Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 5 Issue 2 (2025)

Strategic BDSLCCI Framework for Strengthening Cybersecurity in Educational Institutions and Universities

Shekhar PAWAR
Doctor of Business Administrator (DBA), Swiss School of Business and Management Geneva, Geneva Business Center, Avenue des Morgines 12, Genève, 1213, Switzerland. https://orcid.org/0000-0001-7091-4113.
Atul TRIPATHI
Visiting Faculty, Swiss School of Business and Management Geneva (Switzerland), Liverpool John Moores University (England, United Kingdom), and Edgewood College (Madison, Wisconsin, United States) https://orcid.org/0009-0003-9968-3197.

Abstract
Cyberattacks on educational institutions present significant challenges, jeopardizing the confidentiality of student and staff records, financial stability, operational continuity, and trust in academic systems. Various global data protection laws aim to safeguard sensitive information, yet educational institutions - particularly small and medium-sized establishments - often struggle to implement comprehensive cybersecurity measures. These organizations house vast amounts of personally identifiable information (PII), research data, and financial records, making them prime targets for cyber threats ranging from ransomware attacks to phishing campaigns. To mitigate these risks, the Business Domain Specific Least Cybersecurity Controls Implementation (BDSLCCI) framework offers a structured approach that incorporates Defense in Depth (DiD) and the Confidentiality, Integrity, and Availability (CIA Triad) model. This framework can help institutions align their cybersecurity strategies with evolving regulatory and compliance requirements while enhancing resilience against cyber threats. The author will outline how BDSLCCI can be effectively mapped to the cybersecurity challenges faced by educational institutions, ensuring a safer digital environment for academia.

Keywords: Education Institute; SME; Cybersecurity; BDSLCCI; University; Cyber Threats

1. INTRODUCTION

An educational institution is an establishment committed to delivering structured learning and academic instruction to students of different age groups. It encompasses schools, colleges, universities, technical academies, and training centers, all designed to provide organized programs, certifications, and degrees. These institutions serve as fundamental pillars in nurturing intellectual growth, enhancing knowledge, and

developing essential skills while maintaining adherence to established educational policies and regulatory standards to uphold quality and credibility [1, 2, 3].

Educational institutions play a pivotal role in shaping the global economy and influencing various sectors through workforce development, technological advancements, and social progress. By equipping individuals with essential skills and knowledge, these institutions enhance human capital, leading to increased productivity and innovation. Universities and research centers contribute significantly to scientific breakthroughs, fostering entrepreneurship and job creation. Additionally, education promotes social mobility, reducing inequality and enabling inclusive economic participation. The environmental impact of education is also profound, as institutions drive awareness of sustainability practices and support research on renewable energy and conservation. Furthermore, higher education institutions collaborate with industries to develop cutting-edge technologies, ensuring economic competitiveness and resilience. By integrating education with policy-making, these institutions help shape regulations that address global challenges, including climate change and cybersecurity. The collective contributions of educational institutions underscore their indispensable role in fostering economic growth, social stability, and technological progress on a global scale [4, 5].

In June 2020, the University of California, San Francisco (UCSF) paid a $1.14 million ransom after a ransomware attack encrypted data on its School of Medicine servers. The attack was linked to the Netwalker ransomware gang, which had previously targeted other universities. While UCSF stated that patient care and COVID-19 research were not impacted, the compromised data was critical to its academic work. The incident underscored the rising threat of ransomware attacks on educational institutions, especially those engaged in medical and scientific research [34]. In July 2020, the University of Utah paid $457,059 after a ransomware attack compromised servers in its College of Social and Behavioral Science. The attackers encrypted data and threatened to leak sensitive information. To mitigate risks, the university consulted law enforcement and cybersecurity experts before making the payment, which was partially covered by cyber insurance. Following the attack, students and staff were required to change their passwords, highlighting the growing cybersecurity threats faced by higher education institutions [35]. In October 2021, Ottawa's French-language public school board (CEPEO) suffered a ransomware attack, leading to the theft of 75 gigabytes of sensitive data, including personal and financial information of students, employees, and families. To prevent further exposure, CEPEO paid a ransom to the attackers, though it remains uncertain whether the stolen data was actually deleted [36]. The Union Community School District in Iowa was targeted by the DoppelPaymer ransomware group, which stole and leaked nearly 2GB of sensitive data on the dark web. In this case, The Union Community School District did not pay the ransom. Instead, they restored their systems using secure backups and engaged third-party forensic experts to investigate the breach. However, since the district

refused to pay, the DoppelPaymer ransomware group leaked nearly 2GB of stolen data on the dark web. The exposed files contain personal and personnel information of students and employees, including addresses, phone numbers, Social Security numbers, disciplinary records, and transcripts [37].

A student in Miami-Dade County, Florida was arrested for allegedly hacking into their school's system to change grades. Authorities discovered the unauthorized access and took legal action against the individual. The incident highlights cybersecurity vulnerabilities in educational institutions and the risks associated with unauthorized data manipulation [8]. In another news, Coaches from Braden River High School in Bradenton, Florida, were caught using a college Hudl account to gain unauthorized access to opponents' game and practice videos. The investigation, initiated by Hudl and the Sarasota County School District, revealed that Braden River misused a recruiting login to spy on teams, including Venice High School, which later won the state 7A title. The incident raised concerns about fair play and ethical conduct in high school sports, prompting disciplinary actions and security reviews within the affected institutions [9]. As per one of the news, a 19-year-old man from Richmond, Texas was charged with making a bomb threat during a University of Houston Zoom lecture. The suspect allegedly interrupted the session, made threatening statements, and referenced ISIS. Federal authorities arrested him, and he faces up to 10 years in prison for making threats involving explosives, plus an additional five years for interstate threats [12]. In one more news, a phishing scam at East Tennessee State University (ETSU) led to a data breach, exposing the personal information of approximately 7,700 individuals. The incident occurred when two ETSU employees unknowingly clicked on fraudulent emails, granting unauthorized access to their accounts. The university's IT team discovered the breach and immediately took action by disabling the compromised accounts, resetting credentials, and launching an investigation. ETSU has since notified affected individuals and is implementing additional security measures to prevent future attacks [10]. A malware attack disabled about 50 computers at SUNY Erie Community College in New York, knocking the college's website offline. The incident, discovered early in the morning, affected Windows-based staff computers across all three campus locations [11].

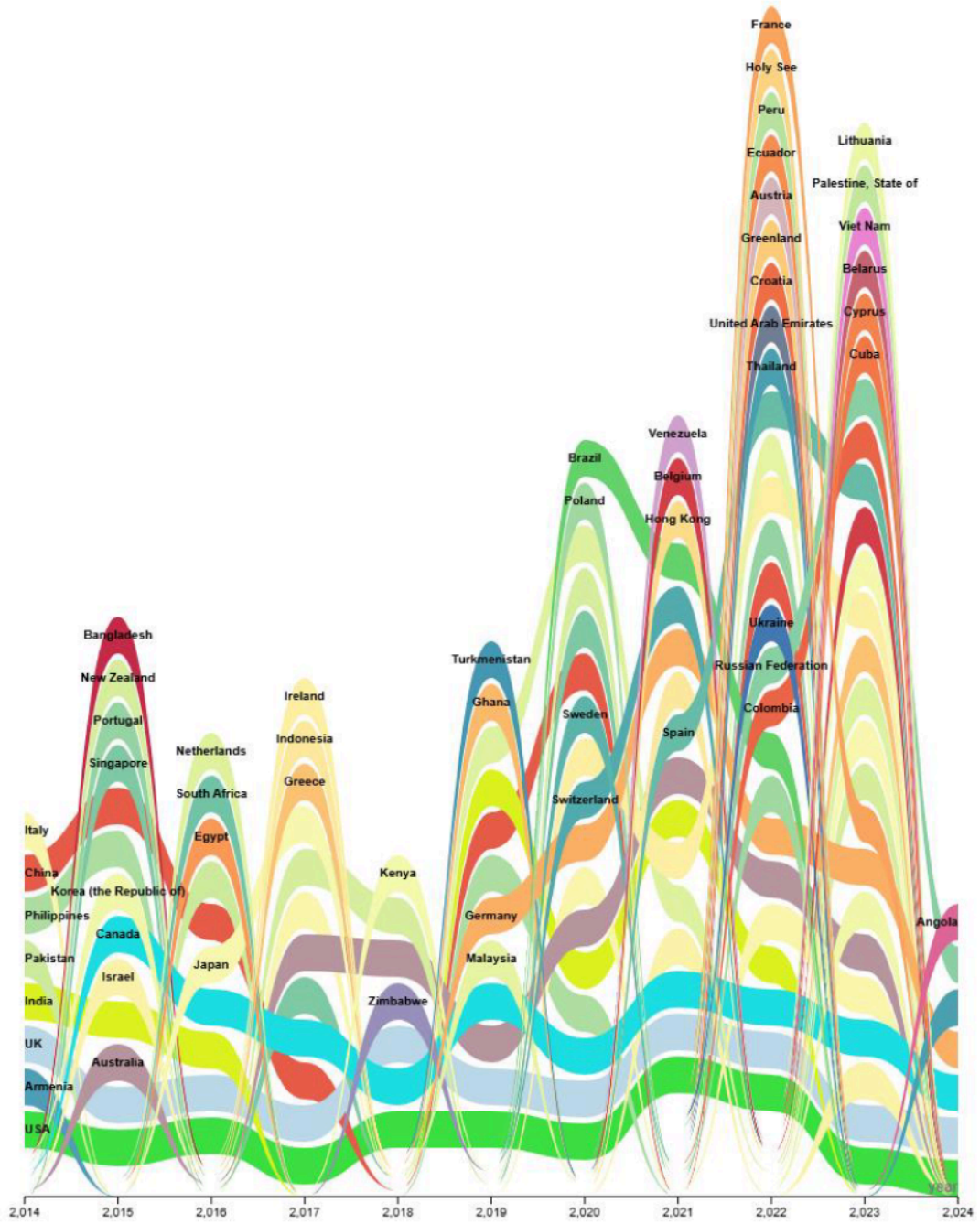

Figure 1: Number of Cyber Attacks on Education Institutes

In 2024, a ransomware attack disrupted operations at New Mexico Highlands University (NMHU) and East Central University (ECU) in Oklahoma. NMHU was forced to cancel classes and experienced outages in internet, VPN connectivity, and

payroll systems, affecting students and staff. The university confirmed the attack on April 5, with law enforcement agencies, including the FBI, assisting in the investigation. Meanwhile, ECU was targeted by the BlackSuit ransomware gang, which compromised student data, including names and Social Security numbers [13]. A cybersecurity incident disrupted IT services at Kansas State University, affecting VPN access, email communications, and online learning platforms. University officials confirmed the breach and took immediate action to investigate and isolate affected systems. As a precaution, impacted services were taken offline while forensic experts assess the situation [14].

According to news, the official website of Sambalpur University in Odisha, India, was hacked by Pakistani agents in a cyberattack. The attackers defaced the university's grievance portal, leaving a message that read "Hacked by Devil Killer." The breach was discovered when students attempted to access the site for postgraduate admissions. The incident raised concerns about cybersecurity vulnerabilities in educational institutions, prompting investigations into the attack [15]. A ransomware attack targeted IIT Madras, disrupting several systems, including its internal email service. The malware primarily affected Windows-based computers, rendering them unusable and leading to data loss. The institute urged faculty and students to back up critical data while investigating the breach. Although student email services were restored, faculty email systems remained affected. The incident highlights cybersecurity vulnerabilities in educational institutions [16]. Several top UK universities, including the University of Cambridge and University of Manchester, were impacted by a DDoS attack claimed by the Anonymous Sudan hacktivist group. The attack targeted the Janet Network, a high-speed data-sharing network used by researchers, disrupting student IT services such as CamSIS and Moodle. While network connectivity has largely stabilized, some systems remain affected. The universities are working with Jisc, a UK-based IT service provider, to resolve outstanding issues. The attack was reportedly motivated by political reasons, citing the UK government's stance on international conflicts [17]. The hacktivist group Anonymous claimed responsibility for cyberattacks against Belarusian government websites, citing the country's involvement in Russia's invasion of Ukraine. The attacks targeted multiple government portals, including the Ministry of Communications, Ministry of Justice, and Ministry of Economy, rendering them temporarily inaccessible. Anonymous stated that the operation was part of its broader campaign against entities supporting Russia [18].

A data breach at the University of Sydney exposed personal information of a small number of international applicants, due to a third-party service provider. The university confirmed that no domestic students, staff, alumni, or donors were affected. Authorities, including the New South Wales (NSW) Privacy Commissioner, have been notified, and impacted individuals are being contacted [19]. A cyberattack at Mount Lilydale Mercy College, a Catholic high school near Melbourne, Australia,

exposed the credit card details of around 400 parents. The breach, discovered by the Australian Federal Police (AFP), did not include CVV (Card Verification Value) numbers but still posed financial risks [20]. A ransomware attack disrupted operations at Kaiserslautern University of Applied Sciences (HS Kaiserslautern) in Germany, forcing the university to take its entire IT infrastructure offline. The attack affected email accounts, telephone systems, computer pools, and library services, impacting over 6,200 students. University officials warned staff and students not to turn on work computers, as the encryption attack may have compromised additional systems [21]. According to news of year 2023, Israeli cybersecurity experts have discovered BiBi, a new wiper malware targeting Linux and Windows systems. The BiBi wiper malware has been identified as part of a broader cyber offensive targeting Israeli organizations, including those in the education and technology sectors. Research by Palo Alto Networks' Unit 42 attributes these attacks to a threat actor closely linked to an Iranian-backed APT group known as Agonizing Serpens (also referred to as Agrius, BlackShadow, Pink Sandstorm, and DEV-0022). Believed to be deployed by pro-Hamas hackers, BiBi is designed solely to destroy data, rather than demand ransom. It achieves this by overwriting files, deleting shadow copies, and disabling recovery features, making data restoration virtually impossible. An Advanced Persistent Threat (APT) is typically a state-sponsored or highly organized group that gains unauthorized access to computer networks and remains undetected for extended periods. However, in recent times, the term has also been used to describe non-state actors conducting large-scale, targeted cyber intrusions for specific objectives [31]. Pakistani hacker groups have been actively targeting Indian organizations, particularly in government, defense, and critical infrastructure sectors. These cyberattacks involve phishing campaigns, malware deployment, and espionage operations aimed at stealing sensitive data and disrupting services. Security experts have linked these activities to APT36 (Transparent Tribe), a known Pakistan-based cyber espionage group [32]. A Chinese-language threat group, known as Xiaoqiying (Genesis Day, Teng Snake), has targeted South Korean research and academic institutions in a series of data exfiltration attacks. The group, which is ideologically driven and pro-China, has also signaled plans to expand its cyberattacks to Japan and Taiwan. While it does not appear to have direct ties to the Chinese government, its activities align with patriotic hacktivism. Researchers warn that the group may continue targeting North Atlantic Treaty Organization (NATO) countries and regions deemed hostile to China [33].

Similar to these few news reports, between 2014 and 2024, cyber news coverage from 56 countries documented approximately 1,335 cyberattacks on educational institutions, underscoring their vulnerability to cyber threats. These cyberattacks targeting educational institutions were widely reported across multiple countries, with the United States accounting for the highest percentage at 68.54%, followed by the United Kingdom at 11.09%. Canada recorded 3.67% of incidents, while Australia and

India contributed 2.17% and 1.72%, respectively. Other notable affected regions include Israel (1.50%), Germany (0.90%), Italy (0.90%), and China (0.82%). Several other countries, such as Ireland (0.60%), the Philippines (0.60%), Netherlands (0.52%), and Singapore (0.45%), also experienced cyber threats. Meanwhile, incidents in New Zealand, South Korea, Japan, Poland, Russia, Spain, Switzerland, and Brazil ranged from 0.37% to 0.30%. A smaller fraction of cyberattacks - below 0.22% - was reported in Malaysia, Colombia, France, Pakistan, Ukraine, Indonesia, Portugal, Zimbabwe, Thailand, Greece, Belgium, Kenya, Sweden, Armenia, and numerous other nations. The widespread distribution of these cyber threats highlights the increasing vulnerability of educational institutions globally.

Figure 1 shows the distribution of cyberattacks targeting educational institutions over the years highlights notable trends in threat activity. The year 2020 witnessed the highest number of reported incidents, accounting for 19.63%, followed closely by 2023 with 19.10%. Cyberattacks saw a steady rise in recent years, with 2022 (12.81%) and 2021 (12.36%) experiencing significant breaches. The trend extends back to 2019, which recorded 9.89% of incidents, emphasizing the growing threat landscape for academia. Earlier years, such as 2015 (6.14%), 2017 (5.99%), and 2018 (5.17%), indicate a gradual escalation of attacks, while 2016 (3.97%) and 2014 (3.07%) witnessed relatively fewer incidents. Notably, 2024, despite being the most recent year in the dataset, accounts for only 1.87%, possibly reflecting evolving cybersecurity defenses or incomplete data reporting. This distribution underscores the persistent and evolving nature of cyber threats against educational institutions, reinforcing the necessity for continuous security enhancements and proactive defense strategies.

The dataset explained here, compiled from various news articles and reports, provides insights into cyberattacks on educational institutions and universities. However, since many of these institutions may not publicly disclose their cybersecurity incidents, the data has certain limitations. Despite this, the analysis remains valuable in understanding the typical cyberattack landscape affecting these educational organizations and highlighting the need for enhanced security measures.

The increasing cyber threats targeting educational institutions demand immediate attention. Currently, there is no standardized cybersecurity framework specifically designed for universities and other educational establishments, leaving them vulnerable to attacks. Additionally, many of these institutions can be classified as small and medium-sized enterprises (SMEs) within the education sector, depending on their size, revenue, and operational structure. In many countries, SMEs are defined based on annual turnover, workforce size, and sector-specific criteria [22, 23, 24, 25]. This further underscore the urgent need for robust security measures and well-defined guidelines to safeguard their digital infrastructure.

2. Cyber Threats On Worldwide Education Institutes

As shown in Figure 2, among the study of the total reported cyberattack incidents targeting educational institutions, the United States accounted for the highest number, with 915 documented cases. If we consider the next seven countries affected by cyber-attacks on these organizations, the United Kingdom ranks second, with 148 incidents, while Canada recorded 49 attacks. Australia reported 29 incidents, India had 23, and Israel documented 20. Meanwhile, both Germany and Italy recorded 12 cases each.

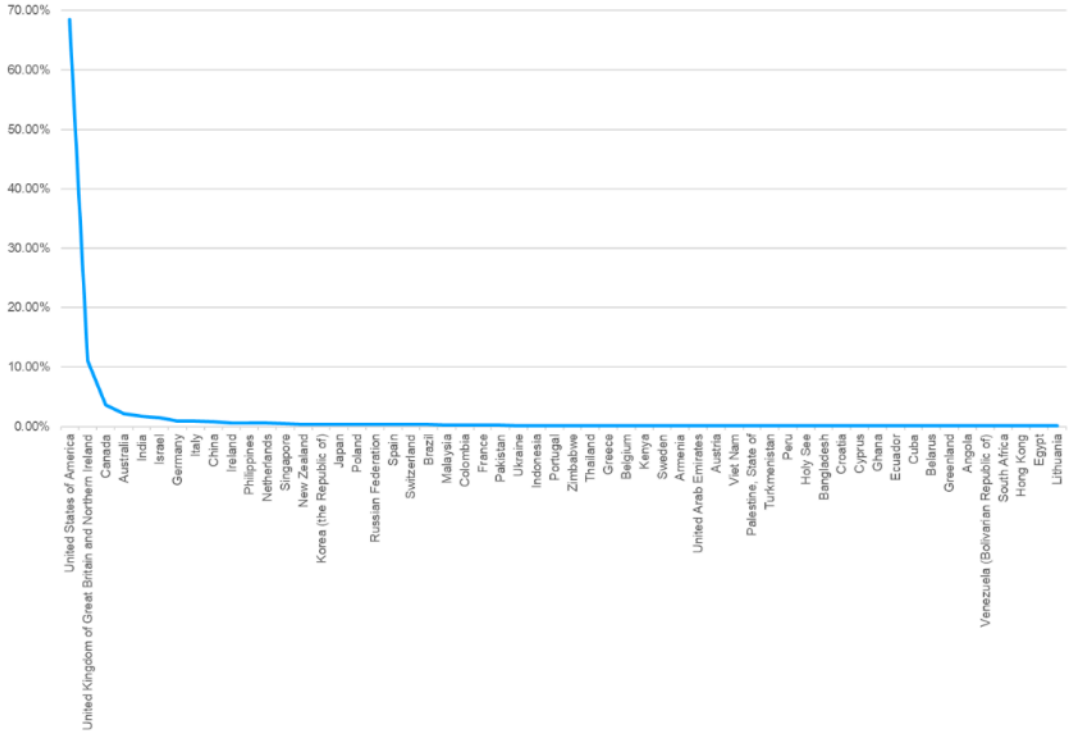

Figure 2: Countrywise Number of Cyber Attacks on Education Institutes

Refer to "Section 7 – List of Abbreviations Used in Images and Graphs" for the abbreviations applied in the diagrams and graphs within this section.

As explained in Figure 3, cyberattacks on educational institutions have become increasingly sophisticated, targeting schools, universities, and research centers worldwide. These attacks are carried out by various threat actors, including ransomware groups, hacktivists, state-sponsored cyber units, and individual cybercriminals.

Below is a detailed breakdown of the threats affecting educational institutions:

Ransomware Attacks:

Ransomware groups such as LockBit, REvil, Hive, Akira, ALPHVM, AvosLocker, Babuk, BlackByte, BlackSuit, Cuba, DoppelPaymer, Egregor, Grief, Medusa, Maze, Quantum, Royal, Snatch, SunCrypt, and Vice Society have launched large-scale

attacks on educational institutions. These groups encrypt institutional data and demand ransom payments, often leading to operational disruptions and financial losses.

Hacktivist and Cyber Espionage Groups:

Hacktivist collectives like Anonymous, Anonymous Sudan, Anonymous Cuba, AnonGhost, Cyber Partisans, Cyber-71, DragonForce, Fallaga Team, Middle East Cyber Army, Moroccan Islamic Union-Mail, New World Hackers (NWH), NoName057(16), People's CyberArmy, Pinoy Anonymouz, Team Mysterious Bangladesh, Team Pak Cyber Lions, and Team System DZ have targeted educational institutions for political or ideological reasons. Some of these groups leak sensitive data or disrupt online services to make a statement.

State-sponsored cyber units such as GRU 85th Main Special Service Center (FancyBear), Islamic Revolutionary Guard Corps (APT 35 Charming Kitten), Ministry of State Security's (MSS) Hainan State Security Department (APT40), People's Liberation Army Strategic Support Force (PLA Unit 61398), and National Security Agency have engaged in cyber espionage, targeting universities for intellectual property theft and intelligence gathering.

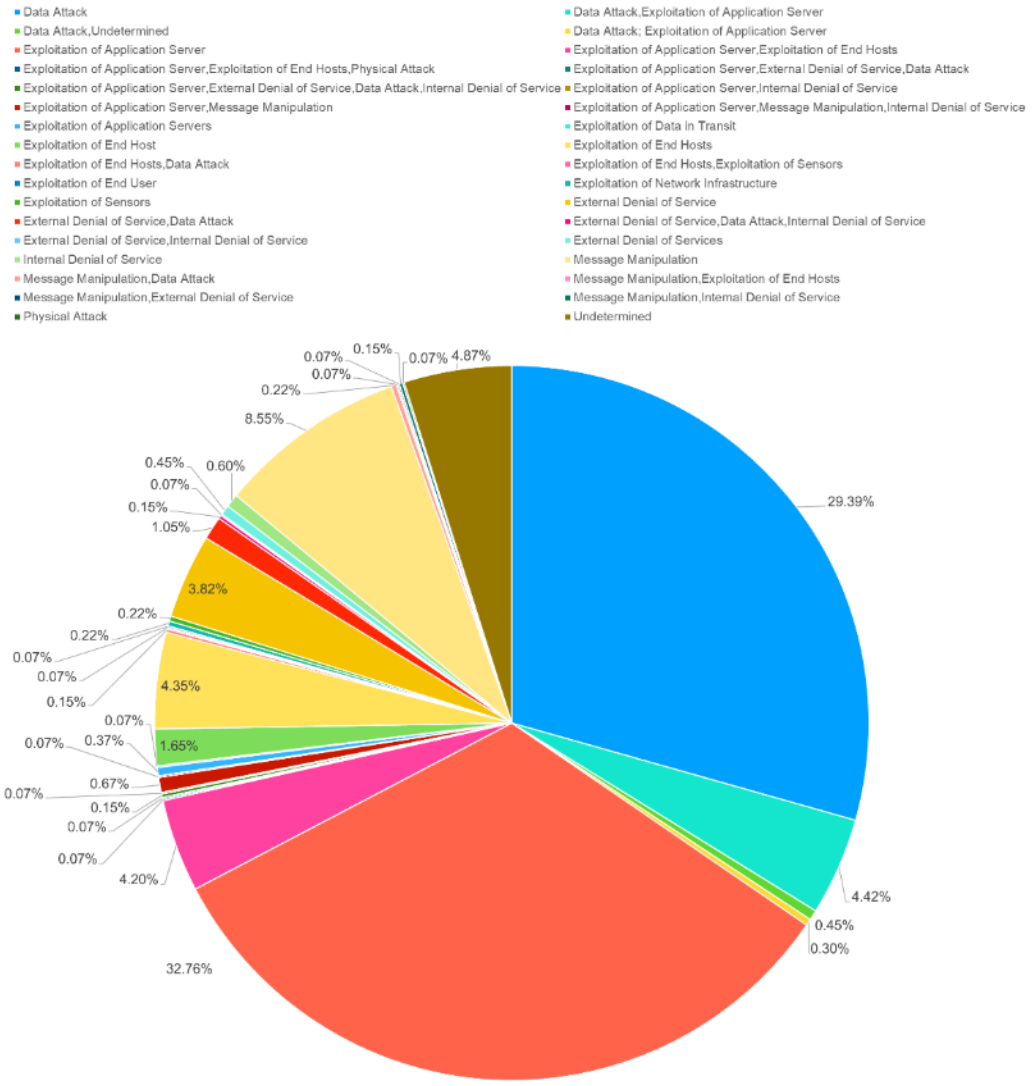

Figure 3: Wordwide Cyber Attack Detail on Education Institutes

Phishing and Social Engineering Attacks:

Threat actors like Bl00dy, Clop, DeleteSec, INC, ITA, Kami Haxor, Karakurt, LulzSecITA, Meow, Mespinoza, RGB, RansomHouse, SCUWatch, ShinyHunters, Silent Librarian, Spid3r, Stormous, Sudoh4k3rs, TA505, Th3 Ap3x, ThreatSec, Transparent Tribe, Trigona, Ulzr1z, VandaTheGod, and Zyklon have been involved in phishing campaigns, tricking students and faculty into revealing login credentials or financial information.

Distributed Denial of Service (DDoS) Attacks:
Groups such as NetPirates AKA @TheNetShip, NetWalker, and Exfocus have launched DDoS attacks against educational institutions, overwhelming their servers and disrupting online learning platforms.

Insider Threats and Individual Cybercriminals:
Some cyberattacks originate from insiders or individual hackers. Notable cases include Andrew "Weev" Auernheimer, Christopher Taylor, Daniel Soares, Alex Mosquera, Erick Vaysman, Eugene Belford, Fredrick Lapointe, Rath Pak, Jimmy Saintelien, Ibraheem Ahmed Al Bayati, Jonathan Powell, Jose Bautista, Kelvin Onaghinor, Laura Rose Carroll, Renauld Clayton, Rhysida, Shandra Gilles, and ViktorLustig. Additionally, students have been implicated in cyberattacks, such as a 13-year-old Benjamin Franklin Middle School student, two Sherman High School students, and an unnamed Fort Zumwalt School District student.

Emerging Threats and Lesser-Known Actors:
Other cybercriminal entities, including Carbonic AKA @MarxistAttorney, Chief AKA @Puttied, Chrichir, Clinkz48, Cryptolulz666, HaX0r Beast Prayer, HelloKitty, JM511, Kyfx, MoRo, NLB Team, PayorGrief, Pinoy Grayhats, Sahoo, Sc0rp!n Att@ck3r from Muslim Cyber Army, Sharpboys, SingularityMD, and X-saad, have also been involved in cyberattacks against educational institutions.

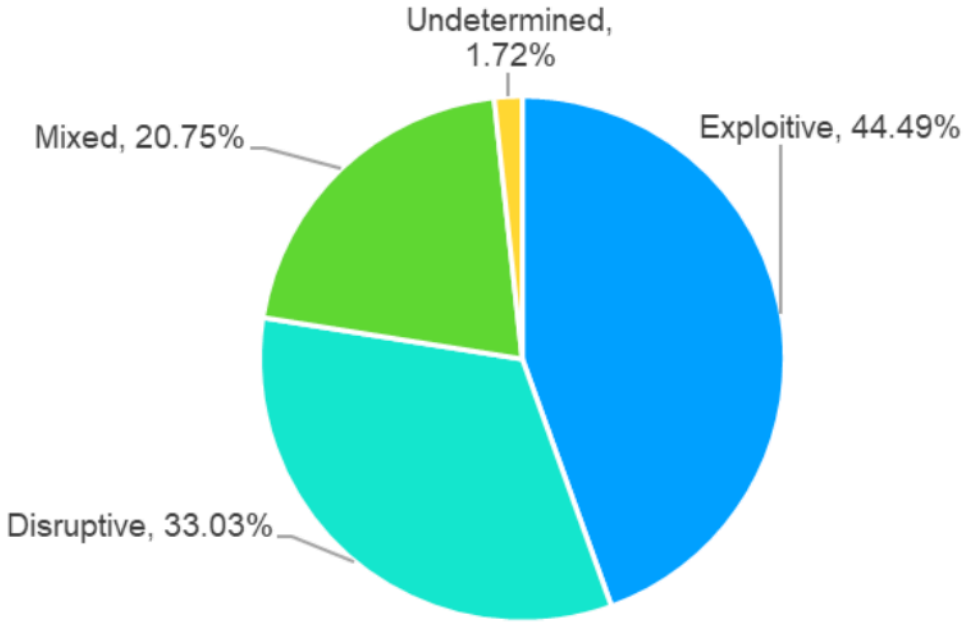

Figure 4: Wordwide Exploit Type on Education Institutes

Figure 4 shows key exploit types of education institutes worldwide. Cyber threats come from various actors with distinct motivations and objectives. Cyber Criminals

operate for financial gain, engaging in activities like data theft, ransomware attacks, and fraud to exploit individuals and organizations. Cyber Hacktivists, on the other hand, are ideologically driven, using cyber tactics to protest, disrupt institutions, leak sensitive information, or deface websites to make a social or political statement. Meanwhile, Cyber Hobbyists are motivated by curiosity and personal challenges rather than malice or financial incentives. They may explore security vulnerabilities but typically avoid causing harm. Cyber Nation-State actors are government-sponsored operatives who engage in cyber espionage, infrastructure disruption, and strategic cyber warfare against foreign entities, corporations, and national security agencies. Finally, Cyber Terrorists employ cyber tactics to advance extremist agendas, targeting digital infrastructure, spreading propaganda, and even conducting cyber sabotage to instill fear and chaos. Each of these threat actors presents unique cybersecurity challenges that require targeted defensive strategies.

Further Figure 5 shows analysis of hacking motive on various education institutes. Hacking motives vary widely, with financial gain being the predominant driver, accounting for 66.74% of attacks. Cybercriminals often exploit vulnerabilities to steal sensitive data, launch ransomware campaigns, or conduct fraud for monetary benefits. Political espionage (1.42%) and industrial espionage (0.30%) involve the unauthorized acquisition of information to gain strategic advantages, whether for state-sponsored operations or corporate competition. Motivations tied to protest represent 4.49%, where hacktivists disrupt systems to make ideological or social statements, while a small fraction (0.07%) combines both protest and financial incentives. Personal attacks (0.22%) stem from individual vendettas, targeting specific people or organizations. Sabotage (0.15%) entails deliberate destruction or disruption of systems, often aimed at critical infrastructure. However, a significant portion (26.59%) remains undetermined, indicating cases where hackers' true motives are unclear or evolving.

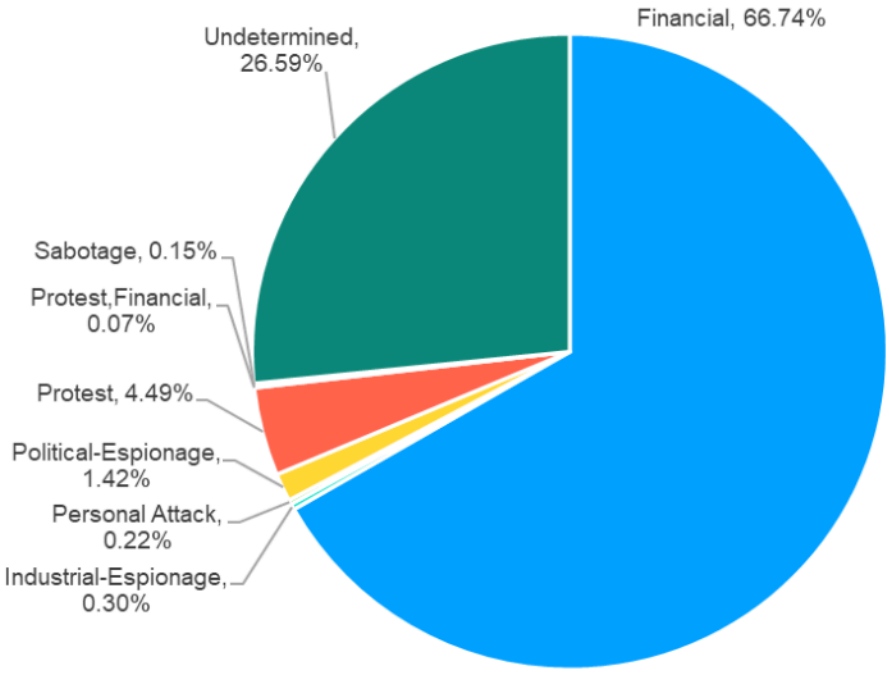

Figure 5: Wordwide Hacking Motive on Education Institutes

Undetermined cyberattacks, where hackers' motives remain unclear or evolve over time, pose significant risks due to their unpredictability. Without a clear intent, education institutes may struggle to detect, assess, and respond to the threat in a timely manner. These attacks often unfold in multi-stage operations, starting with minor breaches that later escalate to ransomware, espionage, or data theft. Attackers may maintain persistent access, modifying security settings and exfiltrating sensitive data without triggering immediate alarms. Additionally, attribution becomes difficult, making it harder to implement effective countermeasures against unknown threat actors. Cybercriminals with shifting motives can adapt their strategies dynamically, rendering traditional defense mechanisms less effective. In educational institutions, such evolving cyber threats can lead to financial fraud, research data theft, or student record compromises, increasing operational and reputational risks.

Understanding these motives helps organizations develop targeted cybersecurity defenses.

As shown in Figure 6, cyberattacks are carried out by various types of threat actors on education institutes, each driven by distinct motives and expertise levels.

The majority of cyber threats - 86.89% - are perpetrated by cyber criminals, who engage in illegal activities such as fraud, ransomware attacks, and data breaches for financial gain. Hacktivists (5.47%) target organizations or governments to make ideological or political statements, often through website defacements, data leaks, or service disruptions. Cyber hobbyists (1.12%) explore security vulnerabilities for curiosity or personal challenge, typically without harmful intent. Nation-state actors

(2.02%) conduct cyber espionage, sabotage, or infrastructure attacks on behalf of governments, often targeting foreign entities for strategic advantage. Cyber terrorists (0.07%) leverage hacking to further extremist causes, aiming to disrupt operations or spread propaganda. Meanwhile, 4.42% of attacks remain undetermined, indicating cases where the nature and intent of the attackers are unclear.

As shown in Figure 7, cyber threat actors operate worldwide on education institutes with varying motivations and attack methods. Undetermined actors account for the largest percentage (66.59%), where attribution remains unclear due to sophisticated obfuscation techniques. Among identifiable groups, Vice Society (5.09%) is a prominent ransomware collective known for targeting educational and healthcare institutions. Cl0p (2.40%) and Clop (1.57%) specialize in ransomware operations, often exploiting vulnerabilities in enterprise systems. Silent Librarian (1.57%) is an Iranian-backed cyber espionage group that focuses on stealing academic research. TA505 (0.90%) is a financially motivated group known for large-scale banking malware and ransomware attacks.

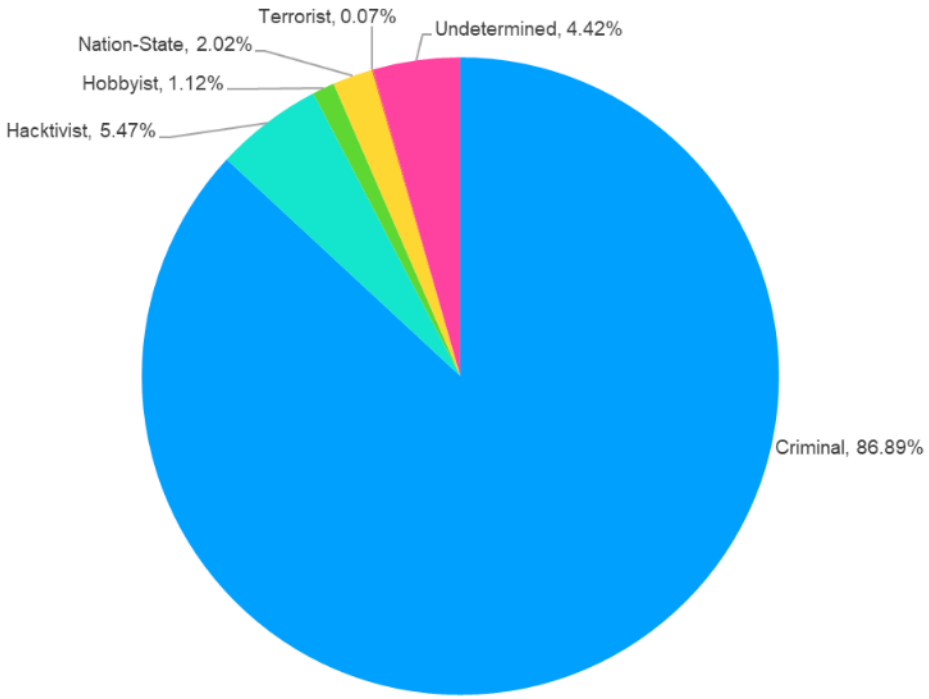

Figure 6: Hacker Types on Worldwide Education Institutes

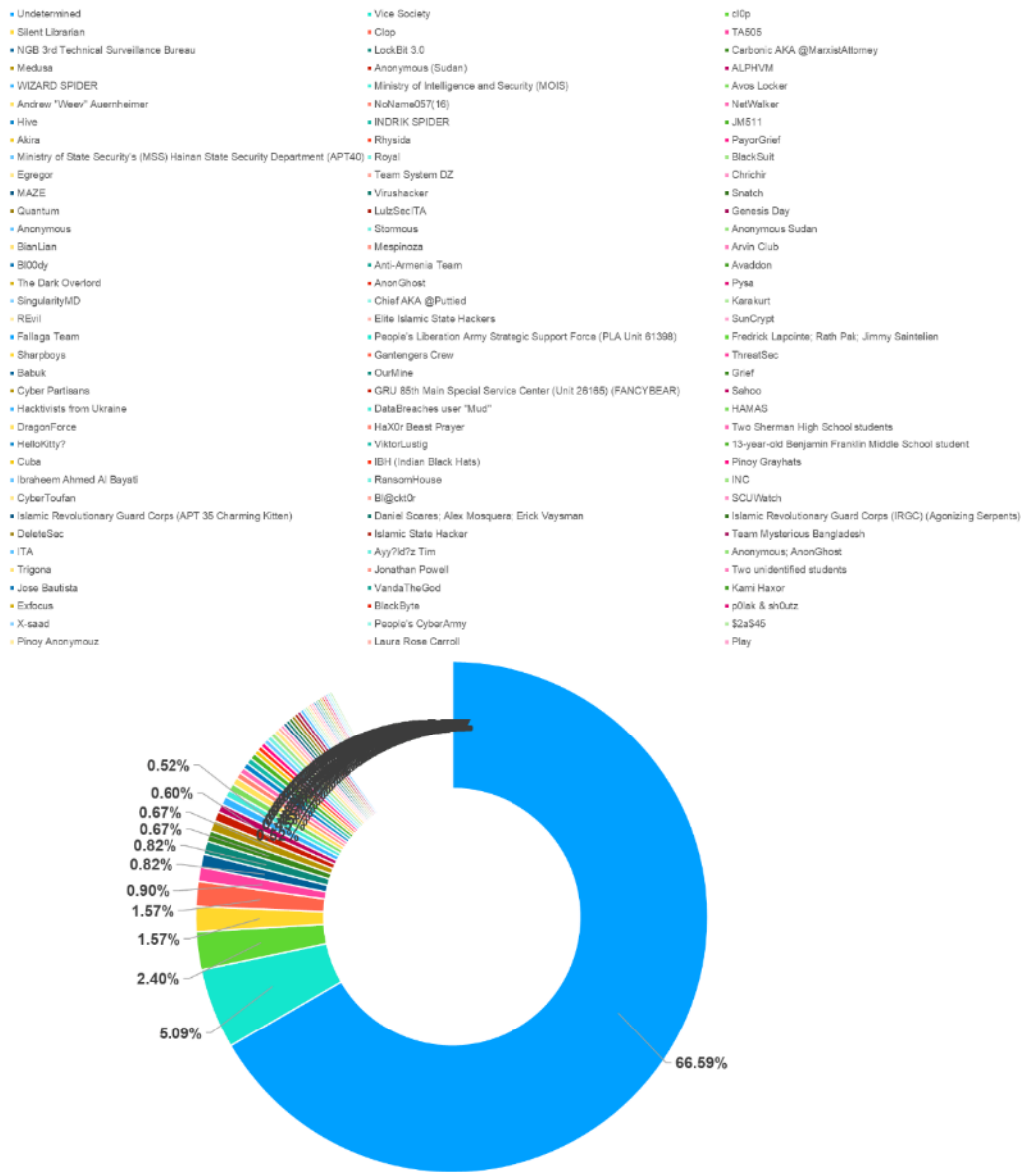

Figure 7: Worldwide Threat Actors on Education Institutes

Nation-state-affiliated groups include NGB 3rd Technical Surveillance Bureau (0.82%), linked to Chinese cyber-espionage operations, and LockBit 3.0 (0.82%), a highly prolific ransomware-as-a-service (RaaS) group. Other prominent attackers include Medusa (0.67%), WIZARD SPIDER (0.52%) - the operators of TrickBot malware - and Ministry of Intelligence and Security (MOIS) (0.45%), an Iranian cyber espionage entity.

Hacktivist and politically motivated actors include Anonymous (Sudan) (0.60%), NoName057(16) (0.37%), and Cyber Partisans (0.07%), each targeting governments

and institutions based on ideological motives. Ransomware operators like Hive (0.37%), Akira (0.30%), and BlackSuit (0.30%) focus on extortion through encrypted data theft. Egregor (0.30%) and Royal (0.30%) are also well-known ransomware players.

Other groups with targeted cyberattack capabilities include NetWalker (0.37%), JM511 (0.37%), and Rhysida (0.30%). State-sponsored espionage activities involve APT40 (0.30%) from China, GRU Unit 26165 (FANCY BEAR) (0.07%) from Russia, and Islamic Revolutionary Guard Corps (APT35 Charming Kitten) (0.07%) from Iran.

With this diverse range of threat actors, cybersecurity defenses must adapt continuously to counter evolving tactics and persistent risks from financially motivated criminals, hacktivists, espionage groups, and cyber terrorists.

3. Cyber Threats On Education Institutes Of Top 8 Victim Countries

The majority of cyberattacks targeting educational institutions have originated from the USA, UK, Canada, Australia, India, Germany, Ireland, and Italy. Analyzing this dataset provides valuable insights into the evolving cyber threat ecosystem, helping to understand attack patterns, motivations, and vulnerabilities within the education sector. These findings can assist in developing more effective cybersecurity strategies to mitigate risks and strengthen institutional defenses.

Refer to "Section 7 – List of Abbreviations Used in Images and Graphs" for the abbreviations applied in the diagrams and graphs within this section.

As illustrated in the Figure 8, cyber-attacks targeting educational institutions in the USA encompass a wide range of threats, originating from hacktivists, hobbyists, nation-state actors, and unidentified entities, each utilizing distinct attack methods.

Cybercriminal Activities Targeting USA's Education Institutes

The majority of cyber threats stem from criminal actors utilizing various exploitation techniques. A substantial portion remains undetermined, highlighting the need for improved threat intelligence and attribution efforts. Notable identified cybercriminal groups include Jose Bautista (USA), Exfocus (Mexico), Jonathan Powell (USA), The Dark Overlord (UK), WIZARD SPIDER (Russian Federation), INDRIK SPIDER (Russian Federation), MAZE, and Clop (Russian Federation), all engaging in EoAS, EoEH, MM, DA, and IDoS tactics.

Financial motives dominate cybercrime, with Avaddon (Russian Federation), NetWalker, Pysa, SunCrypt, DoppelPaymer (Russian Federation), and PayorGrief executing widespread ransomware campaigns. Disruptive attacks, including EDoS and DA, were commonly used by LockBit 3.0 (Undetermined) and ALPHVM (Russian Federation) to cripple targeted entities.

Additionally, mixed attack types - combining financial incentives with disruptive or espionage-focused tactics—were seen among Mespinoza, Quantum, Cuba, Vice

Society, and Rhysida, employing EoAS, DA, MM, IDoS, and other methods to maximize their impact.

Hacktivist Operations Targeting USA's Education Institutes

Hacktivist collectives like Anonymous, NullCrew, AnonGhost, and VandaTheGod spearheaded disruptive and exploitative cyber campaigns, frequently linked to protest movements. Their methods primarily included MM and EoAS, used to deface websites or manipulate online narratives. Elite Islamic State Hackers (USA), Team System DZ (Algeria), and MIUM (Saudi Arabia) executed similar disruptive cyber actions.

Notably, Mirai (Russian Federation) leveraged EDoS to paralyze online services, demonstrating how hacktivists harness digital vulnerabilities to amplify their ideological influence.

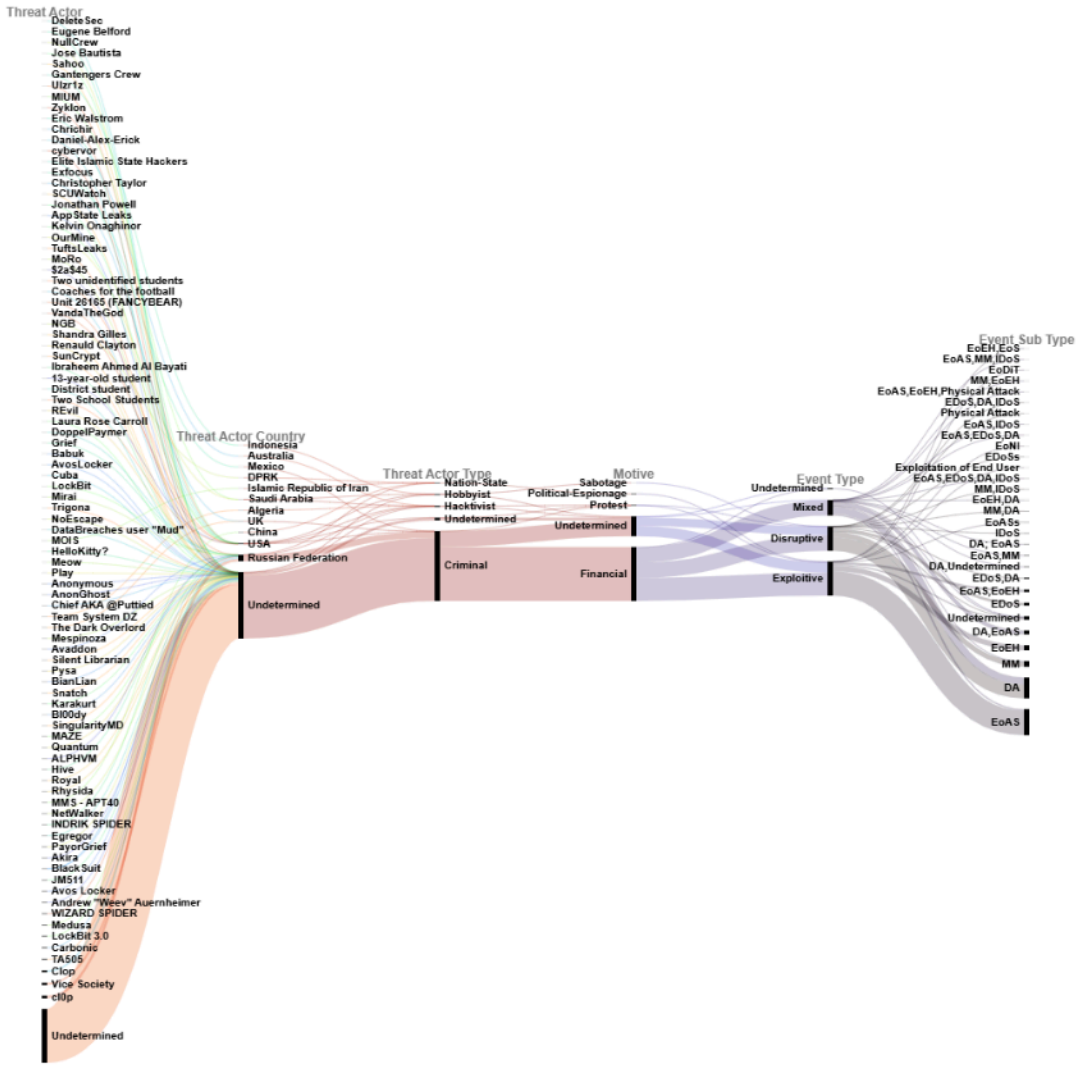

Figure 8: Cyber Threats on Education Institutes of USA

Hobbyist Activities Targeting USA's Education Institutes

Unlike hacktivists, hobbyist attackers - including Zyklon, Gantengers Crew (Indonesia), Chief AKA @Puttied, OurMine (Saudi Arabia), and Two School Students (USA) - engaged in cyber exploits for exploration rather than financial or ideological motivations. These attacks frequently involved EoAS and MM, though Eric Walstrom (USA) and Daniel-Alex-Erick caused disruptive DA, indicating amateur hackers can still inflict damage. Two unidentified students (USA) escalated hobbyist activity into sabotage, demonstrating that even recreational hacking can lead to significant disruptions.

Nation-State Espionage Targeting USA's Education Institutes

Cyber espionage remains a major geopolitical tool, with Unit 26165 (FANCYBEAR) (Russian Federation), MMS - APT40 (China), NGB (DPRK), and MOIS (Iran) engaged in politically motivated espionage. These state-backed actors primarily employed EoAS and EoEH to extract intelligence and disrupt foreign operations, highlighting cyber warfare as an ongoing national security concern.

Unidentified and Mixed Threats Targeting USA's Education Institutes

Several cybercriminal activities remain undetermined, including attacks from Carbonic, cybervor, JM511, SCUWatch, AppState Leaks, Silent Librarian, and Coaches for the football. Their methods predominantly involve EoAS and MM, demonstrating a combination of data exploitation and disruptive manipulation. Some, like TuftsLeaks, were protest-driven, targeting institutions via cyber tactics. Figures such as Weev, Laura Rose Carroll, and Shandra Gilles contributed to mixed-threat cyber activities, incorporating EoAS, IDoS, and DA.

This data showcases a multifaceted cyber threat ecosystem of USA, where attack vectors range from hacktivism and espionage to hobbyist-driven exploits and unidentified cyber operations.

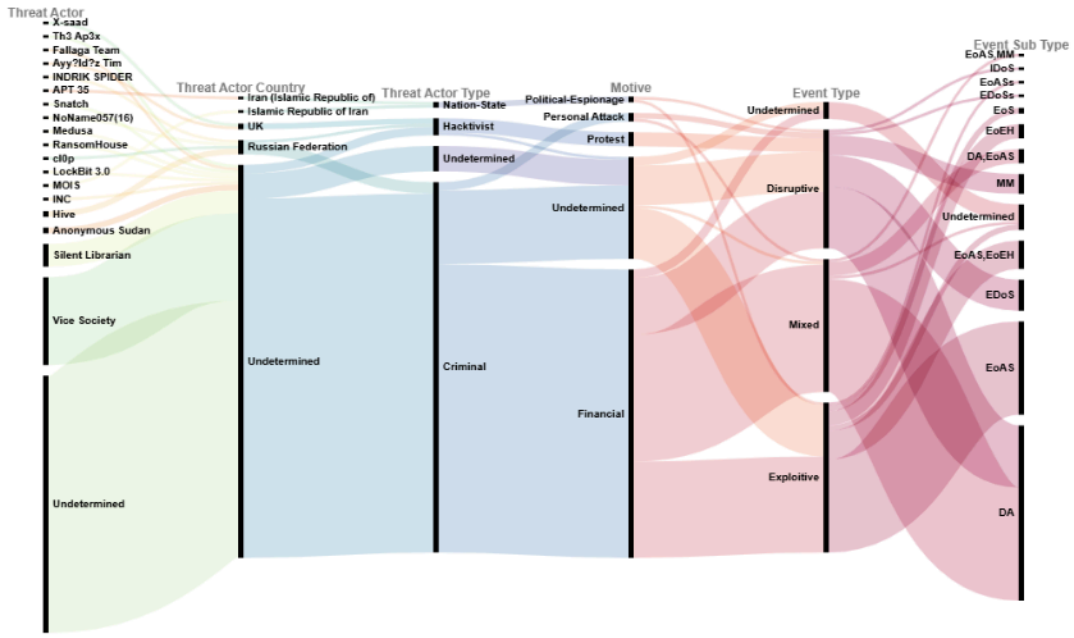

Figure 9: Cyber Threats on Education Institutes of UK

As shown in Figure 9, the cyber threats targeting educational institutions in the UK reveal a diverse array of attack methods, with actors ranging from criminal enterprises and hacktivists to nation-state espionage groups.

Criminal Cyber Threats Targeting UK's Education Institutes

A significant proportion of cyberattacks on UK education institutions originate from undetermined criminal actors, emphasizing the challenge of attributing cyber operations. These threats primarily employ EoAS (Exploitation of Application Server), EoEH (Exploitation of End Host), DA (Data Attack), and MM (Message Manipulation) to target systems for financial gain, personal attacks, and disruption. INDRIK SPIDER (Russian Federation) follows a mixed attack approach, combining DA and EoAS to maximize impact. Vice Society appears frequently in financially motivated cyberattacks, conducting DA-driven extortion campaigns.

Additionally, Silent Librarian has emerged as a persistent cyber espionage entity, executing EoAS and EoEH-based exploits targeting academic research and sensitive institutional data.

Hacktivist Activities Targeting UK's Education Institutes

Hacktivist groups play a notable role in disrupting UK education institutions. X-saad (UK), Fallaga Team, Anonymous Sudan, NoName057(16) (Russian Federation), and Ayy?ld?z Tim (UK) primarily engage in MM-driven disruptive cyber operations, often associated with protest movements. Mirai (Russian Federation) notably employed EDoS (External Denial of Service) tactics, illustrating the use of botnets to overwhelm network resources.

Nation-State Espionage Targeting UK's Education Institutes

Nation-state actors involved in cyber threats against UK institutions include MOIS (Iran) and APT 35 (Islamic Revolutionary Guard Corps (APT 35 Charming Kitten)), both conducting political-espionage cyber operations. Their tactics predominantly involve MM-driven disruptions and undetermined exploitation strategies, reflecting state-sponsored intelligence gathering efforts.

The data of cyber-attacks on UK's education institutes highlights a complex cyber threat landscape, where criminal entities, hacktivists, and nation-state actors exploit education institutions for various motives.

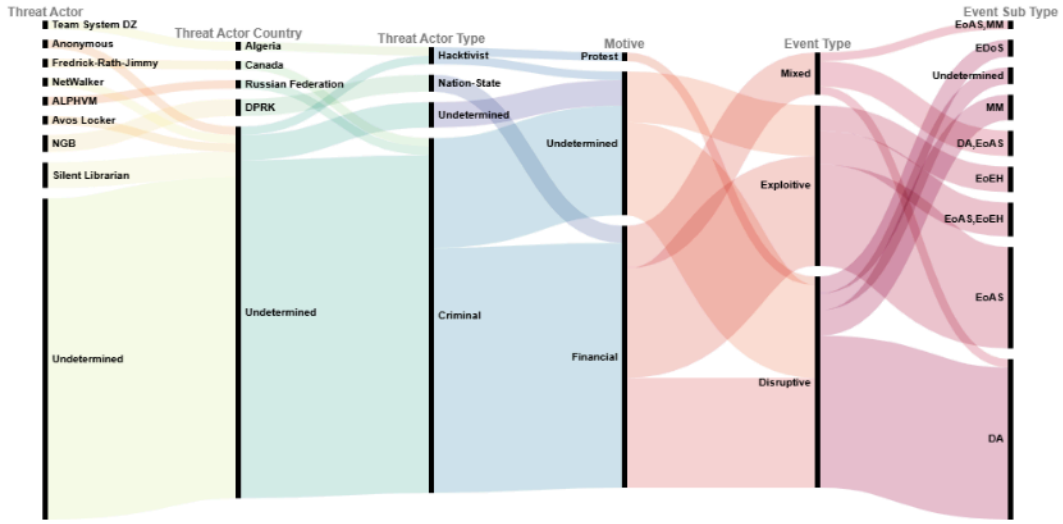

Figure 10: Cyber Threats on Education Institutes of Canada

Figure 10 illustrates the diverse cyber threat landscape facing Canada's educational institutions, where financially motivated cybercriminals, hacktivist groups, and nation-state actors employ a range of attack methods to exploit vulnerabilities.

Criminal Cyber Threats Targeting Canada's Education Institutes

A significant number of cyber-attacks come from undetermined criminal actors, making attribution challenging. These threats largely utilize EoAS (Exploitation of Application Server), EoEH (Exploitation of End Host), DA (Data Attack), and MM (Message Manipulation) to compromise educational institutions. Notable financial cyber threats include Fredrick-Rath-Jimmy (Canada), NetWalker, Avos Locker, and ALPHVM (Russian Federation), all engaging in disruptive and exploitative cyber operations.

Ransomware attacks and data exploitation are key attack vectors, with criminals using EoAS and EoEH to breach systems. Silent Librarian, a well-known espionage group, has repeatedly targeted Canadian institutions via EoAS and EoEH-based cyber exploitation.

Hacktivist Activities Targeting Canada's Education Institutes

Hacktivist groups play an active role in disrupting Canada's education sector, typically leveraging MM and EDoS (External Denial of Service) attacks. Groups such as Team System DZ (Algeria) and Anonymous executed protest-driven cyber disruptions, aiming to impact institutional operations.

Nation-State Espionage & Sabotage Targeting Canada's Education Institutes

Cyber threats tied to nation-state actors include NGB (DPRK), which conducted financially driven DA-based disruptions. These attacks indicate strategic efforts to destabilize infrastructure or extract valuable data from Canadian educational entities. The dataset of cyber-attacks on Canada's education institutes highlights a wide-ranging cyber threat landscape, where criminal enterprises, hacktivists, and nation-state actors employ cyberattacks ranging from financial extortion to ideological disruptions and espionage-driven intrusions.

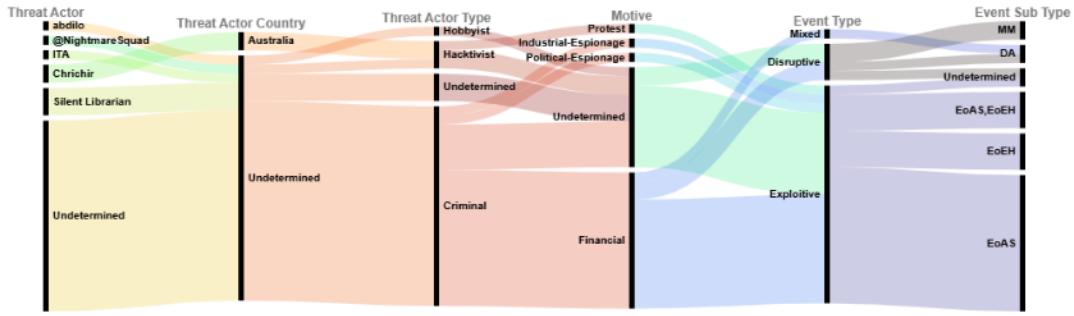

Figure 11: Cyber Threats on Education Institutes of Australia

As shown in Figure 11, cyber-attacks targeting Australian educational institutions highlight a mix of criminal operations, hacktivist disruptions, and hobbyist explorations, reflecting the broader cyber threat ecosystem.

Criminal Cyber Threats Targeting Australia's Education Institutes

The majority of cyber incidents involve undetermined criminal actors, making attribution difficult. These attacks predominantly employ EoAS (Exploitation of Application Server), EoEH (Exploitation of End Host), MM (Message Manipulation), and DA (Data Attack) to target educational systems. Financially motivated cyber threats are prevalent, using EoAS and EoEH for unauthorized access and data exploitation. Additionally, instances of industrial espionage and political espionage suggest that some actors seek strategic intelligence from Australian institutions.

Silent Librarian is particularly active, repeatedly leveraging EoAS and EoEH to infiltrate academic networks and compromise sensitive information.

Hacktivist Disruptions Targeting Australia's Education Institutes

Hacktivist groups such as Chrichir (Australia), @NightmareSquad, and Team System DZ (Algeria) engaged in exploitative cyber operations, utilizing EoAS to penetrate institutional defenses. Many of these activities are protest-driven, seeking to expose vulnerabilities or disrupt online infrastructure.

Hobbyist Activities Targeting Australia's Education Institutes

Some cyber incidents stem from hobbyist-driven exploits, including abdilo, whose tactics align with EoAS-based system exploitation. These attacks may not always be malicious but still pose risks to institutional security.

This dataset about cyber-attacks Australian educational institutions underscores a diverse cyber threat landscape, where criminal actors, hacktivists, and hobbyists exploit vulnerabilities in Australian education institutions.

As illustrated in Figure 12, cyber threats targeting India's educational institutions reveal a mix of criminal, hacktivist, hobbyist, and nation-state actors, each exploiting vulnerabilities using distinct attack methods.

Criminal Cyber Threats Targeting Australia's Education Institutes

The majority of cyber incidents in India's education sector originate from undetermined criminal actors, making attribution challenging. These attacks primarily leverage EoAS (Exploitation of Application Server), EoEH (Exploitation of End Host), DA (Data Attack), MM (Message Manipulation), and EDoS (External Denial of Service) to compromise systems. Financially motivated cyber actors, including ShinyHunters, ViktorLustig, and Arvin Club (Iran), focus on data exploitation using EoAS and EoEH to extract sensitive information.

Instances of protest-driven DA-based cyber disruptions indicate ideological motives behind some attacks.

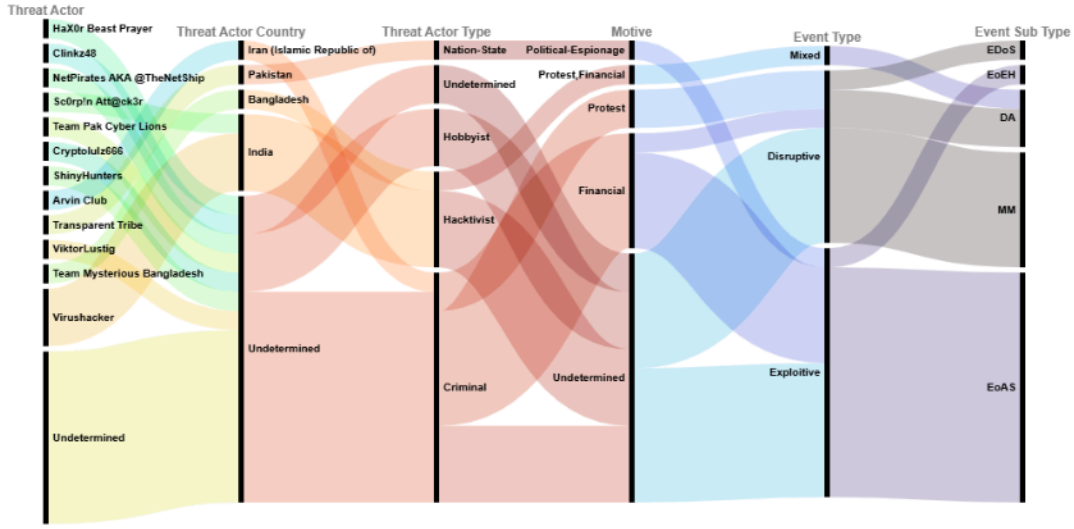

Figure 12: Cyber Threats on Education Institutes of India

Hacktivist Activities Targeting India's Education Institutes

Hacktivist groups actively target Indian institutions using MM and EoAS-based cyber exploits. Virushacker (India), Sc0rp!n Att@ck3r (India), and Team Mysterious Bangladesh (Bangladesh) frequently engage in disruptive and exploitative cyber operations, often linked to ideological or financial motives. Team Pak Cyber Lions

and @NightmareSquad executed similar attacks, with a focus on message manipulation tactics.

Hobbyist Cyber Operations Targeting India's Education Institutes

Some attacks stem from hobbyist-driven explorations, with HaX0r Beast Prayer, Clinkz48, and Cryptolulz666 conducting EoAS-based system exploitations. While hobbyist attacks may not always be malicious, they pose security risks to institutional networks.

Nation-State Espionage Targeting India's Education Institutes

Cyber espionage threats include Transparent Tribe (Pakistan), which engages in EoEH-driven political espionage to extract intelligence from Indian educational institutions. This suggests a broader strategy aimed at information warfare.

India's educational institutions face diverse cyber threats, ranging from financial exploitation and ideological disruptions to nation-state espionage operations.

As shown in Figure 13, cyber threats targeting Israel's educational institutions reveal a complex landscape involving criminal enterprises, hacktivist groups, nation-state actors, and terrorist organizations, each utilizing distinct attack methods.

Criminal Cyber Threats Targeting Israel's Education Institutes

A significant portion of cyberattacks originates from undetermined criminal actors, making attribution difficult. These cyber threats primarily employ EoAS (Exploitation of Application Server), DA (Data Attack), and EoASs (Exploitation of Application Servers) to compromise educational infrastructure. Sharpboys (Iran) carried out financially motivated EoAS-based exploitation, targeting institutional data.

Additionally, DragonForce executed EoASs-driven protest cyber operations, showcasing ideological motives behind some cyber disruptions.

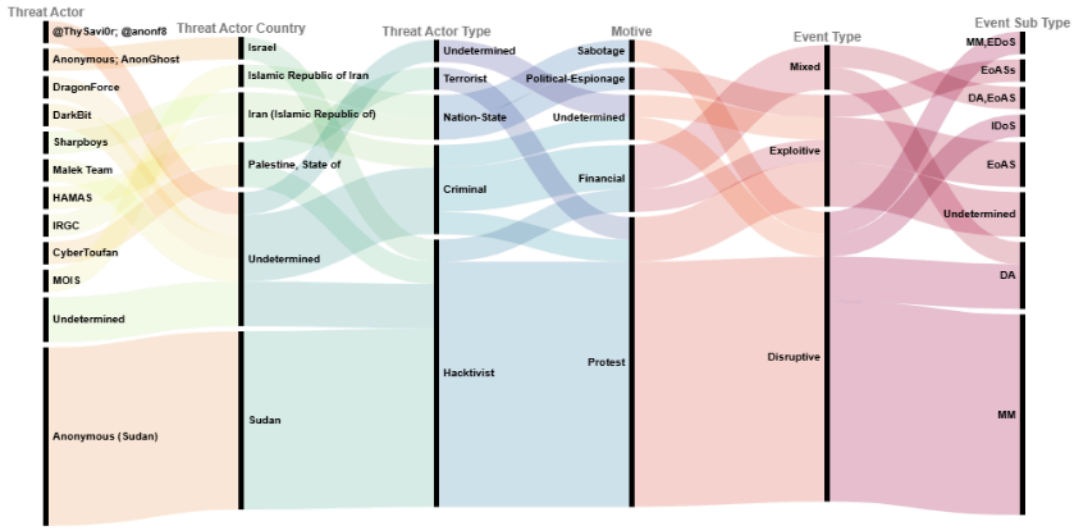

Figure 13: Cyber Threats on Education Institutes of Israel

Hacktivist Disruptions Targeting Israel's Education Institutes

Hacktivist groups actively target Israeli institutions, often using MM (Message Manipulation), IDoS (Internal Denial of Service), and EDoS (External Denial of Service) tactics. Prominent groups such as Anonymous; AnonGhost (Israel), DarkBit, Malek Team, CyberToufan (Palestine), and Anonymous (Sudan) were involved in protest-driven cyber disruptions, frequently using MM to manipulate information or disable online infrastructure. The recurring presence of Anonymous (Sudan) in multiple attack incidents suggests sustained efforts to target Israeli institutions.

Nation-State Espionage & Sabotage Targeting Israel's Education Institutes

Nation-state actors, including MOIS (Iran) and IRGC (Iran), pose a major cyber risk to Israeli institutions. MOIS conducted political espionage operations through undetermined exploitation techniques, likely to extract intelligence. Meanwhile, IRGC focused on DA-driven sabotage, indicating a more destructive approach to cyber warfare.

Terrorist Cyber Threats Targeting Israel's Education Institutes

Cyber threats from HAMAS (Palestine) highlight an emerging trend of terrorist-driven cyber disruptions. MM-based manipulations were employed as part of ideological cyber campaigns, aiming to spread misinformation or disrupt institutional operations.

Cyber threats against Israel's educational institutions demonstrate financially driven cyber exploitation, protest-based disruptions, espionage operations, and sabotage.

As shown in Figure 14, cyber-attacks targeting Germany's educational institutions highlight a mix of financially motivated cybercriminals, disruptive threat actors, and persistent espionage operations, impacting the security of academic infrastructure.

Financially Motivated Criminal Threats Targeting Germany's Education Institutes

A significant portion of cyber incidents is driven by financial exploitation, where criminals employ EoAS (Exploitation of Application Server) and DA (Data Attack) to access and manipulate sensitive institutional data. Vice Society, a well-known ransomware group, was involved in multiple mixed financial attacks, combining DA-driven data breaches with exploitative techniques to maximize disruption.

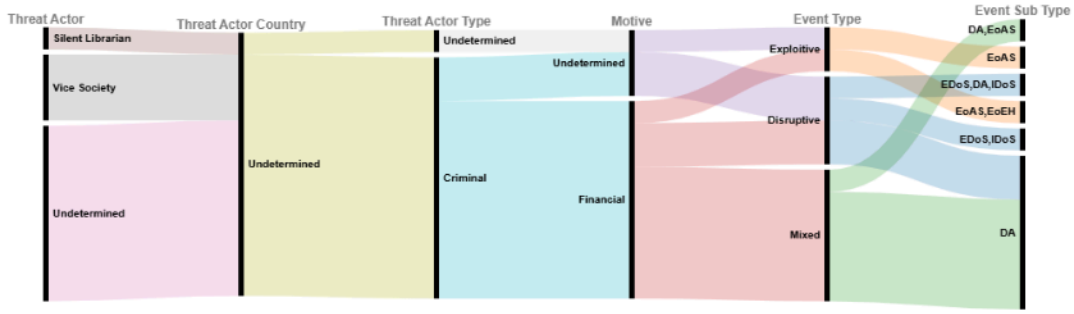

Figure 14: Cyber Threats on Education Institutes of Germany

Disruptive Cyber Operations Targeting Germany's Education Institutes

Several cybercriminal incidents utilized EDoS (External Denial of Service), DA, and IDoS (Internal Denial of Service) to cripple institutional networks and disrupt online services. Attackers with undetermined attribution carried out aggressive disruptive cyber operations, reflecting the broader trend of targeted disruptions in the education sector.

Espionage and Intelligence Exploitation Targeting Germany's Education Institutes

Silent Librarian, a persistent cyber espionage entity, executed EoAS and EoEH (Exploitation of End Host)-driven attacks, likely targeting academic research and institutional data. Their repeated presence suggests a well-coordinated effort to infiltrate educational institutions for intelligence gathering.

Cyber threats against Germany's educational institutions demonstrate a high frequency of financially motivated cybercriminal operations, strategic espionage campaigns, and disruptive cyber tactics.

As shown in Figure 15, cyber threats targeting Italy's educational institutions exhibit a varied attack landscape, involving criminal entities, hacktivist groups, and nation-state actors, each exploiting vulnerabilities using distinct methods.

Criminal Cyber Threats Targeting Italy's Education Institutes

Several cyber-attacks against Italian education institutions stem from undetermined criminal actors, making attribution difficult. These groups primarily use EoEH

(Exploitation of End Host) and EoAS (Exploitation of Application Server) to infiltrate systems and compromise sensitive data. Financially motivated cybercriminal groups, including Royal, Rhysida, and LockBit 3.0, employed DA (Data Attack) and EoAS-driven exploitations, targeting institutions such as University Tor Vergata, University of Salerno, Metronotte Vigilanza, and Comitato Elettrotecnico Italiano.

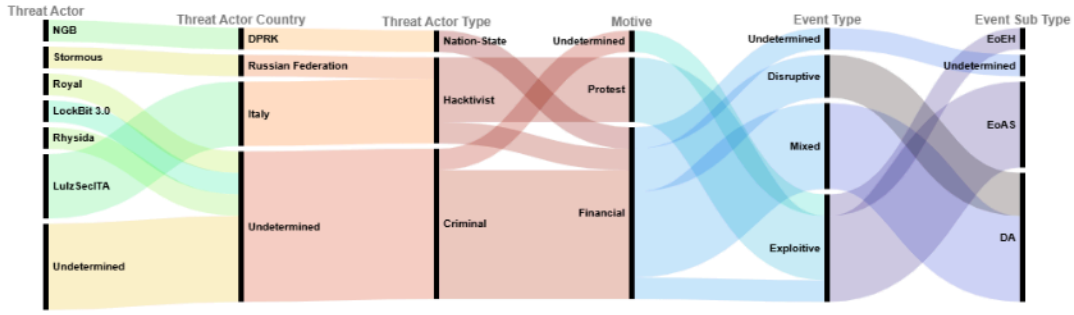

Figure 15: Cyber Threats on Education Institutes of Italy

Hacktivist Disruptions Targeting Italy's Education Institutes

Hacktivist groups actively target educational institutions in Italy, using EoAS-driven exploits and DA-based disruptive attacks. LulzSecITA (Italy) launched protest-driven cyber disruptions against multiple universities, including Roma Tre University, University of Basilicata, and University of Napoli. Meanwhile, Stormous (Russian Federation) conducted mixed financial cyber operations against University Roma Tor Vergata, highlighting broader hacktivist campaigns impacting the academic sector.

Nation-State Cyber Operations Targeting Italy's Education Institutes

Nation-state threats include NGB (DPRK), which engaged in financially motivated DA-driven cyber disruptions against University of Milano-Bicocca. These actions indicate a broader geopolitical cyber strategy, where state-sponsored actors target foreign educational institutions to destabilize infrastructure or extract valuable data.
Cyber threats against Italy's educational institutions demonstrate a mix of financially motivated cyber exploitation, protest-driven hacktivist activity, and state-sponsored cyber disruptions.

4. Gaps and Challenges in Cybersecurity Implementation for Education Institutes

Recent research indicates that educational institutions face significant challenges in implementing cybersecurity effectively. These challenges include limited budgets and resources, insufficient cybersecurity awareness among staff and students, difficulties in managing a diverse range of devices (Bring Your Own Device - BYOD - challenges), the need to balance openness and security within academic networks, and the protection of sensitive student and research data [6].

Figure 16 reveals the typical cyber threat landscape for any education institute, which consists of malware attacks, phishing attacks, insider threats, web attacks, and ransomware. Summarizing this, educational institutions are frequent targets of cyberattacks, with mission-critical assets at high risk. Understanding these assets and the threats they face is essential for strengthening cybersecurity defenses [27, 28]. Below are few high-risk Mission Critical Assets in Education Institutions.

Student & Faculty PII, Academic, & Health Data

Personally Identifiable Information (PII), academic records, and health data are prime targets for cybercriminals. These assets can be exploited for identity theft, financial fraud, or ransom demands. Attack methods like EoAS (Exploitation of Application Server), DA (Data Attack), and EoEH (Exploitation of End Host) frequently target databases holding this sensitive information.

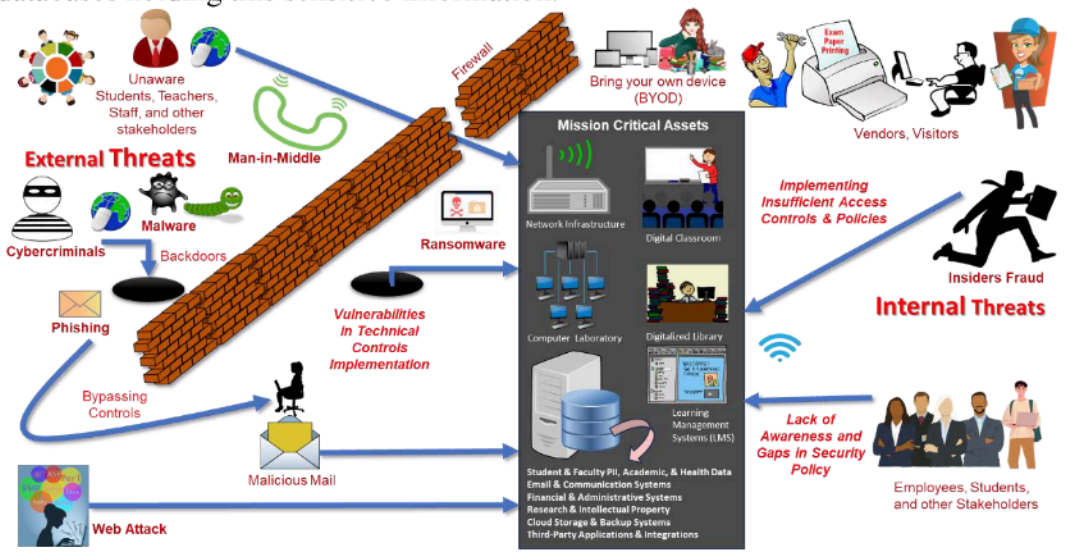

Figure 16: Typical Cyber Threats on Education Institutes

Email & Communication Systems

Phishing, Business Email Compromise (BEC), and ransomware attacks frequently exploit vulnerabilities in institutional email systems. Attackers use MM (Message Manipulation) techniques to spread malware, impersonate faculty, or exfiltrate confidential data.

Financial & Administrative Systems

Cybercriminals often infiltrate financial databases and payroll systems through techniques like EoAS and DA, seeking unauthorized access to funds, payrolls, and financial aid records. Attack groups such as Vice Society and LockBit 3.0 have historically targeted financial assets within education institutions.

Research & Intellectual Property
Academic research, patents, and sensitive institutional data are valuable targets for nation-state espionage actors like MOIS (Iran) and NGB (DPRK). These actors leverage EoEH-driven exploits to exfiltrate intellectual property, threatening institutional credibility and national security.

Cloud Storage & Backup Systems
Cloud-based repositories and backup storage are prime targets for ransomware gangs like Royal and Rhysida, who attempt to encrypt or delete institutional backups. Techniques such as EoAS and DA-based sabotage have been used to compromise cloud security.

Third-Party Applications & Integrations
Many institutions rely on third-party services for administration, communication, and learning. Attackers exploit API vulnerabilities and integration points, using EoAS and EoEH to gain lateral access and expand breaches across interconnected platforms.

Network Infrastructure
Attackers frequently use EDoS and IDoS (Internal Denial of Service) to overwhelm institutional networks, disrupting student access and online learning. Recent cases show institutions falling victim to disruptive cyber operations targeting their networks.

Digital Classroom
Learning platforms, virtual classrooms, and online examination systems face cyber risks ranging from EoAS-driven exploits to MM-based data tampering, allowing attackers to manipulate academic records or disrupt exams.

Computer Laboratories
Laboratories housing high-performance computing systems are often targeted via EoEH exploits, where attackers attempt unauthorized access to research databases, student records, or institution-wide administrative tools.

Learning Management Systems (LMS)
LMS platforms facilitate course administration, grading, and content sharing. Cyber threats such as EoAS-driven exploits and DA-based manipulations can lead to data leaks, credential theft, and system outages, disrupting academic operations.

In short, education institutions face multi-faceted cyber threats, with attackers targeting financial resources, academic integrity, infrastructure, and intellectual property.

Recent research indicates that educational institutions face significant challenges in implementing cybersecurity effectively. These challenges include limited budgets and resources, insufficient cybersecurity awareness among staff and students, difficulties in managing a diverse range of devices (Bring Your Own Device - BYOD - challenges), the need to balance openness and security within academic networks, and the protection of sensitive student and research data [6]. Another research work explains a misalignment between existing legislation and advancements in digital technologies, the absence of clearly defined cybersecurity norms and standards, inadequate confidentiality measures and personal data protection, a shortage of knowledgeable cybersecurity professionals and dedicated units, low awareness among specialists, and the influence of political factors further complicate cybersecurity efforts in the education sector [7].

Universities face significant cybersecurity challenges due to their diverse IT environments, where legacy systems, modern applications, and various devices create multiple vulnerabilities. Their decentralized structure, with individual departments managing their own IT resources, often results in inconsistent security practices and weak points in overall protection. Additionally, the open-access culture prioritizes collaboration and information sharing, which can conflict with stringent security measures, increasing the risk of cyber threats. Lastly, resource constraints, including limited budgets and competing priorities, hinder investments in robust cybersecurity infrastructure and personnel, making it difficult for universities to implement comprehensive security initiatives [38, 39, 40].

5. RELATED WORK

The Business Domain Specific Least Cybersecurity Controls Implementation (BDSLCCI) framework is a cybersecurity framework designed to help organizations, especially micro, small and medium enterprises (MSMEs), depending on region which are also known as small and medium enterprises (SMEs) or small and medium businesses (SMBs), prioritize and implement cybersecurity controls based on their specific business domains. BDSLCCI Framework provides a step-by-step approach to enhance an organization's cybersecurity posture by focusing on business-critical assets and operations. Mission Critical Asset (MCA) is the core asset vital to an organization's operations, such as critical operation computerized system, sensitive databases, software applications, or even digital infrastructure [22, 24, 25, 26].

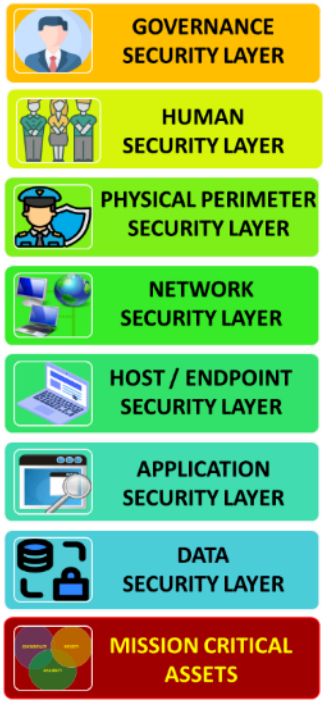

Figure 17: Defense in Depth in BDSLCCI

Defense in Depth: A Multi-Layered Protection Model

Beyond the CIA triad, as shown in Figure 17, BDSLCCI implements a Defense in Depth (DiD) approach, layering security controls across network security, data security, human security, application security, and physical security. By adopting this comprehensive cybersecurity model, educational institutions can mitigate risks associated with open-access networks, Bring Your Own Device (BYOD) policies, and limited IT resources.

Implementing cybersecurity in education requires strategic investment, policy enforcement, and proactive risk management. The BDSLCCI framework enables institutions to overcome financial constraints, align cybersecurity practices with academic operations, and reduce vulnerabilities to cyber threats. By integrating this framework, universities and schools can fortify their defenses, ensuring a secure and resilient learning environment for students and educators.

Figure 18 outlines the Defense in Depth (DiD) layers as defined by the BDSLCCI framework. It categorizes cybersecurity controls into distinct layers, each addressing specific aspects of organizational security. These layers include host/endpoint security, data security, human security, network security, application security, and physical perimeter security. Each layer is further broken down into actionable control areas, such as endpoint protection, encryption, cybersecurity awareness training, network firewalls, application hardening, and physical access controls. This structured approach ensures a comprehensive and prioritized defense strategy,

tailored to mitigate modern cyber threats effectively. The framework emphasizes practical implementation, particularly for small and medium-sized enterprises (SMEs), to enhance their cybersecurity posture systematically [22, 24, 25, 26].

The BDSLCCI (Business Domain Specific Least Cybersecurity Controls Implementation) framework is a strategic approach that enables educational institutions to protect their mission-critical assets by applying the CIA triad - Confidentiality, Integrity, and Availability.

As shown in Figure 19, CIA triad has overlap of each component, but those can be prioritized for each mission critical asset (MCA). Depending on MCA's security priority requirement, priority of the implementation of either Confidentiality, Integrity, and Availability [22, 24, 25, 26].

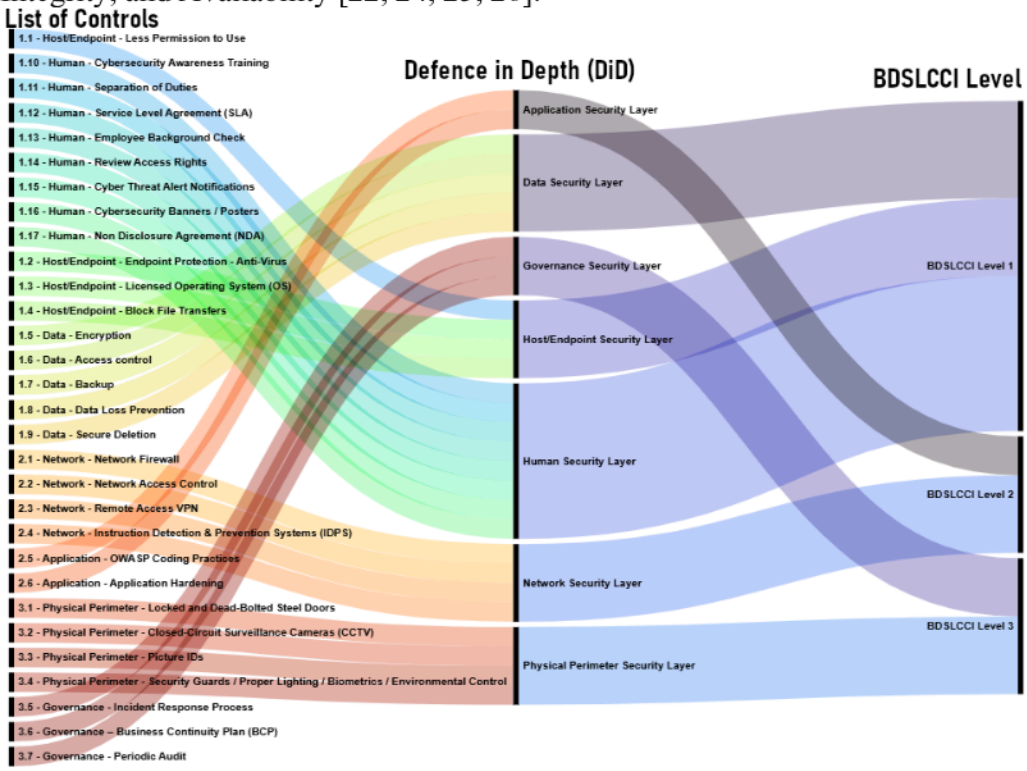

Figure 18: BDSLCCI Framework covering detailed Defense in Depth (DiD) Controls

Prioritization in MCA for CIA triad according to BDSLCCI

For PII data, financial records, and sensitive information such as exam papers — classified as Mission Critical Assets (MCAs) — the BDSLCCI framework recommends prioritizing confidentiality as the first cybersecurity measure. Ensuring data privacy through encryption, access control, and secure storage prevents unauthorized access or breaches. Once confidentiality controls are fully implemented, integrity and availability measures can be introduced in subsequent phases to

strengthen overall security.

For Learning Management Systems (LMS), classified as an MCA, availability should be the primary focus according to BDSLCCI. Since LMS downtime can lead to productivity loss and disruption in academic activities, institutions should first implement cybersecurity controls that ensure continuous accessibility. After securing availability, integrity and confidentiality controls can be introduced to safeguard academic records and prevent unauthorized modifications.

For laboratories engaged in sensitive research work, integrity must be the top priority within the BDSLCCI framework. Any compromise in integrity could have serious consequences, potentially affecting critical systems and, in extreme cases, posing risks to human safety. Therefore, integrity-focused cybersecurity measures — such as cryptographic validation, secure backups, and access monitoring — should be applied first. Once integrity is secured, confidentiality and availability controls can be implemented to further enhance protection in accordance with BDSLCCI recommendations [22, 24, 25, 26].

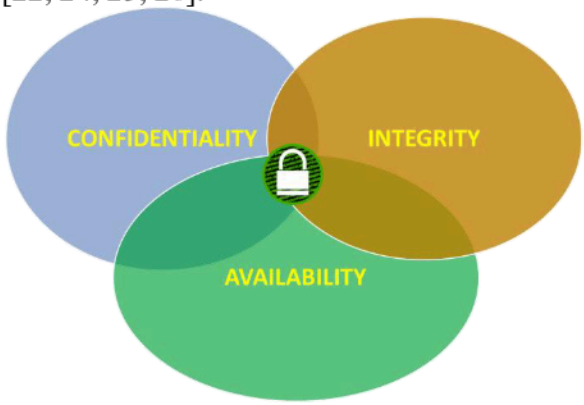

Figure 19: CIA Traid for MCA

BDSLCCI Framework Implementation Levels

The BDSLCCI framework is composed of three distinct levels of cybersecurity controls, each representing a foundational stage of cybersecurity maturity.

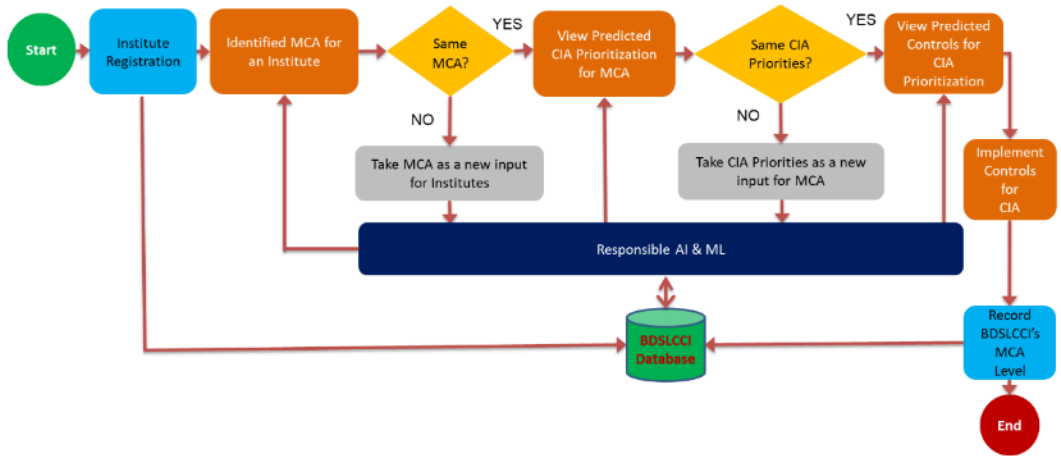

Figure 20: BDSLCCI Recommended MCA Cybersecurity Controls Implementation Flow for Education Institute

As shown in Figure 20, the BDSLCCI framework, available as a web platform, is preconfigured with various Mission Critical Assets (MCAs) for educational institutions. The top management of the institution must evaluate and prioritize which MCAs should be addressed first. If a required MCA is not available on the web platform, the institution can request its inclusion. Based on the selected MCA's priority in terms of confidentiality, integrity, and availability, the institution can systematically advance the deployment of cybersecurity controls.

As illustrated in Figure 21, various layers of Defense in Depth (DiD) can be implemented incrementally, following the recommendations of the BDSLCCI framework. This process is typically carried out in parallel with the implementation of cybersecurity controls for Mission Critical Assets (MCAs).

BDSLCCI Level 1 focuses on implementing cybersecurity controls for Mission Critical Assets (MCA), prioritizing confidentiality, integrity, or availability based on their criticality. At this stage, institutions establish security measures within the Host/Endpoint Security Layer, Data Security Layer, and Human Security Layer, ensuring protection at the fundamental level.

BDSLCCI Level 2 builds upon the first level by addressing cybersecurity controls for the second priority area of MCA, again emphasizing confidentiality, integrity, or availability based on specific institutional needs. This phase integrates security measures within the Network Security Layer and Application Security Layer, enhancing digital defense and operational security.

BDSLCCI Level 3 completes the framework by securing the remaining aspect of confidentiality, integrity, or availability for MCAs. It incorporates Physical Perimeter Security Layer and Governance Security Layer, ensuring a well-rounded cybersecurity strategy that includes infrastructure security and compliance management.

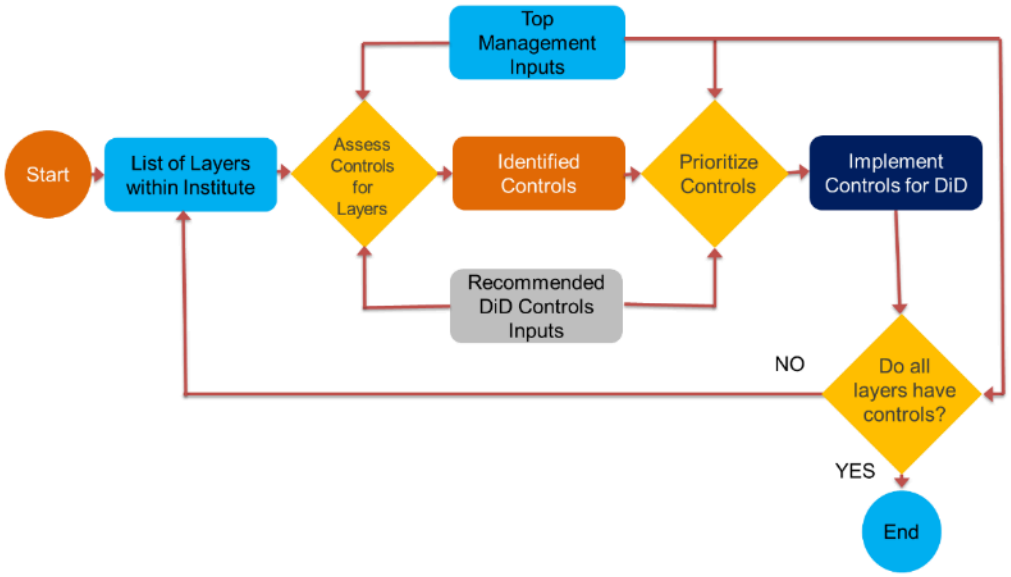

Figure 21: BDSLCCI Recommended DiD Cybersecurity Controls Implementation Flow for Education Institute

These levels are designed to be practical and cost-effective, enabling educational institutions to incrementally strengthen their cybersecurity posture without excessive resource consumption, much like Small and Medium Enterprises (SMEs). By adopting BDSLCCI, organizations can systematically enhance their cybersecurity resilience in a structured and sustainable manner [22, 24, 25, 26].

BDSLCCI Framework Mapping with GDPR and FERPA

The General Data Protection Regulation (GDPR) is a European Union (EU) law designed to protect individuals' personal data and privacy. It was enacted on May 25, 2018, and applies to any organization that processes the personal data of EU residents, regardless of where the organization is located. The BDSLCCI framework helps educational institutions comply with by implementing structured cybersecurity controls that align with data protection requirements [23].

FERPA (Family Educational Rights and Privacy Act) is a U.S. federal law designed to protect the privacy of student education records. It grants parents and eligible students (those over 18 or attending postsecondary institutions) certain rights regarding access, control, and confidentiality of their educational data. Table 1 explains mapping of BDSLCCI controls with FERPA [26, 29, 30].

TABLE 1. BDSLCCI MAPPING WITH FERPA

FERPA Requirement	BDSLCCI Framework Mapping	Control Areas

Confidentiality of Student Records	Data Security Layer, Host/Endpoint Security Layer	Encryption, access controls, secure storage solutions
Access Control & Restriction	Human Security Layer, Governance Security Layer	Role-based access, multi-factor authentication (MFA)
Data Breach Prevention & Notification	Network Security Layer, Physical Perimeter Security Layer	Intrusion detection, firewall protections, security monitoring
Integrity of Academic & Administrative Data	Application Security Layer, Governance Security Layer	Audit logs, data validation, secure backups
Availability of Student & Faculty Information Systems	Physical Perimeter Security Layer, Network Security Layer	Redundant infrastructure, disaster recovery planning
Protection Against Unauthorized Sharing of PII	Data Security Layer, Human Security Layer	Data Loss Prevention (DLP), staff training programs
Secure Management of Third-Party Vendors Handling Data	Governance Security Layer, Physical Perimeter Security Layer	Vendor risk assessment, compliance monitoring, contractual safeguards

FERPA compliance ensures that educational institutions handle student data responsibly, preventing unauthorized disclosures and maintaining data integrity. BDSLCCI recommended controls can be helpful to comply FERPA and GDPR kind of compliance needs for any education institute. The BDSLCCI framework aligns well with these compliance needs by offering structured cybersecurity controls tailored for educational settings. It helps institutions implement encryption, access controls, data monitoring, and breach response mechanisms, ensuring the protection of personally identifiable information (PII) and sensitive student records. Additionally, governance security layers within BDSLCCI assist in establishing regulatory compliance policies, ensuring institutions meet FERPA and GDPR requirements efficiently.

The number of cybersecurity controls required for implementation in educational institutions varies across different frameworks.

ISO/IEC 27001 is a globally recognized Information Security Management System (ISMS) standard designed to help organizations protect sensitive data, manage

cybersecurity risks, and ensure compliance with security best practices. Developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), it provides a structured framework for establishing, implementing, maintaining, and continuously improving information security. The latest ISO 27001:2022 revision includes 93 security controls across four categories - Organizational, People, Physical, and Technological [22, 23, 24, 25, 26].
NIST (National Institute of Standards and Technology) is a U.S. government agency responsible for developing cybersecurity standards and guidelines. It offers frameworks such as the NIST Cybersecurity Framework (CSF) and NIST Special Publications, outlining best practices for security and risk management. The NIST CSF consists of five core functions—Identify, Protect, Detect, Respond, and Recover—mapped to 23 categories and further broken down into hundreds of sub-controls. Additionally, NIST SP 800-53 defines 20 control families, each containing hundreds of individual security controls, making it one of the most comprehensive cybersecurity frameworks [22, 23, 24, 25, 26].
ISO 27001 defines 93 controls, while NIST CSF provides a flexible, risk-based approach with hundreds of sub-controls. While comprehensive, NIST's complexity can pose challenges for institutions with limited cybersecurity expertise.
In contrast, BDSLCCI offers a streamlined, education-institute-focused approach, prioritizing mission-critical assets with a stepwise, tailored list of security controls. BDSLCCI Level 1 can be achieved with approximately 20–25 controls, while Level 2 requires implementing 25–35 controls. Level 3 can be attained with around 36–45 controls. This structured model reduces implementation time and costs, focusing on essential security measures rather than an exhaustive list. Educational institutions benefit from incremental maturity growth, ensuring cybersecurity improvements align with their budgetary and operational constraints [22, 23, 24, 25, 26].
By adopting BDSLCCI, educational institutions can strengthen cybersecurity resilience, mitigate data breaches, and maintain regulatory compliance while optimizing operational security in a cost-effective manner.

6. CONCLUSION

The BDSLCCI framework provides educational institutions with a tailored, step-wise, and cost-effective approach to cybersecurity, addressing their unique challenges and resource limitations. By implementing domain-specific controls, it helps protect sensitive student data, academic records, and institutional research while ensuring compliance with regulations such as FERPA and GDPR.

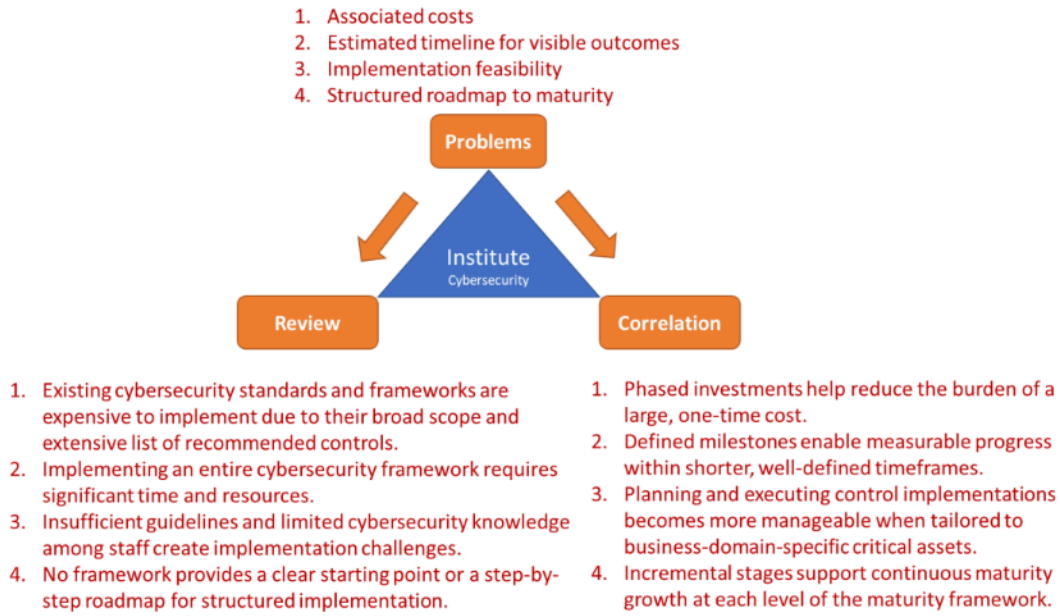

Figure 22: The Correlation of BDSLCCI in Enhancing Cybersecurity Strategies for Educational Institutions

As shown in the Figure 22, the BDSLCCI framework can significantly reduce the overall cost of cybersecurity implementation. It provides a stepwise, tailored list of controls for educational institutions, offering a more efficient and less time-consuming solution.

Additionally, it mitigates cyber risks, including data breaches, ransomware attacks, and unauthorized access to learning management systems. Its structured, stepwise methodology of BDSLCCI can help educational institutions to strengthen their cybersecurity posture without overwhelming financial and operational resources, fostering trust in digital learning environments and institutional resilience.

7. List of Abbreviations Used in Images and Graphs

The following short forms are used in this manuscript:

13-year-old student: 13-year-old Benjamin Franklin Middle School student
APT 35: Islamic Revolutionary Guard Corps (APT 35 Charming Kitten)
Carbonic: Carbonic AKA @MarxistAttorney
Coaches for the football: Coaches for the football team at Braden River
DA: Data Attack
Daniel-Alex-Erick: Daniel Soares; Alex Mosquera; Erick Vaysman
District student: Unnamed Fort Zumwalt School District student
DPRK: Korea (the Democratic People's Republic of)
EDoS: External Denial of Service
EoAS: Exploitation of Application Server
EoDiT: Exploitation of Data in Transit

EoEH: Exploitation of End Host
EoEHs: Exploitation of End Hosts
EoNI: Exploitation of Network Infrastructure
EoS: Exploitation of Sensors
Fredrick-Rath-Jimmy: Fredrick Lapointe; Rath Pak; Jimmy Saintelien
IDoS: Internal Denial of Service
IRGC: Islamic Revolutionary Guard Corps (IRGC) (Agonizing Serpents)
MIUM: Moroccan Islamic Union-Mail
MM: Message Manipulation
MMS - APT40: Ministry of State Security's (MSS) Hainan State Security Department (APT40)
MOIS: Ministry of Intelligence and Security (MOIS)
NGB: NGB 3rd Technical Surveillance Bureau
PLA Unit 61398: People's Liberation Army Strategic Support Force (PLA Unit 61398)
Sc0rp!n Att@ck3r: Sc0rp!n Att@ck3r from Muslim Cyber Army
Two School Students: Two Sherman High School students
UK: United Kingdom of Great Britain and Northern Ireland
Unit 26165 (FANCYBEAR): GRU 85th Main Special Service Center (Unit 26165) (FANCYBEAR)
USA: United States of America
Venezuela: Venezuela (Bolivarian Republic of)
Weev: Andrew "Weev" Auernheimer

Funding
This research received no external funding.
Acknowledgments
This project received no external finance.
Declaration of Interest's Statement
The author declares that there are no conflicts of interest regarding the publication of this paper.

Research Contribution
Shekhar Pawar: Conceptualization, Methodology, Software, Validation, Formal Analysis, Investigation, Resources, Data Curation, Writing - Original Draft, Visualization, Project Administration. **Atul Tripathi:** Writing - Review and Editing.

REFERENCES

1. Team, C. (2024). What is an educational institute? - California Learning Resource Network. [online] California Learning Resource Network. Available at: https://www.clrn.org/what-is-an-educational-institute/.

2. Divya, M. (2022). A STUDY ON EDUCATION SYSTEM IN INDIA. IJRTI, [online] 7(8), p.624. Available at: https://ijrti.org/papers/IJRTI2208108.pdf [Accessed 22 May 2025].
3. Leal, S., Azeiteiro, U.M. and Aleixo, A.M. (2024). Sustainable development in Portuguese higher education institutions from the faculty perspective. Journal of Cleaner Production, [online] 434, p.139863. doi:https://doi.org/10.1016/j.jclepro.2023.139863.
4. Chankseliani, M., Qoraboyev, I. & Gimranova, D. Higher education contributing to local, national, and global development: new empirical and conceptual insights. High Educ 81, 109–127 (2021). https://doi.org/10.1007/s10734-020-00565-8.
5. Kaur, M. and Kaur, H. (2022). CONTRIBUTION OF HIGHER EDUCATION INSTITUTIONS TOWARDS PROMOTING SUSTAINABLE ECONOMIC GROWTH. SCHOLARLY RESEARCH JOURNAL FOR INTERDISCIPLINARY STUDIES, 10(73), pp.17767–17772. doi:https://doi.org/10.21922/srjis.v10i73.11683
6. Vigneswari, T., Pramila, S., Gomathi, M.V. and Madhumitha, M., Enhancing Cybersecurity in Educational Institutions: Challenges and Strategies. Eureka Publications, p.32.
7. Dei, H., Shvets, D., Lytvyn, N., Sytnichenko, O. and Kobus, O., 2024. Legal Challenges and Perspectives of Cybersecurity in the System of State Governance of Educational Institutions in Ukraine. Journal of Cyber Security and Mobility, pp.963-982.
8. CBS Broadcasting Inc. (2014). Student Arrested For Allegedly Changing Grades. [online] Cbsnews.com. Available at: https://www.cbsnews.com/miami/news/student-accused-of-changing-grades-arrested/.
9. Halley, J. (2018). Florida high school caught hacking into opponents' Hudl videos. [online] USA TODAY High School Sports. Available at: https://www.usatodayhss.com/story/sports/high-school/2018/07/27/school-nicknamed-the-pirates-steals-opponents-hudl-videos/76322946007/.
10. Robinson, T. (2018). ETSU breached after phishing scam. [online] SC Media. Available at: https://www.scworld.com/news/etsu-breached-after-phishing-scam.
11. Prohaska, T.J. (2020). Malware Attack Knocks NY Community College Offline. [online] GovTech. Available at: https://www.govtech.com/security/new-york-community-college-computers-disabled-by-cyberattack.html.
12. U.S. Attorney's Office, Southern District of Texas (2020). Local man charged with making threat during university Zoom lecture. [online] Justice.gov. Available at: https://www.justice.gov/usao-sdtx/pr/local-man-charged-making-threat-during-university-zoom-lecture.

13. Greig, J. (2024). Universities in New Mexico, Oklahoma respond to ransomware attacks. [online] therecord.media. Available at: https://therecord.media/ransomware-new-mexico-highlands-east-central-oklahoma-universities.
14. Toulas, B. (2024). Kansas State University cyberattack disrupts IT network and services. [online] BleepingComputer. Available at: https://www.bleepingcomputer.com/news/security/kansas-state-university-cyberattack-disrupts-it-network-and-services/.
15. Nayak, S. (2021). Pakistani agents hack Sambalpur University website. [online] KalingaTV. Available at: https://kalingatv.com/odisha/pakistani-agents-hacks-sambalpur-university-website/.
16. TNN (2020). IIT-Madras servers under ransomware attack, email services down. [online] The Times of India. Available at: https://timesofindia.indiatimes.com/city/chennai/iit-m-servers-under-ransomware-attack-email-services-down/articleshow/74216771.cms.
17. Coker, J. (2024). Top UK Universities Recovering Following Targeted DDoS Attack. [online] Infosecurity Magazine. Available at: https://www.infosecurity-magazine.com/news/universities-recovering-ddos-attack/.
18. Mascellino, A. (2022). Anonymous Claims Attacks Against Belarus for Involvement in Russian Invasion of Ukraine. [online] Infosecurity Magazine. Available at: https://www.infosecurity-magazine.com/news/anonymous-claims-attacks-against/.
19. Toulas, B. (2023). University of Sydney data breach impacts recent applicants. [online] BleepingComputer. Available at: https://www.bleepingcomputer.com/news/security/university-of-sydney-data-breach-impacts-recent-applicants/.
20. Toulas, B. (2023). University of Sydney data breach impacts recent applicants. [online] BleepingComputer. Available at: https://www.bleepingcomputer.com/news/security/university-of-sydney-data-breach-impacts-recent-applicants/.
21. Martin, A. (2023). Cyberattack on German university takes 'entire IT infrastructure' offline. [online] Therecord.media. Available at: https://therecord.media/ransomware-attack-kaiserslautern-university-applied-sciences-germany.
22. Pawar, S., & Palivela, H. (2025). Review and Design of Business Domain-Specific Cybersecurity Controls Framework for Micro, Small, and Medium Enterprises (MSMEs). Archives of Advanced Engineering Science, 1-19. https://doi.org/10.47852/bonviewAAES52024438.
23. Pawar, S. (2025). How BDSLCCI can Help SMEs to Achieve Data Protection Compliance, Such as EU GDPR and the DPDP Act of India. International

Journal of Engineering Research & Technology, [online] 14(3). doi:https://doi.org/10.17577/IJERTV14IS030077.

24. Pawar, S.A. and Palivela, H. (2023). Importance of Least Cybersecurity Controls for Small and Medium Enterprises (SMEs) for Better Global Digitalised Economy. Contemporary Studies in Economic and Financial Analysis, [online] 110B(978-1-83753-417-3), pp.21–53. Available at: https://ideas.repec.org/h/eme/csefzz/s1569-37592023000110b002.html [Accessed 8 Mar. 2024].
25. Pawar, S. and Palivela, H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). International Journal of Information Management Data Insights, [online] 2(1), p.100080. doi:https://doi.org/10.1016/j.jjimei.2022.100080.
26. Pawar, S. and Palivela, H. (2025). NEED OF PARADIGM SHIFT IN CYBERSECURITY IMPLEMENTATION FOR SMALL AND MEDIUM ENTERPRISES (SMES). International Journal of Cybersecurity Intelligence & Cybercrime, [online] 8(1). doi:https://doi.org/10.52306/2578-3289.1184.
27. Ulven, J.B. and Wangen, G., 2021. A systematic review of cybersecurity risks in higher education. Future Internet, 13(2), p.39.
28. Alexei, L.A. and Alexei, A., 2021. Cyber security threat analysis in higher education institutions as a result of distance learning. International Journal of Scientific and Technology Research, (3), pp.128-133.
29. Radway, S., Quintanilla, K., Ludden, C. and Votipka, D., 2024, May. An Investigation of US Universities' Implementation of FERPA Student Directory Policies and Student Privacy Preferences. In Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (pp. 1-35).
30. Rainsberger, R., 2024. Consider how FERPA applies to coaches, staff accessing student-athletes' academic records. Campus Legal Advisor, 24(5), pp.4-5.
31. Toulas, B. (2023a). Israel warns of BiBi wiper attacks targeting Linux and Windows. [online] BleepingComputer. Available at: https://www.bleepingcomputer.com/news/security/israel-warns-of-bibi-wiper-attacks-targeting-linux-and-windows/.
32. Lakshmanan, R. (2022). Pakistani Hackers Targeting Indian Students in Latest Malware Campaign. [online] The Hacker News. Available at: https://thehackernews.com/2022/07/pakistani-hackers-targeting-indian.html.
33. Greig, J. (2023). Chinese-language threat group targeted a dozen South Korean institutions. [online] Therecord.media. Available at: https://therecord.media/chinese-language-threat-group-targeted-south-korea.
34. Tidy, J. (2020). How hackers extorted $1.14m from a US university. BBC News. [online] 29 Jun. Available at: https://www.bbc.com/news/technology-53214783.

35. University of Utah Communications (2020). University of Utah update on data security incident | @theU. [online] attheu.utah.edu. Available at: https://attheu.utah.edu/facultystaff/university-of-utah-update-on-data-security-incident/.
36. Craigslord (2021). Ottawa french public school board paid hackers ransom after data breach. [online] Global News. Available at: https://globalnews.ca/news/8413098/ottawa-french-school-board-data-breach/.
37. DataBreaches.net (2021). Update on Union Community School District ransomware incident – DataBreaches.net. [online] Databreaches.net. Available at: https://databreaches.net/2021/06/12/update-on-union-community-school-district-ransomware-incident/.
38. Vachheta, H., Pawar, I., Hukare, K. and Jadhav, S. (2024). Cybersecurity in the Digital Era: A Comprehensive Framework for Safeguarding Data Integrity, Privacy and Critical Infrastructures Against Evolving Threats. International Journal of Advanced Research in Science, Communication and Technology (IJARSCT) International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal, [online] 4(1), pp.2581–9429. Available at: https://www.ijarsct.co.in/Paper22665.pdf.
39. Alhalafi, N. and Veeraraghavan, P. (2023). Exploring the Challenges and Issues in Adopting Cybersecurity in Saudi Smart Cities: Conceptualization of the Cybersecurity-Based UTAUT Model. Smart Cities, [online] 6(3), pp.1523–1544. doi:https://doi.org/10.3390/smartcities6030072.
40. Md. Alimul Haque, Ahmad, S., John, A., Mishra, K., Binay Kumar Mishra, Kumar, K. and Nazeer, J. (2023). Cybersecurity in Universities: An Evaluation Model. SN computer science, 4(5). doi:https://doi.org/10.1007/s42979-023-01984-x.