ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 12, Issue 2, pp: (51-61), Month: April - June 2024, Available at: www.researchpublish.com

Cybersecurity In Education

Jumanah Hasan AlSanad

The Public Authority for Applied Education and training (PAEET), Kuwait

DOI: https://doi.org/10.5281/zenodo.12566761

Published Date: 27-June-2024

Abstract: **In this research, we presented an explanation of the definition of cybersecurity, its importance, and its types. We also explained the difference between information security and cybersecurity, as well as the importance of both. we also mentioned how cyber security is important in the education sector and the Role of training and education in enhancing Cybersecurity.**

Keywords: **cybersecurity, information security, education sector.**

1. INTRODUCTION

The world today is experiencing a great scientific renaissance and progress in the field of communication and Information Technology, in a way that scientific and technical development has become a measure of international competition towards comprehensive development. This rapid and successive renaissance in the technical field has been accompanied by a global trend towards e-learning, believing in its importance and to utilize of its advantages and various interactive applications in the field of education and the knowledge industry, as well as to achieve the goals of the educational system, meet the learner's personal needs, and qualify the learner to deal with the changes of modern life.

One of the most prominent manifestations of self-learning during the nineties and the beginning of the millennium was the learning of electronic hacks and unstructured attacks carried out by some individuals for the purpose of experience and passion, which showed the importance of codifying these practices and benefiting from these skills, capabilities and human resources in a manner that does not contradict electronic and public ethics...

With the development of Technology, Communications and modern information networks, an integrated system of Sensitive Needs has been formed to preserve the property of technologically and communication-related countries, which has made the qualification of specialists in the field of Information Security an imperative necessity adopted by universities, colleges and specialized institutes. In the era of digital technology, educational institutions must pay great attention to cybersecurity as an essential part of their mission by taking effective preventive and educational measures. A safe and protected educational environment can be provided to everyone within the educational system.

In this research, we will highlight cybersecurity in general and its relation to education as the latest field of technical learning and education.

Cybersecurity is a fundamental challenge in today's networked and digital age, where the threats facing individuals and organizations alike are multiple. It is about protecting electronic data and systems from hackings, espionage and electronic fraud, which necessitates the adoption of modern strategies and technologies for defense and prevention. In this introduction, we will take an overview of the challenges and the importance of cybersecurity in the age of modern technology and how to address these challenges effectively and efficiently. At the beginning, the concept of cybersecurity should be recognized as a relatively recent concept and is there a difference between it and the concept of Information Security.

2. SUBJECT

The definition of cybersecurity

Cybersecurity can be defined as defending computers, servers, mobile devices, electronic systems, networks and data from malicious attacks ranging from business organizations to personal devices. These attacks are divided into several categories, including network security, application and information security, operational security, disaster recovery, and business continuity.

Both network security and application security focus on securing computer networks along with software and hardware that are free from threats and vulnerabilities, respectively, while disaster recovery is related to the organization's reaction in the event of data loss and trying to restore its operational capabilities to continue the organization's work. In addition, there are several types of attacks that are known to a certain extent that can be divided into categories, which are: cybercrime aimed at financial gains, cyber-attacks that are mostly political, and cyber terrorism.

These attacks are organized using various means, including malware that includes viruses and Trojans, spyware, ransomware, adware, botnets, SQL injection, phishing, etc. The National Institute of standards and technology (NIST) defined cybersecurity as protection, damage prevention and restoration of electronic communication services and systems, including information stored in these systems. In addition to, cybersecurity covers everything related to electronic systems, communications, cloud services, networks, and critical infrastructure security.

The definition of Information Security

Most people want their personal information to be secure so that only authorized persons can access and use it, and this is the goal of Information Security (Infosec).

According to the National Institute of standards and technology (NIST), information and communication technology includes the protection of information and its systems from unauthorized use; as this field aims to provide availability, integrity and confidentiality. One of the ways to understand information and communication technology compared to cybersecurity in looking at the field as a comprehensive term that includes all data, not just data stored within cyberspace; which highlights how cybersecurity is one of the types of information security, but they are not identical. While information security teams work to create and implement information protection policies and systems, for large organizations strict security systems are required to protect customers.

Information security can be simplistically described as preventing unauthorized access or alteration while data is stored or transferred from one device to another. This information may be biometrics, social media profile, data on mobile phones, etc.; so it covers research on information security in various sectors including cryptocurrencies and cyber forensics.

Information security is created to cover three objectives; they are Confidentiality, Integrity and Availability or what is known as "CIA"; the confidentiality of data must be maintained, including: personal information and high-value information, and it is important to prevent any unauthorized access.

Moving on to integration, the stored data must be kept in the correct order; therefore, any unorganized modification by an unauthorized person must be canceled directly, but authorized personnel must be able to access the stored data at any time. To ensure the effective operation of information security, organizations have put in place several policies such as access control policy and password policy, along with data support and operational plans. Procedures can also include logos, network intrusion detection systems, and regulatory compliance.

Overlaps between information security and cybersecurity:

Information security and cybersecurity overlap in many ways, in addition to having similar security practices, and both require similar education and skills.

1. **Common security practices**

The most important overlap between information security and cybersecurity is that they use a three-pronged model “CIA” for developing security policies that include confidentiality, integrity, and availability of information.

2. **Confidentiality of the information:**

This ensures that only authorized users can access and modify information. From a consumer perspective, for example, we expect online retailers to store and protect our data such as credit card information, home addresses, and other personal information.

3. **Integrity of the information:**

The integrity of the information ensures that it has not been tampered with and is completely reliable; If we return to the example of the online retailer, the data transferred between the retailer and the bank he is dealing with must be secure, and if this does not happen, there will be a discrepancy between the actual cost of your goods and the amount you paid.

4. Availability of information:

Information availability means that data is available when you need it; For example, if you want to know how much money is in your bank account, you must be able to access that information.

The difference between information security and cybersecurity:

Both the terms cybersecurity and information security are related to the security of computer systems, and most of the time they are used synonymously, but they should not be interchangeable. The difference between information security and cybersecurity can be summarized in the following points:

Information Security	**Cybersecurity**
Information security aims to establish and maintain systems and policies and protect data from all forms of threats of any kind: analog, digital, physical and not just data.	Cybersecurity aims to protect attacks in cyberspace such as data, storage sources, devices, etc.
While information security deals with unauthorized access, modification, detection and disruption.	Cybersecurity deals with cybercrime, cyber fraud, and law enforcement.
Information security lays the foundation for data security and trains them to prioritize resources before dealing with threats or attacks.	Cybersecurity professionals who are specially trained handle advanced Persistent Threats (APT).
Cybersecurity focuses on protecting information from cyber-attacks such as ransom ware and spyware	The information security expert develops means of access to data for authorized individuals and develops security measures to maintain the integrity of the information

In this regard, many government agencies and private sector organizations in the State of Kuwait have activated some initiatives aimed at protecting the national infrastructure, data and assets, formulating information security policies and rules, and providing means of protection against any potential risks from cyberspace. It has also been enacted Laws and legislation related to cybercrime to cover many of the activities of cybercriminals and hackers. Although, there is still an urgent need to govern these initiatives, manage the activities associated with them, and ensure the existence of an integrated, comprehensive, and flexible methodology to manage national cybersecurity. This requires a national strategy that integrates these efforts and initiatives and ensures that all cybersecurity risks are addressed, whether within organizations or through Internet ports that connect the State of Kuwait to the outside world.

The National Cybersecurity Strategy for the State of Kuwait is a response to the State of Kuwait's Government realisation of the challenges and threats magnitude resulting from cybersecurity risks, affecting the state, institutions and individuals as a whole, and to draw a roadmap towards enhancing information security in all its forms to ensure that all capabilities are harnessed, and all measures are taken.

The great interest in the field of cybersecurity has led to rapid and strong movements in the educational field at high levels. Specialized government and private colleges have been established in this field and some cyber units have emerged in a group of universities. In addition to many agreements between the Ministry of Education and the competent authorities. There are future plans to train and qualify male and female students on software from the foundational level to the level of expertise and progress. Accredited courses and many voluntary initiatives have been launched for training and qualification in the field of cybersecurity...

The most important types of cybersecurity:

Cybersecurity aims to defend computers, as well as networks, servers, and devices from any attempt at sabotage. There are many types of cybersecurity, the most important of which are the following:

1. Application Security

Application security aims to keep electronic programs and devices away from threats and hacks, as it ensures that the hacker does not have access to protected data. It is mentioned that application security is one of the security stages that are created at the program or device design stage.

2. Cloud Security

It is one of the means used to protect information and personal data stored on the Internet in what is known as the cloud through some online programs such as Google Drive, Microsoft OneDrive, and Apple iCloud. All of which are highly efficient and capable storage media.

3. Operational Security

This type of security reviews the various permissions that users have to access the network and determines where and when data is stored or shared with others.

4. Network Security

It aims to protect the computer network from any attack that tries to penetrate it, whether these attacks are from inside or outside this network. This type of security uses many modern technologies and protocols that help it complete this task.

5. Disaster Recovery and Business Continuity

Disaster recovery refers to how the organization responds to any hacking incident that causes the loss of some data, or stored processes. This process is exemplified by this institution's restoration of its operational capacity in the way it was before the hacking to ensure continuity of work with the highest capacity and efficiency.

As explained above, the concept of cybersecurity shows the need to protect the infrastructure and assets of Kuwait's vital resources and to regulate communications and exchange information to ensure that they do not carry any threats or are not used to the detriment of the interests of the State and institutions.

In this connection, several government agencies and private sector institutions in Kuwait have activated some initiatives aimed at protecting national infrastructure, data and assets, formulating information security policies and rules and providing protection against any potential risks from cyberspace, Laws and legislation related to cybercrime have also been legislated to cover many of the activities of cybersecurity criminals and hackers. There is still an urgent need for the governance of these initiatives and the management of related activities, and to ensure that there is an integrated, comprehensive and flexible methodology for managing national cybersecurity, which requires a national strategy that integrates efforts and initiatives and ensures that all Internet ports are addressed to the outside world.

Kuwait's National Cybersecurity Strategy is a response to the Government of Kuwait's awareness of the magnitude of threats and challenges resulting by cybersecurity risks affecting the State and its institutions and individuals as a whole and to map the road map towards enhancing information security in all its forms to ensure that all possibilities are harnessed, and all necessary measures taken.

Kuwait's national cybersecurity strategy:

First objective :Promoting a culture of cybersecurity that supports the safe and correct use of cyberspace:

Promoting national awareness of cybersecurity for all segments of society by publicizing the risks associated with the use of cyberspace and encouraging the use, means, security solutions and protection.

Work with the Ministries of Education and Higher Education and its affiliated institutions to develop academic and educational curricula related to cybersecurity.

Working with the private sector with Internet service providers and telecommunications companies to improve the level of cybersecurity and ensure the protection of circulating data by promoting awareness of threats to cybersecurity and encouraging the availability of best practices and the application of best protection systems.

Second objective: Protection and control of assets, critical infrastructure, national information and information network in Kuwait:

Establishment of the National Cybersecurity Centre.

Establishment of cybersecurity operations centers in critical sectors in Kuwait.

Development of the National cadres in cybersecurity fields such as combating cybercrime.

Developing national bases and standards for information security technology.

Developing national bases and standards for information security technology.

Developing national cadres in the field of combating cybercrime and in accordance with international standards.

Develop a business continuity and response plan to manage national cybersecurity events and crises for the country's sectors.

Develop and strengthen the means of protection in the state of Kuwait's civil and military networks to reduce the possibility of exposure to cyber-attacks.

Developing legislation and laws on cybercrime and cybersecurity to keep pace with technological development.

Develop cybersecurity regulations, controls and standards for critical networks, electronic services and important systems.

Monitoring the extent to which critical sector institutions comply with national cybersecurity regulations and policies.

Third objective: Provide means of cooperation, coordination and exchange of information among various local and international authorities in the field of cybersecurity:

Developing an information exchange system between government agencies, the private sector and leading cybersecurity companies.

Develop a system of cooperation and information exchange with international and regional organizations and engage in cybersecurity programs to deal with cyberthreats, facilitate access to reliable information and ensure an effective response to all threats.

Develop a reporting mechanism for threats, hacker attacks, or computer crimes.

Development of partnerships with international police to develop joint investigation mechanism for cybercrime.

Cybersecurity in education:

Did you know that the education sector is witnessing a disturbing increase in cyber hacking incidents? According to recent statistics, hundreds of schools and universities around the world have been faced cyber-attacks in recent years, which indicates the seriousness of this problem. Cyber threats have escalated coinciding with the development of technology and the educational system’s reliance on digital media and information technology to facilitate the educational process and achieve communication and distance learning.

Cybersecurity in education has become one of the most important priorities, as electronic information and data in schools and universities must be secured from cyber-hacking and educational networks must be protected to ensure the safety of students and teachers. Furthermore, all members of the educational community must be sensitized to the danger of cyber hacking and enhance awareness of how to prevent this risk and protect personal data.

Cybersecurity in education is a vital topic that requires a lot of attention and thought. The educational sector represents an important target for cyber-attacks due to the amount of sensitive data stored in it, and the necessity of protecting the privacy of students and teachers, and ensuring the continuity of the educational process in a safe and productive manner.

The most important points that should be focused on:

- Securing information and electronic data in schools and universities.
- Protecting educational networks and combating cyber threats.
- Raising awareness of parents and teachers about the importance of cybersecurity.
- Establishing policies for the permitted use of devices and networks.
- Educating students about cybersecurity and the risks of using social media

Cybersecurity guidelines for employees

Schools and universities should establish clear cybersecurity guidelines for employees. This includes instructions for securing passwords, preventing reuse, and storing them in secure ways. Employees should be educated on the importance of cybersecurity and adhere to policies and guidelines regarding downloading applications and sharing personal information on social media. Schools should also instruct students about safe use of technology and keeping personal information secure

Some basic cybersecurity guidelines for employees:

1. Secure your passwords and avoid using weak passwords. Create strong passwords that consist of a combination of capital and small letters, numbers, and special symbols.

2. Ensure that old passwords are not reused. Change your passwords regularly to maintain security.

3. Secure personal and sensitive information in your digital files. Use file encryption and secure storage technologies to protect against unauthorized access.

4. Educate employees about common cyber threats and how to deal with them. Provide training courses and workshops to help employees become familiar with the necessary security precautions.

5. Examine links and attachments in email carefully before opening it. Check the source and reliability before interacting with unknown messages.

The role of parents and teachers in cybersecurity

Parents and teachers represent a significant role in enhancing cybersecurity in schools and universities. Parents should have awareness of the importance of cybersecurity and its role in protecting students. Parents can help educate students about safe internet practices, enhance their awareness of the dangers of cyber hacking, and teach them how to prevent it.

Teachers must be responsible for teaching students about cybersecurity and making them aware of the potential risks and how to face them. Cybersecurity education should be included in school curricula and best practices in the use of digital technology should be followed.

Furthermore, Schools must cooperate with parents to maintain cybersecurity. Schools can provide workshops for parents to teach them how to protect their children while using internet and provide the tools and resources necessary to achieve this

Guidance for parents and teachers:

- Educating students about the importance of cybersecurity and how to protect themselves online.
- Monitor children's use of electronic devices and ensure that they are used in safe ways.
- Teach children about the dangers of sharing personal information and promote online privacy protection.
- Teaching children about electronic fraud and how to deal with it.
- Participate regularly with the school to maintain cybersecurity and exchange necessary information.

The role of parents and teachers in enhancing cybersecurity contributes to creating a safe and reliable online educational environment for the student. We must work together to keep students safe and protect them from cyber threats.

Establish permissible use policies

Establishing clear and transparent policies for the permitted use of electronic devices and networks in schools and universities is an imperative necessity. This contributes to ensuring cybersecurity and protecting important information and data. Permissible use policies include several aspects aimed at enhancing the security of the electronic educational environment.

Policies for the use of electronic devices

Policies for the use of electronic devices relate to determining the proper use of electronic devices within schools and universities. Rules and guidelines are determined regarding the use of mobile phones, tablets, laptops, and other electronic devices used in the educational environment. These policies aim to regulate the use of devices and ensure that there is no distraction and deviation from educational activities.

Malicious website filtering policies

Malicious website filtering policies block access to sites that contain inappropriate or harmful content. The permissible rules and classifications are defined to prohibit access to sites that contain pornographic content, violence, hate promotion, or any content that is inconsistent with the goals of sound education. These policies aim to provide a safe and appropriate environment for students and employees.

Wireless network usage policies

Wireless network usage policies aim to provide rules and guidelines for the use of wireless networks in schools and universities. These policies include things like connection guidelines, secure networks, logging, and basic protection from cyberattacks. The security and safety standards necessary to protect data and wireless communications within the educational environment are determined.

Countering malware

Countering malware policies include specifying precautionary measures and directives to protect important information from malware and viruses. These policies include using protection programs, updating them regularly, and achieving a high level of security for systems and data. The focus on malware aims to reduce cyber threats and ensure continuity of educational services without disruption or data breach.

Establishing permissible use policies is one of the main keys to achieving cybersecurity in educational institutions. By clarifying the required rules and guidelines, schools and universities can ensure the safe and proper use of technology and electronic data. These policies must be known and followed by everyone in the educational environment to ensure effective cybersecurity.

Awareness of danger through social media

Students should be guided and made aware of the dangers of social networking and excessive sharing of personal information. They should be aware of the danger of sharing details of their personal lives on social media platforms and the need to protect their privacy. Cybersecurity awareness should be promoted on social media and students should be encouraged to practice proper etiquette and act with caution when using these platforms.

Today's student is exposed to great challenges when using social media. Some may think that sharing details of their personal lives on these platforms is safe, but the truth is that this may lead to this information being out of the scope of privacy and cyber breaches.

Students should be aware that what they share on social media could become public and may be used against them in the future.

Students should acquire knowledge and proper understanding about using these platforms safely. They should be aware of the importance of protecting personal privacy and not sharing sensitive information on social media. They must also know how to act with caution and avoid behaviors that may lead to fraud and cyber exploitation.

Through appropriate awareness and education, many problems and risks resulting from excessive participation on social media can be avoided. Teachers and parents bear the responsibility of guiding students and educating them about the dangers and the importance of safeguarding their privacy and online safety.

The importance of protecting privacy on social media platforms

Social media platforms are attractive environments for young people, but they also pose significant risks. Many personal information is collected on these platforms, which could be used for illegitimate purposes and to deceive individuals.

It is important to encourage students to protect their privacy and take necessary precautions when using social media platforms. They should ensure to adjust their privacy settings and review them regularly to ensure that their personal information is not shared with undesired individuals. They should also avoid accepting friend requests or engaging in conversations with people they do not already know.

Blocking websites and content filters

Measures should be taken to block harmful websites and prevent access to inappropriate content for students. **Monitoring and filtering tools** can be used to classify and block sites with unsuitable content. It is crucial to ensure students are protected from harmful content and provide a safe online learning environment.

Blocking websites and content filtering are essential components of cybersecurity strategy in educational institutions. Using **monitoring and filtering tools** enables teachers and administrators to filter harmful content and prevent access to sites containing inappropriate material for students. Blocking harmful websites contributes to protecting students from exposure to inappropriate and harmful content such as violent or pornographic materials.

Monitoring and filtering tools help in identifying and categorizing harmful websites and preventing access to them. These tools are configured to monitor user activity on the network and analyze the content present on websites to ensure there is no harmful or inappropriate content. Additionally, monitoring and filtering tools contribute to protecting students' personal data and preventing access to sensitive information.

Some tips to protect privacy on social media:

- Adjust privacy settings according to your personal preferences.
- Review posts or photos that may disclose sensitive or personal information.
- Do not share personal information publicly.
- Do not open unknown links or messages from unknown people.

Monitoring and filtering tools

Many monitoring and filtering tools are available in the market for educational institutions. It's important to choose the most suitable tool based on the institution's needs. Many of these tools provide simple and flexible user interfaces for setting up filtering and monitoring configurations.

When using monitoring and filtering tools, they should be carefully configured to ensure that safe and necessary websites for learning are not blocked. These tools should allow teachers and administrators to filter content based on individual student needs and identify websites and applications that contribute to achieving learning objectives and academic development.

The Role of Training and Education in Enhancing Cybersecurity

It is essential to provide training and education for students and employees about cybersecurity and safe online practices. Students should be systematically taught about the importance of cybersecurity and how to prevent cyber-attacks. Employees should be trained on how to handle sensitive information and implement security practices. Teachers play a crucial role in educating students about internet safety and encouraging them to adhere to safe cyber behavior.

For example, schools can organize workshops and awareness sessions for students to introduce them to cybersecurity concepts and train them on how to use the internet and social media safely, informing them about the security challenges they might face and how to deal with them. Similarly, employees in educational institutions should receive necessary training to acquire cybersecurity skills, recognize security vulnerabilities, and understand how to prevent them.

- Guide students on safe internet practices and warn them of potential risks.
- Educate students about official email and other secure communication methods.
- Raise awareness about cyber laws and digital rights.
- Encourage them to use strong passwords and update them regularly.
- Train employees on security practices.
- Make employees aware of the importance of protecting sensitive information and securing it properly.
- Inform them about phishing techniques and how to handle them properly.
- Explain to employees how to identify malware and prevent it.

By increasing awareness and providing necessary training, cybersecurity in educational institutions can be enhanced, reducing potential risks. Investing in **educating students about cybersecurity** and training employees on safe practices, strengthens the overall cybersecurity protection for the educational community.

Partnership with Cybersecurity Companies

The education sector benefits from outstanding partnerships with cybersecurity firms to provide consulting and cybersecurity solutions. Collaboration with these companies is essential to enhance the stability of the educational environment and protect educational institutions from cyber threats. The partnership contributes to cybersecurity analysis and provides customized plans and strategies to ensure information safety and keep networks and electronic devices secure.

By involving experts and technicians from these companies, specialized consultations on cybersecurity are provided, and innovative solutions are offered. Understanding the cybersecurity challenges faced by the education sector helps in developing appropriate protection strategies and addressing existing and emerging threats.

Areas of cooperation with cybersecurity companies include consulting on designing secure networks and improving security policies and procedures. Continuous training and education for employees can be provided to enhance their security awareness and develop their skills in handling potential cyber threats.

Schools and universities can benefit from **cybersecurity consulting** to improve their security readiness and assess potential threats. Cybersecurity requires regular updating and reviewing of policies and strategies to ensure their suitability for the changing educational environment and evolving cyber threats.

In summary, partnering with cybersecurity companies is crucial to enhance cybersecurity in the education sector. This collaboration provides expertise and consulting to improve security practices and develop the necessary technology to maintain information safety and protect against increasing cyber threats.

The table below highlights some of the key benefits of partnering with cybersecurity companies in the education sector:

The Importance of Cybersecurity for the Future of Education

Cybersecurity in education is seen as a fundamental element for the future of education, as the education sector witnesses increasing use of information technology and reliance on electronic networks. With the growing popularity of digital education technologies and remote learning, the cybersecurity challenge becomes more significant.

Ensuring **the safety of educational networks** and protecting important data and information are essential for achieving an effective and successful educational experience. Good cybersecurity allows educational institutions to ensure the continuity of online education, maintain their reputation, and keep students' and employees' information safe.

With the increasing challenges in cybersecurity, educational entities must be ready to change and evolve. Schools and universities need to enhance **the safety of educational networks** and identify and address new and evolving threats effectively.

Information technology plays a crucial role in the modern learning process, but it comes with security challenges. Educational institutions must be prepared for these challenges and make every effort to protect sensitive data and information.

Future cyber threats are multiple and diverse, so preparation for various scenarios and providing solutions and strategies to address these challenges is necessary. Equipping educational entities with specialized cybersecurity teams and providing appropriate training for employees are essential parts of the action plan to enhance cybersecurity in education.

By investing efforts and resources in cybersecurity, the education sector can achieve a safe and effective education. Cybersecurity contributes to maintaining the confidentiality and integrity of personal data and providing a learning environment that motivates students to innovate and grow. Without good cybersecurity, educational institutions can be exposed to serious threats that could negatively impact their reputation and viability.

By turning to companies and experts in the field of cybersecurity and leveraging their knowledge and expertise, educational institutions will be able to implement security best practices and innovate in this vital area. Future cyber challenges should be a catalyst for improving security strategies and promoting awareness and education in the educational sector.

Future Cybersecurity Challenges

- Increase sophisticated and growing cyberthreats.
- The increasing use of information technology and its ability to communicate and exchange.
- Poor security in educational applications and systems.
- The prevalence of targeted cyberattacks and personal data breaches.

Protecting cybersecurity in education requires cooperation and coordination between schools, universities, companies, and Governmental institutions. There must be a strict commitment to implementing security policies and modern protection technologies to keep data safe and protect the educational community.

It's important for educational institutions to recognize the importance of cybersecurity and the need to develop robust strategies to address future threats. Investing in cybersecurity will help preserve the reputation of educational institutions, the quality of education, and the safety of important data for students and staff.

Action Plan to Strengthen Cybersecurity

To strengthen cybersecurity in the education sector, we propose a comprehensive action plan aimed at enhancing protection and preparing for security challenges. This plan will include implementing cybersecurity policies and guidelines, **assessing the organization's security readiness**, identifying risks and taking the necessary measures to address them.

Implementing cybersecurity policies in an educational institution is an important step in creating a safe and reliable learning environment. Policies and guidelines should be established that set the standards for keeping sensitive data and information safe. This includes defining stakeholder areas and clearly distributing responsibilities, and establishing policies to regulate the use of technology and identify unacceptable behaviors.

After implementing cybersecurity policies, the **security readiness** of the organization should be **assessed**. The strengths and weaknesses of the current security architecture should be analyzed and areas that need improvement should be identified. **The security readiness assessment** contributes to identifying needs and allocating the necessary resources to enhance cybersecurity.

After analyzing security readiness, potential security risks must be identified, and measures must be put in place to address them. These measures can include the use of advanced security technologies, such as firewalls and intrusion detection systems, to combat attacks and minimize threats. Emergency recovery procedures and an effective emergency response plan should also be put in place.

The plan is not limited to implementing policies and analyzing risks but can also guide ongoing training for staff and students. Regular training helps raise awareness about cybersecurity and teaching basic skills to prevent cyberattacks. Policies and procedures should be updated according to security developments and develop more advanced strategies and tools to combat future threats.

With the guidance of a cybersecurity action plan, an educational institution can protect its sensitive data and information and comprehensively enhance cybersecurity. By implementing policies, assessing readiness, identifying risks, and guiding training, a safe and reliable learning environment can be maintained in the education sector.

Is there a need to teach cybersecurity in schools and universities?

With the widespread use of Internet programs and personal computers among all age groups, the lives of many are threatened by the information and data on their devices.

There are many specialists in the development of learning programs and sections calling for the addition of a material called cybersecurity for school students to prepare them to use their devices properly and avoid any cybercrimes that could affect their lives.

For those who don't know, cybersecurity is the protection of personal computers, communication accounts, electronic systems, networks, and everything related to the Internet from hacker attacks, data breaches, and privacy.

Those who advocate for teaching cybersecurity aim to raise awareness among students and teach them about the dangers of using the Internet and the issues that can arise from it.

There are many benefits to teaching cybersecurity. It involves raising students' awareness and educating them about the use of the internet and electronic devices. It also includes introducing them to data protection programs, how to employ and benefit from them, as well as learning about attack prevention programs and how to stop hackers from accessing their accounts and personal data. This, in turn, qualifies them to manage their electronic projects in the future and protect them from the dangers of the web.

At the same time, studying this field professionally would be very costly. I believe it is impossible to provide it to all students for free in schools, as it requires paid subscriptions for certain programs, in addition to a specialist in the field rather than just a regular teacher.

Additionally, it is a field that requires a significant amount of time and practical hours to study, which could negatively impact the overall academic performance of the students.

Challenges of Cybersecurity in Education:

1. Personal and Financial Data: Sensitive personal information of students and parents, such as financial information, addresses, and medical data, is stored within learning management systems. Protecting this data is vital to prevent identity theft and its use in fraudulent activities.

2. Technical Challenges: The adoption of technology in education brings security challenges such as malware, breaches, distributed denial-of-service (DDoS) attacks, and more. Educational institutions must provide protection for the systems and networks they use.

3. Security Awareness: Continuous education of students and teachers about information security is essential. Awareness must be raised regarding phishing emails, malicious links, and basic protection methods such as strong passwords and two-factor authentication.

Strategies to Enhance Cybersecurity in Education:

1. Developing Security Policies: Establish clear policies for data protection and technology use, including defining access permissions and providing ongoing training for staff.

2. Using Advanced Security Technologies: Adopt security solutions such as intrusion detection systems and access control devices to keep data safe.

3. Collaboration with the Academic Community and Industry: Partner with external entities to share knowledge and stay updated on the latest cybersecurity threats.

4. Proactive Threat Response: Develop strategies for rapid response to security incidents and assess potential damages.

3. CONCLUSION

In the digital age, educational institutions must place significant emphasis on cybersecurity as a fundamental part of their mission. By implementing effective preventive and educational measures, they can provide a safe and secure learning environment for everyone within the educational system.

4. SUMMARY

Cybersecurity in the education sector is of great importance for preserving the safety of information and electronic data and ensuring the security of educational networks. By adopting security guidelines, raising awareness, and providing training, the risks of cyber breaches can be effectively reduced, thus protecting the educational community.

Investing in cybersecurity enhances the quality of education, preserves the institution's reputation, and safeguards data integrity. This requires collaboration with specialized cybersecurity firms to develop updated and effective protection strategies to address evolving threats.

It is important for educational institutions and members of the educational community to have a strong commitment to enhancing cybersecurity and overcoming the challenges they face. This requires providing continuous training and education for teachers, students, and parents about best practices and safe behaviors online.

REFERENCES

[1] https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

[2] https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security

[3] https://online.utulsa.edu/blog/information-security-vs-cybersecurity/

[4] https://www.institutedata.com/blog/what-are-the-7-types-of-cyber-security/

[5] https://securuscomms.co.uk/cybersecurity-in-education-the-latest-trends/

[6] https://www.proofpoint.com/au/threat-reference/security-awareness-training

[7] https://esoftskills.com