IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Need of Cyber Security in Higher Education in Present Era

Md. Sadre Alam
Assistant Professor
Department Of Education;
Gaya College, Gaya (Magadh University, Bihar).

Abstract

Cyber security needs to be a priority for the Education Sector. Education institutions need to make cyber security a priority. Despite the sector facing major challenges such as a lack of staffing and a lack of funding and resources, cyber attacks are no less frequent or less severe in education. In fact, they seem to be gaining ground in prevalence year-on-year as instances of breaches in schools and higher education are widely reported. In recent years we've seen news of ransom attacks causing financial damage like that on the University of Calgary where the institution allegedly handed over $20k to cybercriminals, and malware attacks causing mass disruption similar to the disruption which caused the Minnesota School District to shut down for a day while IT professionals rebuilt the system. The more worrying breaches are where student safety is compromised. Educational institutions are entrusted to safeguard their students, many of whom are minors, but a weak cyber security infrastructure can put them at risk. This was made all too clear when the CCTV in several schools in Blackpoll was allegedly breached, and the footage was reportedly live-streamed on the internet. It's an unfortunate fact that, while cyber security in Education is necessary to protect against financial loss and prevent disruption, it's also crucial to protect students from harm. This is why the sector needs to do everything it can to ensure their applications and systems are protected, and work to overcome any challenges.

In this article, we'll look at the current state of cyber security in Education. We'll discuss the most common reasons for the attack, the highest threats, and the main challenges facing the sector to help you understand why cyber security needs to be a priority, and how you can make it a priority for your educational institute. Cyber security is a concern for all modern organizations. These organizations cannot achieve their cyber security goals through hardware and information technology (IT) workers alone, so all employees who use computer networks must be trained on the knowledge, skills, and policies related to cyber security. This paper reviews what is known about effective cyber security training for end-users of computer systems. The fact that the Internet has positively impacted people's lives, there are negative issues that are emerging related to the use of the Internet. Cases like cyber bullying, online fraud, racial abuse, pornography, and gambling had increased tremendously due to the lack of awareness and self-mechanism among Internet users to protect themselves from being victims of these acts. Young children specifically, need to be educated to operate safely in cyberspace and to protect themselves in the process. As our nation rapidly builds it's. Cyber-Infrastructure, it is equally important that we educate our population and children to work properly with this infrastructure. Cyber-Ethics, Cyber-Safety, and Cyber-Security issues need to be integrated into the educational process beginning at an early age. The valuable aspects of cyber-security are technology, operations, awareness, training, and education. This paper focuses on issues related to cyber security in India and presents various methods in bringing awareness in the educational system. The objective of this systematic review paper is to explore why it is so critical that modern learners are educated about the risks associated with being active in cyberspace and the strategies that stakeholders can use to promote cyber security education in schools. In this paper, we have discussed the importance of cyber security in the education Sector.

Keywords:-Cyber security, cyber safety, cyber education, cyber awareness, cyber-infrastructure, social-networking, cyber-ethics.

Introduction

The ability to securely connect to virtual systems is an important element within a safe and supportive learning environment. This is particularly the case within institutions of higher education (IHEs), where students are increasingly learning in digital formats; faculty, staff, and visitors are constantly accessing and sharing information online; and more infrastructure and facility functions are being managed online. To maintain their collaborative culture, colleges and universities house robust information technology (IT) networks and multi-layered infrastructure systems with varying levels of access and connectivity. Unfortunately, this open environment has made IHEs around the world targets in 2017 cyber-attacks. Social media is being used as a medium of expressing feelings and provoking discussions and to get some attention or to come into the limelight. People are not paying attention to things such as whether data is authentic and secure or not. Because of this, data becomes more vulnerable. Moreover, the use of the internet is not limited to adults only Nowadays everyone is using the internet. Also corona. Pandemic has changed the whole picture. Classrooms are now online, and students are learning online. In this era of technology and multimedia, knowledge of cyber security is also important for children. Although Internet has vast potential and benefits for everybody, the excessive use of the Internet may be harmful as it may lead to cyber risks for example sextortion, cyber addiction, gaming and gambling addiction, cybersex pornography, and personal information exposure.

Cybercrime against children and adolescents is certainly a concern for parents, as they sometimes do not realize their child is a victim of cybercrime. Many parents are unaware of the activities their children perform in cyberspace. Some children are bullied through comments and insults; they may also be intimidated, harassed, abused, or sexually exploited. Grooming children and adolescents to become victims of sexual abuse is worsening, as more and more of these sexual predators are using fake identities on the internet when seeking victims. The objective of cyber security education is to educate the users of technology on the potential risks they face when using internet communication tools, such as GY 200 social media, chat, online gaming, email, and instant messaging. Although there is much past research conducted on cyber security, in different areas, fewer articles focused on the steps that need to be done particularly by schools to help cultivate cyber security awareness in detail. The objective of this paper is to discuss why it is so critical that modern learners are educated about the risks associated with being active in cyberspace, what factors hamper this education, and the importance of a cyber security curriculum that can be used by teachers in junior or primary schools, in the specific context of the Indian education system.

Cyber Security

Cyber security is the practice of protecting critical systems and sensitive information from digital attacks. Also known as information technology (IT) security, Cyber security measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization. In 2020, the average cost of a data breach was USD 3.86 million in the United States. These costs include the expenses of discovering and responding to the breach, the cost of downtime and lost revenue, and the long-term reputational damage to a business and its brand. Cybercriminals target customers' personally identifiable information (PII) - names, addresses, national identification numbers (e.g., Social Security numbers in the U.S., fiscal codes in Italy), and credit card information - and then sell these records in underground digital marketplaces. Compromised PII often leads to a loss of customer trust, regulatory fines, and even legal action. Security system complexity, created by disparate technologies and a lack of in-house expertise, can amplify these costs. But organizations with a comprehensive cyber security strategy, governed by best practices and automated using advanced analytics, artificial intelligence (AI), and machine learning, can fight cyber threats more effectively and reduce the lifecycle and impact of breaches when they occur.

The emergence of the internet allows humans to enjoy two realms: their real life, and the virtual world. With search engines such as Google and Yahoo and video sharing sites such as YouTube, all information is now available at people's fingertips. However, the growing world of cyberspace may also have negative effects on internet users, such as through cybercrime. Such issues should therefore be contained early so they do not have a major impact. In this context, cyber security implementation among internet users is very important. Cyber security education is necessary because cybercrime cases can occur anywhere regardless of individuals, organizations, and places. The definition of cyber security is the state of being protected against the criminal or unauthorized use of Electronic data or the measures taken to achieve this. The explosion of Information Communication Technology (ICT) has brought great changes to our lives. With the existence of the World Wide Web, individuals and organizations can easily display any information, but if this is used for damaging purposes it will hurt people's lives. In addition, the internet makes pornography accessible, which can generate social problems, including crime.

The internet can also be an unhealthy channel for crimes and misbehavior, being the main cause of Malay teenagers truanting from school. Cyber security can also be defined as the activity, process, ability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. The internet undoubtedly increases one's knowledge. For example, online computer games require users who are highly skilled in English, to understand game settings and procedures. This will indirectly encourage the development of reading, writing, and speaking skills in English. However, a computer game will usually be fun, and take the user a long time to complete. This can cause teens to become lazy, or to concentrate on game play and gadgets. Adolescents can also become addicted, and productive activities, such as reviewing their lessons, are ignored.

Need for Cyber Security Education

The COVID-19 pandemic has had a profound impact on education, bringing about a sudden boom in remote and online learning. While the transition has forced many schools to implement innovative solutions, it has also revealed stark vulnerabilities in their cyber security strategies, which is especially concerning given that schools have become the new target for attackers. A big problem is that even before the pandemic, cyber security hasn't been a priority in education. A lack of funding and skilled personnel has meant that schools have basic system set-up errors or leave old issues unlatched. Now, in the mass digital movement, these gaps can be even more damaging, and schools are quickly realizing that they need the knowledge and updated technological infrastructure to continue virtual learning securely in the long term. Children's use of the internet is changing fast, in response to considerable societal, market, and technological innovation. As children's frequent engagement with online videos, music, and gaming, messaging and searching implies, their internet use is broadly positive. Parents of three- to four-year-olds report that their child is likely to watch cartoons, mini-movies, animations, or songs on YouTube. The content children watch as they grow older differs, as older children watch more music videos, vloggers, YouTube personalities, and funny videos. The role of schools is important in teaching critical digital literacy to students, as well as in guiding and informing parents regarding children’s internet use at home.

Types of cyber attacks

In the education system, the children must be made aware of the possible attacks and types of intruders. They should know about the frauds and scams like phishing, cyber theft, and their historic records. They must know about the types of malicious software, their preventive measures, etc. The curriculum must also include the advanced concepts like the safe use of social networking and mobile devices using
GPRS. They must also be aware of the terms like:-

1) Hardware/Desktop Security
2) Wi-Fi security, wired security
3) Password Protection/ (File/Folder)level security
4) Malicious software: • Phishing, Hoaxes • Shareware, Malware, Virus, Worm, • Trojans, Zombie and Botnet, Spyware, Adware,
5) Social networking

Attacks security Students are acquiring information technology skills marks question on the educators' abilities to ensure that positive habits of on-line behaviors are being formed. Whereas the teacher giving information about security lacks the knowledge and up-to-date information related to Cyber awareness issues, particularly concerning security. Teacher technology training must be provided for skills development and awareness. A new kind of emerging cybercrime is the Hacktivists. The current record shows the least awareness of cyber-crimes at all levels in India. There is an urgent need for introducing courses in various fields. The Department of National Security defines cyber security as, "preventing, detecting, and responding to attacks." Indian Education system needs cyber security awareness programs with the increasing use of Indian users in social networking and mobile devices.

Challenges and Issues for cyber security education

Among the biggest cyber challenges facing the education sector is an increased number of cyber attacks that aim to steal personal information, extort data for money, or disrupt schools' ability to operate. Recently, schools have been regularly targeted with the following three types of cyber attacks to achieve these goals. Cyber security education is an important and pertinent topic as it plays a major role in mitigating the risks caused by a global shortage of cyber security experts. To better support, this crucial function, a cyber security skills framework needs to be agreed upon by academics in this field, along with an increase in the visibility of cyber security education and training. Without these, there is likely to be a long-term shortfall between the number of skilled cyber security professionals and demand, potentially leaving organizations, institutions, and governments are vulnerable.

Education System

1) No separate lesson plans for cyber security awareness.

2) Teachers are not aware of the current threats in information technology. Teachers may face problems in developing their knowledge of the latest technology and thus ensuring students are safe.

3) People are not aware of the reason for the educational course and so do not make any effort to understand or learn the course.

4) It is related to the subject matter and non-interactive learning system.

5) People tend to forget what they learned about information security if there is no practical implementation.

6) The training and education programs don't consider the present knowledge and experience of their target audience and the problem of "One-size-fits-all" appear.

7) The course material is usually not presented memorably and therefore makes no impression.

8) The complete and comprehensive education of the users in cyber security involves a continuum of three levels of education.

Measures to be taken to ensure Cyber security

1) Use an Internet Security Suite
2) Install a firewall
3) Use Strong Passwords
4) Keep Your Software Up-to-Date
5) Take appropriate actions if you have been a Victim.
6) Learning safe chatting and messaging skills.
7) Installing and updating anti-virus software and regularly downloading security protection updates.
8) Preventing stranger access to private computer files
9) Individual awareness about all the laws and rights before using any new software.

10) Government must participate in funding cyber education and create strong partnerships with local, state, and regional governments, industry, and educational institutions.

11. Government should provide proper laws for cyber-crime and prosecute people who steal digital property or harm others online.

Cyber security in higher education is becoming an urgent focus area for college and university directors, administrators, and boards. Higher education institutions are facing cyber security incidents and breaches at an increasing frequency, and the nature of these attacks are varying significantly in sophistication, objective, and scope. At the end of March, the U.S. Department of Justice and the U.S. Department of the Treasury announced law enforcement efforts in response to Iranian state-sponsored cyber-attacks on hundreds of universities around the globe, including more than 100 U.S.-based institutions. In January, a successful spear-phishing attack at the University of Hawaii made the news; it resulted in a data breach impacting approximately 2,400 faculty, staff, students, and student applicants. Last summer, computer equipment theft at Washington State University resulted in the loss of personally identifiable information (PII) and protected health information (PHI) for approximately one million individuals. These are just some of the most recent publicly disclosed examples, and they underscore the broad spectrum of cyber security risk in higher education institutions.

A "checklist" of cyber security best practices for higher education institutions or a "one-size fits all" approach will not suffice and does not exist. Each institution will have unique data elements, technology footprints, processes, risks, and other attributes which need to be considered to develop an accurate portrait of the school's cyber risk.

In addition to the significant uptick in threat activity, there has also been a proliferation of cyber security and data protection regulations with which higher education institutions may need to comply, depending on the nature of each institution's unique profile, including their academic and research activities. Organizations in the sector should evaluate how their operations are relevant to the Health Insurance Portability and Accountability Act (HIPAA) Security Rule; the protection of student data under Family Education Rights and Privacy Act (FERPA) regulations; the protection requirements of the U.S. Federal Controlled Unclassified Information (CUI) as outlined under the National Institute of Standards and Technology (NIST) Special Publication 800-171 relevant to government information or contractors; and Payment Card Information Data Security Standard (PCI-DSS) requirements, among others.

The First Step:-
Cyber Security Risk Assessment

To manage these cyber security threats, risks, and compliance challenges, each institution should start by conducting a thorough assessment and analysis of its current cyber security environment and posture, with a focus on understanding underlying drivers of cyber risk, what information they create and store is the most valuable, key threats, other risk considerations, and the regulatory and compliance landscape. This must be done with a holistic approach, acknowledging all dimensions of cyber security. Academic environments are rich with sensitive information, often including student records and other personally identifiable information, financial aid and/or transaction data, and healthcare information as well as data related to cutting-edge, specialized research. Institutions may find themselves squarely in the crosshairs of malicious actors simply by being a potential source of this type of information. A "checklist" of cyber security best practices for higher education institutions or a "one-size fits all" approach will not suffice and does not exist. Each institution will have unique data elements, technology footprints, processes, risks, and other attributes which need to be considered to develop an accurate portrait of the school's cyber risk.

The Second Step:-
Planning an Evidence-Driven Risk Mitigation Plan

Once an independent and objective view of the institution's current cyber security position is established, and the greatest risks identified, then each institution can move on to the second stage: thoughtfully planning a risk-prioritized approach to achieving its cyber security governance, risk mitigation, and compliance objectives. Much

higher education institutions have highly decentralized information technology and/or security functions, which can make governance and control difficult. Adding to the cyber security in higher education challenge is the culture of open sharing of information and data that is commonly pervasive across institutions like these. Implementing strong cyber security controls can often pose a significant change management challenge in these conditions but it is a necessity, and it cannot be done without the critical first step of understanding the institution's unique compilation of risks. Use your biggest risks as a guide to help you design and adopt strong controls despite the many challenges present in an educational setting.

The Third Step:-
Implementation and Continuous Improvement

After these first two steps, it's time to act. Implement reasonable but effective policies, standards, controls, tools, processes, and technologies. Leverage experienced internal and external cyber security resources when necessary to ensure technical solutions are configured properly and governance co-related protocols are structured effectively. But even when you reach this point, the work isn't done. Plans and strategies should be periodically reviewed and adjusted to keep up with the ever-changing cyber risk and compliance landscape. These steps can enable a holistic transformation of an institution's cyber security program. Higher education and research institutions are facing significant and increasing information security challenges and must act quickly. Threat actors won't wait to attack while an organization figures out how to defend itself. The data protection regulations with which many of these organizations must comply are proliferating and being enforced without pause. While it's tempting for anyone under these kinds of pressures to jump to tools and solutions, the first step especially for financially careful colleges and universities starts with the fundamentals. Identify the key risks, threats, and compliance drivers.

Evaluate current capabilities versus target objectives. Strategize and plan for enhancement. Then implement and iterate. Building a culture of cyber security awareness requires a process for continuous improvement, because only with consistent effort can institutions stay a step ahead. Cyber security in education is a topic that has been raised in profile over the last few years. This is partly because of the increasing number of attacks that are targeting organizations in general, particularly during the onset of the corona virus pandemic. It’s also because education organizations and institutions have often been slow to react to an increasingly dangerous security landscape, leading many to become prime targets and victims of cyber attacks. To combat these organizations should start taking cyber security in education more seriously and assess whether their current strategy is enough to defend themselves against modern threats. Take a look at these stats for an indication of where the sector is and the necessity for institutions to take more effective action.

Why Education is a target for cybercrime

Education is a target for cyber criminals with Education venues varying in size, purpose, and stature, the motives for attack can vary too. For example, what might be a common threat for world-renowned Universities/Colleges might not be an issue for schools or school districts? So, institutions need to evaluate the risk and understand what data is vulnerable to unauthorized access.

DDoS attacks Distributed Denial of Service or DDoS attacks are a common type of attack on all levels of Education venues. This is where the attacker's motive is to cause widespread disruption to the institute's network, harming productivity.

This can be a relatively easy attack for amateur cyber criminals to carry out, especially if the target network is poorly protected. There have been instances of students or teachers successfully carrying out a DDoS attack, with motives ranging from simply wanting a day off, to protesting the way a complaint was handled.

Data theft – This is another attack affecting all levels of education because all institutions hold student and staff data, including sensitive details like names and addresses. This type of information can be valuable to cybercriminals for several reasons, whether they plan to sell the information to a third party or use it as a bargaining tool and extort money.

The concerning aspect of this type of attack is that hackers can go unnoticed for long periods. As was the case at Berkeley, where at least 160,000 medical records were allegedly stolen from University computers over several months.

Financial gain – Another motive for hackers attacking an educational institution is for financial gain. This might not be as high risk for public schools, but with private institutions and Universities/Colleges handling a large number of student fees, they're a prime target for cybercriminals.

Today, it's usual for students or parents to pay fees via an online portal, often transferring large sums of money to cover a whole term or year of tuition. Without proper protection or preparation on the part of education institutions, this presents a weak spot for cybercriminals to intercept.

Espionage – The fourth reason why education is a target for cybercrime is espionage. In the case of higher education institutes like Universities/Colleges, they're often centers for research and hold valuable intellectual property.

Universities/Colleges need to be suitably protected, as it's thought that science, engineering, and medical research by UK Universities have been previously compromised by hackers, and with plenty of time and money to fund them, professionals are often at the helm of these attacks. With these four motives in mind, how hackers attack Education networks can further help us understand how to protect them.

Hackers attacking Education networks can further help us understand how to protect them. Children at school in an ICT lesson using school computer show Education is targeted JISC's 2018 Cyber security Posture Survey questioned IT professionals within further and higher education. They were asked to name the top cyber threats facing their institutions, and the top three answers give us insight into the most common ways Education networks are breached.

Phishing – Phishing scams often take the form of an email or instant message and are designed to trick the user into trusting the source in a fraudulent attempt to access their credentials – whether that's sensitive student data or confidential research.

This type of attack is highlighted as the top threat facing higher education venues, suggesting hackers regularly target the sector using the method.

Ransomware/Malware – Also in the top three cyber threats highlighted by the report, Ransomware and malware attacks prevent users from accessing the network or files and cause disruption. More advanced forms of this threat can see attackers hold files to ransom.Ransomware or malware typically infects devices using a Trojan, a file, or an attachment disguised to look legitimate. However, some ransomware (like the WannaCry attack) has been shown to travel between devices without user interaction.

Lack of awareness – The third threat listed by professionals in both further and higher education is a lack of awareness or accidents. This could be on the part of staff or students who aren't sufficiently trained to practice good cyber hygiene or accidentally compromise the network.

Despite taking on different appearances, human error plays a key part in each of these three Education sector cyber security threats. However, with better overall cyber security training, and awareness of the motives and methods of attackers, education venues could better protect themselves against cyber attacks.

However, the sector is also facing challenges that hinder progress.The challenges Education is facing. The JISC report also investigates the challenges facing IT professionals when it comes to protecting Education networks. When asked to rate how well their institution is protected on a scale from 1 (not at all) to 10 (very well), further education scored lower overall than higher education. The mean score for further education institutions was 5.9, while higher education scored 7.1.

The rationale behind lower scores included:

A lack of resources and budget – potentially pointing to the lack of finances to invest in cyber security, be it software or staff.

Cultural issues – a 'Bring Your Own Device' culture is common in Educational institutions and can present difficulties in securing the wider network, particularly with IT staff already facing stretched resources.

An absence of policy – setting out policies for using the network and making sure they're adhered to can be difficult in large institutions with a dynamic user population.
Despite these challenges, the Education sector is still expected to secure its networks against unauthorized access and cyber threats. Especially when the repercussions can be as severe as the examples we discussed earlier. But there are some critical steps every institution should undertake to lay the foundations for a secure IT network.

Conclusion

Based on a synthesis of the literature selected, The IT industry has been playing catch-up with hackers and cybercriminals for decades. Thus there is a need for a cyber-security curriculum shortly which will in-build the cyber-security understanding in the current youth and finally, the IT sector will get more profound, securely skilled professionals it was found that it is very important to protect children through cyber security education so that they can become aware of the potential risks they face when using internet communication tools, such as social media, chatting, and online gaming. However, there are several challenges to cyber security education. These include the level of teachers' knowledge, and the lack of expertise, funding, and resources. It is very important for all relevant parties, including teachers, parents, peers, and the government, to work together to find the best solution to protecting children from Cyber crime and cyber bullying through school-based cyber security education. The media, such as television and radio, must also play an important role in educating children through cyber security campaigns because such campaigns are more interactive and interesting for children to understand. Hence Effective cyber-security policies best practices must be planned and most important must be implemented at all levels. In the future, the Government's role and education systems' participation in the cyber security awareness approach will lead to a strongly secured nation.

References list

1) F. Khalid, Understanding university students' use of Facebook for collaborative learning,‖ International Journal of Information and Education Technology, vol. 7, no. 8, pp. 595-600, August 2017.

2) F. Annasingh and T. Veli, An investigation into risks awareness and e-safety needs of children on the internet, ‖ Interactive Technology and Smart Education, vol. 13, no. 2, pp. 147-165, 2016.

3) L. Muniandy and B. Muniandy, The impact of social media in social and political aspects in Malaysia: An overview, ‖ International Journal of Humanities and Social Science, vol. 3, no. 11, pp. 71-76, 2013.

4) V. Ratten, A cross-cultural comparison of online behavioral advertising knowledge, online privacy concerns and social networking using the technology acceptance model and social cognitive
theory, ‖ Journal of Science & Technology Policy Management, vol. 6, no. 1, pp. 2536,2015.

5) M. D. Griffiths and D. Kuss, Online addictions, gambling, video gaming and social networking, ‖.The Handbook of the Psychology of Communication Technology, Chichester: John Wiley, pp. 384-406, 2015.

6) L. Mosalanejas, A. Dehghani, and K.
Abdollahi Fard, The student's experiences of ethics in online systems: A phenomenological study,‖ Turkish Online Journal of Distance Education, vol. 15, no. 4, pp. 205-216, 2014.

7) D. Krotidou, Neokleous, and A. Zachariadou Exploring parents' and children's awareness on internet threats about internet safety, ‖ Campus-Wide Information Systems, vol. 29, no. 3, pp. 133-143, 2012.

8) N. Ahmad, U. A. Mokhtar, Z. Hood et al.,
Cyber security situational awareness among parents, ‖ presented at the Cyber Resilience Conference, Putrajaya Malaysia, pp. 7-8, November 13-15, 2019.

[9] Monika D. Rokade, Yogesh Kumar Sharma Identification of Malicious Activity for network packets using deep learning. International Journal of Advanced Science and technology.