even, and profit respectively. To increase profit and reduce losses, CVaR needs to be reduced.

IV. CYBER THREAT SIMULATION AND CVAR ANALYSIS

We will discuss five prominent scenarios, which has been mentioned earlier (Phishing, DDoS, Ransomware, Data Breach, and IoT vulnerabilities) to utilize CVaR and financial as well as mathematical computation analogy.

A. *Phishing*

Phishing attacks are fraudulent schemes where cybercriminals craft misleading emails and create fake websites with the intent to deceive individuals for surrendering their personal information or login details. Phishing can have many forms. The Table III explains the various phishing attacks for the school ecosystem [27].

TABLE III. PHISHING ATTACKS IN THE CONTEXT OF SCHOOL

Phishing Type	***Details***
Spear Phishing	Personalized Spam like email attack, which targets to individuals
Clone Phishing	Email attack by replicating an authentic email
Whaling	Variant of spear phising to target school district executives
Vishing	Voice phising, which used autnentic school number to trap parents, students, or school staff's members.
BEC (Business Email Compromise)	Business email compromise to impersonate school distict authorities for misleading school staff, vendors such as school pay, and third parties who conduct after school programs
Snowshoeing	Attackers can find a work around to break traditional filters by pushing messages via diffeternt school domains and IP addresses

There is a risk related to confidentiality if an individual becomes a victim of phishing attack. We can explain with the following analogy.

- The person has taken personal loan of $10K with variable APR interest of 5%, which can introduce penalties if person is unable to pay loan installment timely. The total loan payment amount will increase due to penalties.
- A student is reviewing junk, spam, and promotional emails on his device (asset value is 9) 3 times a day (morning, afternoon, and evening), which contains student's personal information. The probability of phishing occurrence remains 3/24 (i.e.1/8, considering 24 hours day), however, it can change if number of reviews get increased per day (i.e. for 4 time's review the probability of attack will increase to 4/24 or 1/6). Due to increase in probability the CVaR can increase from 1.875 (5/3 * 1/8*9) to 2.5 (5/3 * 1/6 *9). The increased CVaR is similar to penalty of delayed loan payment.

B. *Ransomware*

Ransomware is a type of malicious software that encrypts a user's data or system, denying access until a ransom is paid to the cyber attacker who deployed the malware. This is major issue related to "Non Availability" of cyber assets (Figure 2).

Fig. 2. Ransomeware Symbolic Representation

The following analogy can be used to explain the scenario.

- Suppose a person loses all his wealth by making bad financial decisions and he files a bankruptcy. The financial institutions will start liquidizing all his financial assets such as home, land, and foreign reserves etc. to recoup the losses.
- The ransomware phenomenon can be explained in the similar lines. If a hacker successfully inserts a malware to your asset or device, the hacker can have a complete access to your device along with the confidential information such as passwords, SSN, bank accounts etc. This situation will have a cascaded risk such SSN can be used for identity theft and bank account as well as passwords can introduce unwanted access to financial assets. In this case the losses can have a compounded impact, which can be explained negative compound interest formula.

$$P_{Loss} = P_{Orig}\,(1-r)^n$$

Where r = 5/3 * 1/10 = 5/30 = 1/6 (assuming likelihood 10% and initial CIA impact is 5/3)

For P_{Orig}(cyber asset value) = 9 and n = 100, which indicates that losses have been extended to 100 different non-cyber assets such as finance, real estate, insurance, and other affiliated items indirectly. After putting the values the equation will be as follows.

$$P_{Loss} = P_{Orig}\,(1-1/6)^{100} = \sim -0.2 * P_{Orig}$$

-0.2 P_{Orig} indicates CVaR 120% losses of the original asset value, which demands additional cost out of the total asset value to pay the losses. This simulation will help students to understand real impact of enabling cyber unsafe environment. If students in school don't follow the proper cyber hygiene, a bad actor can control students' device and access to various school resources, which could cause unprecedented losses.

C. Data Breaches

A data breach, or data leakage, refers to the unauthorized release of private information. The motivation towards this could be related to financial rewards, political benefits, or conduction espionage etc. It can occur horizontally in various industries. The following Table IV reflects private data information of different entities [28]

TABLE IV. PII DATA ATTRIBUTES

Entity	***PII Data***
Person Identity	Name, Address, Phone. SSN, License
Personal Finance	Finance Account, Credit Card, Tax Information
Personal Authentication	Biometric Data
Personal Characteristics	Finger Printing, Handwriting
Personal Digital Asset	Internet Protocol, Media Access Control (MAC)

Educational institutions face security incidents when unauthorized parties, either from within or outside, infiltrate their databases and extract private details. This often leads to the theft of critical personal information of both students and school staff, such as identification numbers, academic history, medical data, and behavioral records. Data leaks are like secret passages that bad guys use to get into your private information. Attackers look for things like your name, birthday, and even your passwords. They can sell this info in hidden places on the internet or use it to get into your other accounts. It's not just about taking money from your bank; they can use small bits of info to cause big problems. The scariest part is when they get enough details to pretend to be you. This can cause a lot of trouble, like having to deal with the law and diminishing your reputation [29]. According to GAO report on data security, it has been reflected that intentional and accidental data breaches are originated from students and staff respectively (Figure 3) [30].

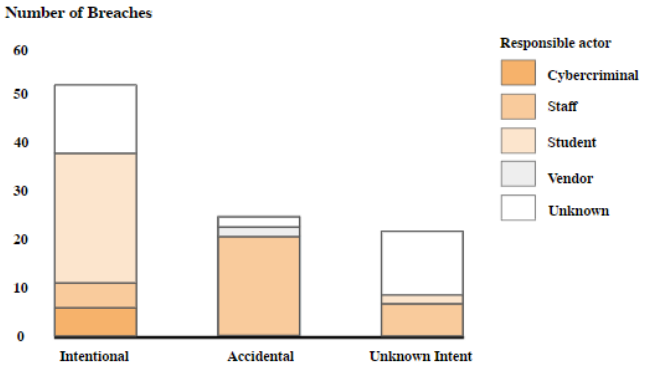

Fig. 3. Source: GAO Analysis of K-12 Cybersecurity Resource Center Data

The following example can be used to explain the of privacy breach scenario to students in the realm of cyber risks.

- Based on the Forbs research the number of average high school student in US are 850 [31]. Suppose the 20% students are doing intense use of internet and mobile during school hours.
- The 20% students (170 students) will have more possibility of data breaches. If 170 are the favorable instances for data breach due to high usage of internet. The probability $P_1 = \frac{170}{850} = 0.2$ shows probability of 1 data breach.
- Furthermore, the probability of at least one data breach could be evaluated as $P_{atleast\_1\_data\_breach} = 1 - P_{no\_data\_breach}$
- Now since we know the probability or risk of data breach. The CVaR can be calculated using CIA average impact and total asset value.
- If the data classification of the asset is increased (such as sensitive to mission critical), the overall business value gets incremented, which in turn increase the cyber-asset value based on equation (1). However, to avoid data breach on any cyber asset, we need to make sure proper controls such as data authentication, authorization, encryption, firewall, secure connections, and systems' upgrade have been applied to safeguard cyber assets. However, if the business value of the asset is not increasing, introducing additional controls can reduce cyber asset value due to increment in the unwanted control cost.

D. Distributed Denial of Service (DDoS)

A DDoS attack is a malicious attempt to disrupt normal traffic to a web service by overwhelming it with a flood of internet traffic. This deluge of requests overloads the system, depleting its resources so it can't carry out its usual activities. As a result, legitimate users are unable to access the service because it's been forced to shut down due to the excessive demand (Figure 4).

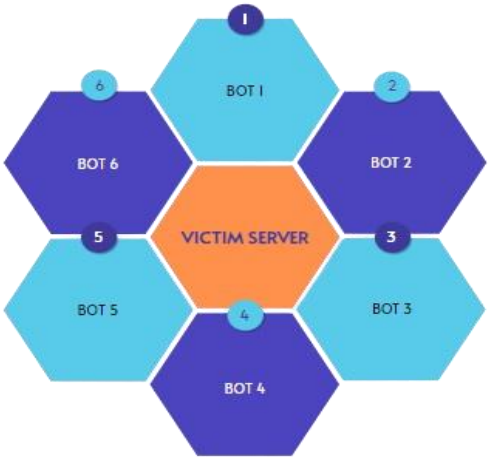

Fig. 4. VICTIM SERVER: DDoS Attack via Multiple Bots

Imagine if attackers want to make a website non-functional, they send out a bad virus through emails or get a control of multiple computers in a given network which work as bots. The group of 'bots' work together like a team, which is called a 'botnet'. The attacker sends commands to these bots to visit a website at the same time, which is too much for the website to handle, therefore it stops working. This is an example of DDoS attack. It outlines the importance of individual devices used by students and staff. A vulnerable device can be utilized by the attackers by exploiting the vulnerabilities in the device. This scenario can be easily explained to students using following example [32].

- Suppose P_B and P_M are the probability of bandwidth and memory exhaustion of the server.
- If P_B and P_M are not exhausted, the server will allow and process authorized traffic.
- The following equation can define the probability of DDoS attack if both bandwidth and memory of the server gets exhausted via multiple incoming requests from bots, which is beyond threshold of the server. The good server turns to victim server.
- $P_{DDoS} = 1 - (1 - P_B)(1 - P_M)$
- With the help of P_{DDoS}, which reflects likelihood, the CVaR can be calculated using CIA average impact and total asset value.

E. IoT Vulnerabilities

Cyberattacks are big problems, just like huge storms that cost a lot of money. They can hurt businesses, hospitals, schools, and governments, costing billions every year. Cyber threats have become more common in due to IoT, introduction Mobile learning devices (MLD), and wearable technologies in the context of schools and educations institutions. People who work in educational institute needs to look out for new dangers in this evolving space and share what they find in terms of systems vulnerabilities. Many schools still use old computer systems, which can be risky. Old network configurations and systems that aren't updated let hackers break in easily. It is critical that people who make decisions, teachers, and students know about these risks. It's especially important for smart devices and online learning tools. The objective is to make everyone more aware about the dangers and how to stay safe. With this approach, schools can protect themselves and their students from cyberattacks [33].

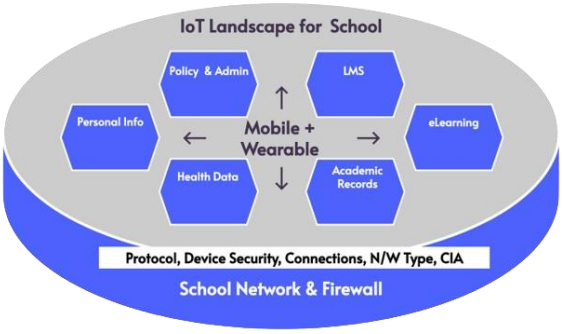

Fig. 5. IoT Landscape of School

The Figure 5 displays an example about how the IoT devices such as smart phone and wearables generate a cyber risk for school system. In the world of internet intra connected school systems are accessible to smart devices through internet. The smart devices such as smart phone not only access the school systems but also access to other smart 3rd party devices such as smart security camera, smart thermostat, smart light, and smart clock. Therefore apart from known CIA impact as well as measures, it is viable to consider other CIA impacts due to network type, protocol type, and device security in the realm of IoT security risk [34]. Our earlier risk equation can be modified as follows.

$$R_1\,(Risk) = L_1(Liklihood) * IM_{1\_IoT}(IoT\ Impact)$$

Where $IoT\ Impact = \frac{1}{5}(CIA_{nwt} + CIA_{prt} + CIA_{het} + CIA_{des} + CIA_{known})$

The explanation of the terms are as follows.

- NWT (Network): The IoT systems connected to insecure networks can be easily hacked, leading to loss or theft of data, or even unauthorized control.
- PRT (Protocol): IoT devices uses protocols, which can be targeted by attackers. Each protocol has different purposes such as MQTT, TCP, and UDP used for communication, and Wifi, Bluetooth, and RFID used for connectivity.
- HRT (Heterogeneous Systems): The different types of systems are inter connected in an IoT setup, which could cause higher the cyber risk.
- DES (Device Security): Devices without proper security are highly susceptible to cyber-attacks. The impact varies with the type of device; for instance, certain IoT attacks have targeted specific devices like IP cameras and routers.
- Known-CIA: Attacks that compromise confidentiality, integrity, and availability (CIA) issues pose a high risk.

The above explanation provides a meaningful approach to high school students for thinking about IoT and associated cyber risks. For a given likelihood and average impact score corresponding to various attributes (nwt, prt, het, des, cia) the risk can be calculated. Further with the help of risk and total asset value, CVaR can be evaluated.

V. Cyber Knowledge Evaluation for High School

During extensive research we have observed that problem based learning (PBL) is the need to hour to learn cybersecurity concepts effectively and this type of learning will help to enable authentic assessment framework. This section will

explain effective learning and assessment process in the context of cyber security.

A. Problem Based Learning of Cybersecurity

The modern concept of Problem-Based Learning (PBL) originated from a shift in health sciences education in North America that began more than three decades ago. The traditional approach to medical training, which was heavily lecture-based and followed by demanding clinical sessions, was no longer suitable. This was due to the overwhelming increase in medical knowledge, the advent of new technologies, and the evolving needs of medical practice. PBL was developed as a response to these challenges, offering a more effective and humane way to educate future medical professionals. Due to dynamic change in the cybersecurity ecosystem, PBL method holds good for learning cybersecurity concepts effectively. The following points explain the PBL for cybersecurity [35].

- **Active Involvement:** In cybersecurity, students learn best by doing. For example, instead of just reading about network security, they might participate in a simulated cyber-attack to understand how to defend against real threats and quantify the risk.
- **Learning to Learn:** The field of cybersecurity is always expanding. PBL teaches them how to quickly find and understand new information when they need it. For instance, they might learn how to stay updated on the latest security protocols or hacking techniques.
- **Real-World Relevance:** PBL aligns with what cybersecurity professionals actually do. Instead of just theoretical knowledge, students might work on real-world projects like securing a small business's network as part of summer programs, which gives them practical experiences.
- **Adaptability to Change:** Cybersecurity is a field that changes rapidly. PBL allows educational programs to adapt to these changes by updating the problems and scenarios students work on, ensuring students learn the latest information and techniques.
- **Flexible Structure & Integration:** Even though PBL is different from traditional teaching methods, it can be integrated into existing educational structures. For example, a cybersecurity program might replace some lectures with workshops where students work together to solve security challenges. Math and finance courses can be extended with mandatory supplements of cybersecurity problems to utilize financial and mathematical concepts in cybersecurity. The integration of mathematics and financial literacy will help to evaluate the risks originated from cyber-attacks to make informed decision in students' daily digital activities.

In summary, PBL in cybersecurity education means students are actively engaged in solving real and current problems, learning how to learn, and gaining practical experience that will be directly applicable in their future career. The cyberspace is continuous evolving with the introduction of new vulnerabilities as well as attack mechanisms. The problem simulation for all attacks are required significant efforts. It will required to modify the course content to sync with the latest trend and innovations in the cybersecurity landscape.

B. Authentic Assessment Framework

Authentic assessment redefines classroom dynamics by making daily activities more engaging and reshaping the roles of students and teachers. It turns assessment into a continuous, integrated part of learning, rather than a separate, intimidating event. This approach helps identify students' strengths and potential, making assessment a constructive part of the educational journey. The study explains various attributes of authentic assessment (Figure 6) in the realm of cybersecurity and provide example assessment questions to establish that framework for high school students [36].

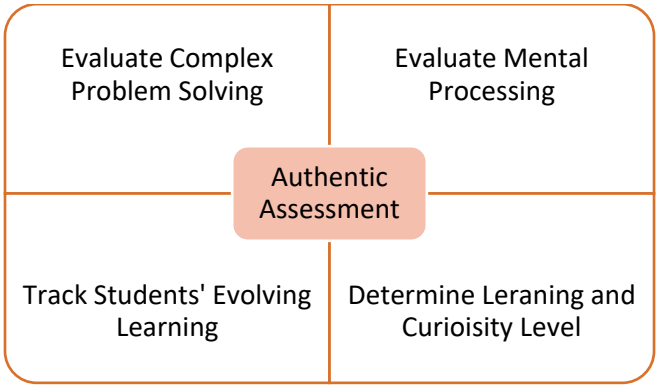

Fig. 6. Authentic Assessment Framework

- **Enable and Evaluate Complex Problem Solving:** Traditional assessments often focus on memorizing facts rather than understanding concepts and applying them. They test for specific, yet limited knowledge that doesn't translate well to real-life situations. In contrast, real-world tasks require collaboration, project management, and the ability to apply knowledge creatively. Effective assessment should be part of the learning process, helping students develop deeper understandings and practical skills. This approach to assessment encourages ongoing learning and the practical application of knowledge in the context of cybersecurity risk analysis. The sample assessment questions will be as follows, which can enable critical thinking, effective design skills, and implementation of theoretical concepts for practical use cases.
    - What are the different parameter needs to be considered for evaluating effective physical security risk of the school?
    - What are the risk associated when a visitor violates authentication and authorization process during school visit?
    - What are the possible cyber risks using public or private network instead of school network in school premise?
- **Evaluate Mental Processing:** Education aims not just to create specialists but to nurture students as active and reflective learners. Standardized tests, with their focus on numerical scores, fail to capture

the complex learning processes and disengage students from self-assessment. Authentic assessment should reveal the student's understanding and the intellectual journey, not just the final product. The process of creating and developing work is as valuable as the finished work itself. Reflective learning, through self-evaluation and introspection, helps students recognize their strengths and improve their work, embodying the true purpose of education. The following questions will enhance students' creativity and ability to develop cyber risk models using interdisciplinary knowledge of other domains such as finance and mathematics.

- How can we define a process to handle cyber incident in school during holidays to manage anticipated risks?
- What are necessary component to design a risk model for the confidentiality issues in the context of school activities?
- What are the different attributes to simulate cyber risk using financial and mathematical variables? Further, Design the cyber risk quantification model using financial and mathematical concepts.

- **Track Students' Evolving Learning:** Effective assessments should do more than gauge what students grasp; they should also track the transformation of their understanding. Such assessments act as a testament to the students' developing abilities and their journey towards tackling complex issues, making nuanced decisions, and executing intricate tasks. However, the prevalence of standardized tests has left schools unprepared to document and appreciate the gradual evolution of students' learning. Traditional tests, with their normative scores, fail to detail how students' progress from their past selves. An example of meaningful assessment is the use of "process-folios" in art education, which, unlike traditional portfolios, showcase a diverse array of student work that reflects the depth and expansion of their cognitive growth over time. The hypothetical scenario based questions will provide an opportunity to students to apply cognitive skills and learned concepts for creating or developing responses, which should be reviewed to understand evolution of their learning in the context of given subject area.
  - If CIA triad is violated, what are the list of risks associated? What are the possible resolutions?
  - If cyber risk is evaluated, what is the possibility of residual risk and associated list of cyber harms on various cyber assets?
  - If the smart device belong to a student gets compromised, what are the anticipated list of cyber-attacks?
- **Determine Learning and Curiosity Level:** Assessment is meant to be a driving force for ongoing learning and teaching improvement, going beyond the limits of traditional testing practices. Unfortunately, assessments are frequently treated as separate from the actual learning process, serving merely to signal its start or to summarize its conclusion. Instead, they should be integrated throughout the educational experience to truly support and reflect the learning journey. It is very significant for teachers to understand the learning level and curiosity level of students. Providing due diligence on students' learning and curiosity level the assessment can be refined to better engage students for the positive learning outcomes. In this context, the students feedback can be collected along with a metric can be consolidated for the teachers' review for the assessment refinement. The questions should be as follows.
  - Are you able to apply learned cybersecurity concepts while taking the assessment (students' engagement and curiosity)?
  - Were you curious to review the hint given in the question? Was the hint useful in answering the questions ((students' engagement and curiosity)?
  - Were you able to correlate the finance and math concepts to solve the cyber-risk related questions (students' engagement and curiosity)?
  - How many students received the above average learning score and vice versa (Learning outcome and course refinement)?
  - What percentage of students utilized hint to solve questions (Learning outcome and course refinement)?
  - What percentage of students provided most accurate answers (Learning outcome and course refinement)?
  - How many students utilized completely new or innovative design (Learning outcome and course refinement)?

Authentic assessment, however, offers comprehensive and evolving insights into student comprehension by weaving together evaluation, learning, and teaching. If relegated to mere semester bookends, even authentic assessments lose their effectiveness. In a genuine assessment-focused setting, the emphasis is on intricate thought processes and deep understanding, as seen in classrooms where students actively apply their learning to create design, develop models, or execute self-assessment for efficient learning experiences.

VI. CONCLUSION

High school students are currently facing a substantial gap in cybersecurity knowledge, which is crucial for protecting themselves and their digital environments. This lack of cyber awareness leaves them susceptible to cyber threats, endangering both individual and institutional digital security. The deficit of cybersecurity professionals globally further intensifies this vulnerability, posing a risk to future cyber defenses. The paper explains the concept of Cyber Value-at-Risk (CVaR) to quantify the risk associated with digital assets, employing basic mathematics, finance, and probability to evaluate and lessen these risks by enabling practical learning among high school students. The proposed method equates cyber assets with financial terms to illustrate how strategic

countermeasures can diminish the risk to these assets. Consistent cybersecurity best practices are highlighted as essential, comparable to the accumulative negative effect of compound interest. The suggested method utilizes the calculation of risk originated through common cyber-attacks within an educational context. The concept of problem-based learning, learning as well as motivational theories, and a genuine assessment framework will help to facilitate practical cybersecurity education for high school students. It will help to create effective digital citizens and resolve future workforce skill gap in the realm of cybersecurity. The risk quantification of cyber assets is an evolving concept. Irrespective of risk evaluation of cyber assets, the importance of incorporating security practices in daily internet usage, which includes using strong authentication methods, encryption, anti-virus software, secure connections, and regular upgrade of systems, should not be ignored. This is increasingly vital for high school students to understand the concept of layered defense for achieving cyber excellence. Due to frequent and extended use of online platforms and internet, students are the prime targets for cyber-attacks. As technology advances, particularly with the Internet of Things (IoT) and Artificial Intelligence (AI), the future research is required to find better ways for educating students by continuous refinement of curriculum about cyber risks through the perspectives of machine learning, human behavior analysis, and investigation of system anomalies to bolster cybersecurity. The goal is to prepare students to navigate and protect themselves in a digital world that is becoming more interconnected and intelligent. By understanding these risks and the measures to counter them, students can contribute to a safer digital environment. The urgency of this matter stems from the potential consequences of cyber threats, which can range from personal data breaches to large-scale disruptions.

REFERENCES

[1] Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378-382.

[2] Goran, I. (2017). Cyber security risks in public high schools.

[3] Cybersecurity in Education: What Teachers, Parents and Students Should Know, Available at- https://bootcamp.berkeley.edu/blog/cybersecurity-in-education-what-teachers-parents-and-students-should-know/

[4] Liu, F., & Tu, M. (2020). An Analysis Framework of Portable and Measurable Higher Education for Future Cybersecurity Workforce Development. *Journal of Education and Learning (EduLearn)*, *14*(3), 322-330.

[5] Wang, N., & Johnson, M. (2019, January). AI education for K-12: Connecting AI concepts to high school math curriculum. In *Workshop on Education in Artificial Intelligence K-12, 28th International Joint Conference on Artificial Intelligence*.

[6] Hill, A. T., & Meszaros, B. T. (2011). Status of K-12 personal financial education in the United States. *Journal of Consumer Education*, *28*, 1-15.

[7] Miller, D., Hite, N. G., Slocombe, T., & Railsback, B. (2010). STUDENT PERSPECTIVES TOWARD KEY PERSONAL FINANCE VARIABLES. *Delta Pi Epsilon Journal*, *52*(3).

[8] Garneli, V., Giannakos, M. N., & Chorianopoulos, K. (2015, March). Computing education in K-12 schools: A review of the literature. In *2015 IEEE Global Engineering Education Conference (EDUCON)* (pp. 543-551). IEEE.

[9] Godsted, D., & McCormick, M. H. (2007). National K-12 financial literacy research overview. *Networks Financial Institute Report*.

[10] Ayeyemi, M. (2023). A Systematic Review of Cybersecurity Education in K-12 Context.

[11] Torres, M., Mullins, A., & Thompson, N. (2022). Education Cybersecurity Assessment Tool: A cybersecurity self-assessment tool for the Australian K-12 sector.

[12] Chen, W., He, Y., Tian, X., & He, W. (2021). Exploring Cybersecurity Education at the K-12 Level. In SITE Interactive Conference (pp. 108-114). Association for the Advancement of Computing in Education (AACE).

[13] Ibrahim, A., McKee, M., Sikos, L. F., & Johnson, N. F. (2024). A Systematic Review of K-12 Cybersecurity Education Around the World. *IEEE Access*.

[14] Javidi, G., & Sheybani, E. (2018, October). K-12 cybersecurity education, research, and outreach. In 2018 IEEE Frontiers in Education Conference (FIE) (pp. 1-5). IEEE.

[15] Tirumala, S. S., Sarrafzadeh, A., & Pang, P. (2016, December). A survey on internet usage and cybersecurity awareness in students. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)* (pp. 223-228). IEEE.

[16] Ross, T. (2020). *Technology in the K-12 education system* (Doctoral dissertation, Utica College).

[17] Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *NIST special publication*, *800*(2017), 181.

[18] Kreider, C., & Almalag, M. (2019). A framework for cybersecurity gap analysis in higher education.

[19] 2017 Global Information Security Workforce Study, Available at- https://informationsecurity.report/Resources/Whitepapers/e3da7993-49a9-4b7c-ac32-a08da483a02e_2017GlobalInformationSecurity_wp.pdf

[20] AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, *119*, 102754.

[21] Urhahne, D., & Wijnia, L. (2023). Theories of motivation in education: An integrative framework. Educational Psychology Review, 35(2), 45.

[22] Learning Theories: Five Theories of Learning in Education, Available at- https://www.nu.edu/blog/theories-of-learning/

[23] Reshan, A., & Saleh, M. (2021). IoT-based Application of Information Security Triad. *International Journal of Interactive Mobile Technologies*, *15*(24).

[24] Toygar, A., Rohm Jr, C. E., & Zhu, J. (2013). A new asset type: digital assets. *Journal of International Technology and Information Management*, *22*(4), 7.

[25] IT Asset Valuation, Risk Assessment and Control Implementation Model, Available at- https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/it-asset-valuation-risk-assessment-and-control-implementation-model

[26] Linsmeier, T. J., & Pearson, N. D. (2000). Value at risk. *Financial analysts journal*, *56*(2), 47-67.

[27] What Is Phishing? Available at- https://www.fortinet.com/resources/cyberglossary/phishing

[28] Guide to Identifying Personally Identifiable Information (PII), Available at- https://www.technology.pitt.edu/help-desk/how-to-documents/guide-identifying-personally-identifiable-information-pii

[29] Strategies to prevent school data breaches effectively, Availale at- https://preyproject.com/blog/data-breaches-in-schools-what-measures-you-should-take#

[30] Data Security, Available at- https://www.gao.gov/products/gao-20-644

[31] What's The Right High School Size And Structure? Available at- https://www.forbes.com/sites/tomvanderark/2021/06/04/whats-the-right-high-school-size-and-structure/?sh=3238d73daa18

[32] Johnson Singh, K., & De, T. (2017). Mathematical modelling of DDoS attack and detection using correlation. Journal of Cyber Security Technology, 1(3–4), 175–186. https://doi.org/10.1080/23742917.2017.1384213

[33] Fernández-Caramés, T. M., & Fraga-Lamas, P. (2020). Teaching and learning iot cybersecurity and vulnerability assessment with shodan through practical use cases. Sensors, 20(11), 3048.

[34] Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. EURASIP Journal on Information Security, 2020, 1-18.

[35] Boud, D., & Feletti, G. (2013). The challenge of problem-based learning. Routledge.

[36] Perrone, V. (1991). Expanding Student Assessment. Association for Supervision and Curriculum Development, 1250 N. Pitt Street, Alexandria, VA 22314.