VIT
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

Security Awareness Training Program

Cybersecurity and Ethical Hacking

By Team 8.2_Kodhai U [20BRS1237]

CONTENTS

ABSTRACT

Overview on Security Awareness Training

We use social media and e-mails on a regular basis as a means of communication these days and almost all our personal data including pictures, passwords, and other important documents. Hence, awareness on how to keep these data safe and about the possible threats and attacks they could suffer is important. That is why, Security Awareness Training is an awareness effort whose main goal is to increase the understanding about cyber-attacks and threats to common people as well as employees working at major companies. It is extremely necessary for companies to be cautious about cyber threats, attacks, and data breaches as this could pose a great threat to the privacy of their clients. As a result, it could be a threat to the company as well. So, every organization need to have a well-trained cybersecurity team that can ensure the safety of the data and privacy of the clients. Further, common people also require awareness about cybercrimes and how to stay safe and protect their data from hackers and attackers.

As mentioned, programmes for cybersecurity awareness training are created to inform employees of the value of cybersecurity, provide them with the information and abilities to recognise and counteract cyberthreats, and encourage responsible online conduct. These initiatives seek to educate staff members on the possible dangers and weaknesses brought on by technology use while also arming them with the resources they need to defend the company from cyberattacks.

INTRODUCTION

Project Purpose

The main goal of this project is to increase the understanding of cyberthreats and the security risks associated with one's actions. It is also to empower common people as well as employees to be safe and more secure in the online community. Further, it is necessary for employers and the companies to manage and mitigate organizational risks and identify cyber-attacks while helping the organization in fighting and preventing security breaches. It is known that data breaches are expensive and it must be secured. It is possible that simple human errors can cause breaches. Hence, this program helps in understanding and dealing with these errors that could occur while performing everyday tasks.

There are several ways to come about this program. It must be designed in such a way that it reaches the target audience. Hence, it is important that the target audience are fixed before starting the training. The training could be for company leaders or employers who set up the organization's infrastructure including the cybersecurity team, or it could be for employees who are working under the organization and need to know the importance of being cautious while working in the company's systems or even their own as individuals.

These initiatives aim to develop a cybersecurity culture inside the company, where staff members actively participate in securing the assets of the company and recognise the value of protecting sensitive information.

The educational initiatives are designed to increase people's comprehension of numerous cybersecurity ideas, including phishing, social engineering, password hygiene, malware, and data protection. They offer helpful advice on how to recognise and handle these dangers successfully. People are frequently seen as the cybersecurity defences of an organization's weakest link. By teaching staff members about typical dangers and recommended practises,

awareness training programmes seek to decrease human error and mistakes that might result in security breaches. These programmes seek to lessen the frequency of security issues brought on by employee mistake, such as clicking on harmful links or falling for social engineering scams, by arming staff with the appropriate information and abilities.

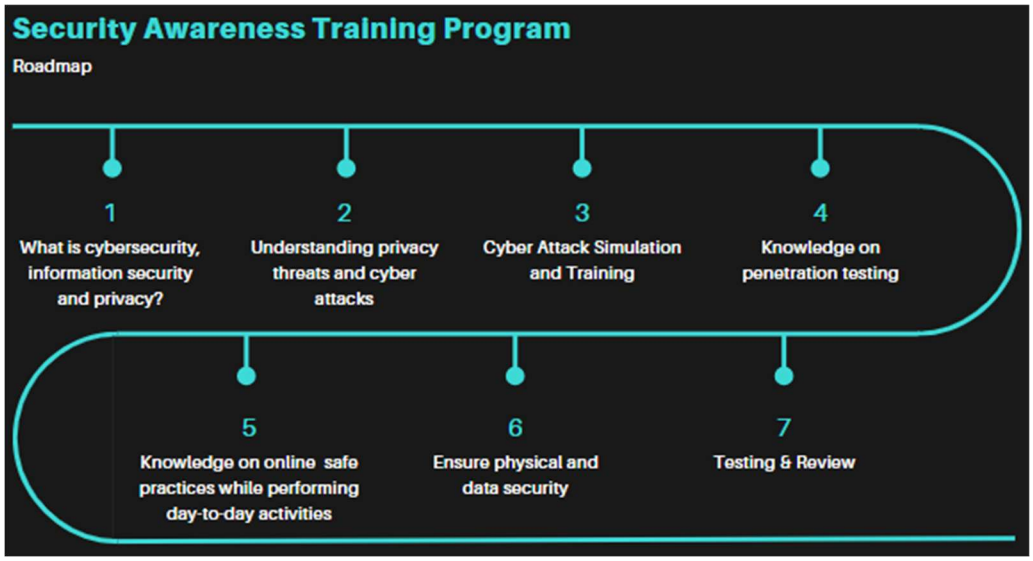

Fig 1.1 Security Awareness Training Program Roadmap

Overview on Cybersecurity

The practise of preventing unauthorised access, damage, theft, and disruption to computer systems, networks, and digital information is referred to as cybersecurity. The interconnection of our digital world and our growing reliance on technology have made cybersecurity a top priority for all stakeholders, including people, corporations, and governments. It includes a range of actions, including putting security protocols into place, encrypting data, performing routine audits, and informing users of potential dangers and best practises.

In today's world, cybersecurity awareness is crucial. Protection against cyber threats is extremely important especially in a huge organization that hosts data of millions of users. To exploit flaws in computer systems and networks, cybercriminals constantly create new tactics. By spreading knowledge about cybersecurity, people and businesses can become aware of potential dangers like malware, phishing scams, ransomware, or data breaches. With this knowledge, they can safeguard their systems and sensitive data proactively, decreasing the likelihood that they will become the target of cyberattacks.

Further, personal information has become a valuable asset in the digital era, thus it must be protected. Individuals are frequently the target of cybercriminals who want to access their personal information, such as financial information, social security numbers, or login credentials. People can use safe online platforms, create strong passwords, and recognise and prevent potential scams by being informed of cybersecurity best practises. This gives consumers the ability to protect their personal data and reduce the possibility of identity theft or financial damage.

Cyberattacks can have catastrophic effects for companies. A successful attack may lead to monetary losses, reputational harm, business disruption, or the loss of confidential customer information. Employees can learn about safe computer practises, recognise suspicious activity, and comprehend their responsibility in ensuring a secure working environment through encouraging cybersecurity awareness within organisations. By strengthening the organization's defences, this lowers the risk of successful cyberattacks.

As more activities in both the personal and professional spheres become digital, privacy has grown to be a major concern. Cybersecurity education emphasises the significance of online privacy protection. Individuals can make wise judgements about the data they publish, use caution when using social media platforms, and take precautions to protect their privacy rights by being aware of the hazards involved with sharing personal information.

In addition, cybersecurity is important for ensuring national security as well as being a worry for people and businesses. Critical infrastructure systems, governmental institutions, and military organisations might all be the targets of cyber espionage, sabotage, or disruption. Governments may inform citizens about potential cyber risks, encourage responsible online conduct, and set up effective defences to safeguard critical services and infrastructure by encouraging cybersecurity awareness on a national scale.

Both individuals and organisations may suffer large financial losses as a result of cyberattacks. Knowledge of cybersecurity enables people and organisations to assess the possible financial repercussions of a cyber catastrophe and take preventative action. To lessen the financial impact of an attack, this involves constantly updating software and security systems, putting strong authentication mechanisms in place, and storing up crucial data.

In the modern digital economy, confidence and trust are essential for carrying out transactions and interacting with others online. Customers, partners, and stakeholders are more likely to trust individuals and companies that show a strong commitment to cybersecurity. Organisations are encouraged to embrace industry best practises, follow legal obligations, and take a proactive stance in protecting data and privacy as a result of increased public awareness of cybersecurity. As a result, relationships are strengthened and client confidence is increased.

Cyber dangers frequently transcend geographical boundaries, necessitating worldwide cooperation and teamwork to effectively combat them. Countries can exchange information, cooperate on threat intelligence, and work together to improve cybersecurity measures through raising awareness about cybersecurity on a global scale. An international culture of cooperation and information sharing is encouraged by greater knowledge, forging a unified front against online threats. Individuals, businesses, and governments may reduce risks, safeguard sensitive data, and promote a safer digital environment for everyone by being aware of the dangers, implementing best practises, and keeping up with the ever-changing cyber threat landscape.

LITERATURE SURVEY

The Cybersecurity and Infrastructure Agency (CISA) Cybersecurity Awareness Program proposed ways to help people understand the importance and tried to promote safe and secured practices online. This was specifically provided for Americans where they can access resources and tools that could be required for them to take proper decisions while keeping their data protected.

Another article suggests three important elements that are necessary to be covered in a security awareness program – Email Security Protocols, Malware recognition and avoidance, and password security. They offered several cybersecurity solutions and ways to keep one's data protected. There are specific topics that also need to be added in an awareness in addition to the above mentioned three: Privacy, Email/Phishing Security, Web/Internet Security, Social Media Usage, Social Engineering, Public Wi-Fi Safety, Guidance on working remotely, SQL injection, etc.

Proposed solution

A proper awareness program can be conducted in various ways. It can be an in-person training or a long-form computer-based training. Either way, for the program to be effective, it needs to be short and focused on individual topics making it easier for the audience to understand and get a hang of what are the important points to be noted, remembered and how to implement it on a regular basis. An awareness program can include the following:

- **Reading modules:**
  Hand-books or modules covering basic and important topics in the field that every individual needs to know. The audience each can be provided with a booklet that sums up what they need to know to have a basic understanding on the topics including the safety rules and protocols that can be easily followed by anyone to ensure extra safety towards their data or accounts including topics like two-factor authentication, how to choose a safe and uncrackable password, how to safeguard your accounts, what is firewall and why do we need it, etc.
- **Videos:**
  Short video lectures explaining how cybercrime-attacks are performed and how it can be prevented and protected.
- **Classroom-based Training:**
  The typical method for promoting cybersecurity awareness involves having participants attend live training sessions led by trainers or cybersecurity professionals. With the help of this technique, the trainer and the participants may speak with each other in real time and participate in direct conversation. In a classroom setting, participants have the chance to interact directly with the trainer and other attendees. This encourages a community of learners who may ask questions, exchange experiences, and learn from one another's various viewpoints. Additionally, it provides individualised learning opportunities since instructors may adjust the talks, examples, and information to fit the requirements and backgrounds of the participants. This makes it possible to handle the cybersecurity issues and problems that are important to the organisation in a more focused manner. In a classroom context, instructors can present live demonstrations of cybersecurity technologies, strategies, or simulated attack scenarios. Participants'

practical knowledge and ability to apply cybersecurity principles in practical settings are both improved by this hands-on approach.

- **Gamification and Simulation-based Training:**
  Innovative techniques like gamification and simulation-based training are employed in cybersecurity awareness programmes to keep participants interested, encourage active learning, and improve the efficiency of training. Gamification is the process of adding game mechanics, design aspects, and game components to training exercises in order to make them more interactive, entertaining, and engaging. It is usual practise to utilise points, badges, leaderboards, challenges, and awards to instill a sense of accomplishment, competitiveness, and incentive among players. Interactive tests, scenario-based challenges, virtual missions, and progress monitoring are all possible components of gamified cybersecurity awareness training. Gamification raises participants' enthusiasm, improves information retention, and motivates them to actively engage in the training by changing learning into a game-like experience.

THEORITICAL ANALYSIS

Some Important Security Terms and Methods

Password Management:

In today's digital environment, password management is a vital component of cybersecurity. Protecting sensitive information with strong and secure passwords is now more crucial than ever due to society's growing reliance on online accounts and services. To protect our personal and financial information in this age of ongoing data breaches and hacker attempts, it is essential to comprehend and put into practise sound password management procedures.

The first step to successful password management is creating strong, one-of-a-kind passwords. A strong password often consists of a mix of numbers, special characters, and both uppercase and lowercase letters. Avoid using widely used words, predictable patterns, or private information like birthdays, names, or addresses. Choose complicated and random combinations instead, which are difficult for hackers to decipher. The process of creating and storing strong passwords can be significantly streamlined by using a password manager. Password managers are safe programmes that keep your passwords safe by encrypting them and storing them in a database that is secured by a master password. They can create complex passwords for you, removing the need for you to remember them all and lowering the likelihood that you would use weak or obvious passwords. Furthermore, auto-fill features offered by password managers make using strong passwords on a variety of platforms and devices simpler and more convenient.

Another crucial component of efficient password management is routine password changes. Although there is some disagreement on how frequently to change passwords, it is typically advised to do so every three to six months. Regular modifications reduce the likelihood of a password compromise. Changing passwords right away after a security breach or unauthorised access guarantees that the compromised credentials are no longer valid. It is crucial to remember that password changes shouldn't feature recognisable patterns or gradual variations. To preserve security, every password update should produce a password that is unique and robust.

Reusing passwords should be avoided as well. Many people tend to use the same password on numerous accounts out of convenience. However, this method is very dangerous. A hacker may be able to access all other accounts that share the same password if they are successful in obtaining the password from one compromised account. Use different passwords for each account to stop this cascading effect. A password manager may safely store and organise passwords for many accounts, negating the need to reuse them, even though it may be difficult to remember a lot of passwords.

Password management gains an additional layer of protection thanks to multi-factor authentication (MFA). MFA demands various forms of identity from users to access an account. It typically entails combining something you have (such a security key, your fingerprint, or a one-time code received on your mobile device) with something you know (a password). Even if a password is hacked, this dual verification procedure considerably improves security by lowering the likelihood of unauthorised access. Enabling MFA is strongly advised whenever possible, especially for important accounts like email, banking, and social media platforms.

Multi-factor authentication (MFA) adds an extra degree of security to password management. MFA requires users to provide several kinds of identification to access an account. Usually, it involves fusing a password with something you already have (such a security key, your fingerprint, or a one-time code you received on your mobile device). This dual verification process significantly increases security by reducing the risk of unauthorised access, even if a password is cracked. It is highly recommended to enable MFA whenever you can, especially for crucial accounts like banking, social networking, and email.

Email/Phishing Security:

In today's digital environment, email security and defence against phishing attempts have become essential considerations. Given that email is one of the main ways that people and businesses communicate, it's critical to recognise the dangers of phishing and take appropriate security precautions to protect sensitive data.

To deceive people into disclosing personal information like usernames, passwords, or financial information, attackers will pretend to be a reliable entity (known as "phishing"). These attacks are often carried out through phoney emails that look official and frequently imitate well-known organisations or people. Phishing attacks try to trick their victims into opening malicious attachments, clicking on harmful links, or providing sensitive information. There are several best practises that people and organisations should adhere to strengthen email security and defend against phishing attempts.

First and foremost, when it comes to email interactions, it is crucial to exercise caution and scepticism. Be wary of emails you don't expect, especially ones that ask for private or delicate information. Consider the sender's email address, subject line, and content if an email sounds shady. To identify a phishing email, look for any grammatical or spelling problems. Be especially wary of emails that convey a feeling of urgency or attempt to elicit an emotional response because phishing attackers frequently use these strategies.

A further useful step is to independently get in touch with the alleged sender of the email to confirm its validity. Instead of responding to the email directly or opening any embedded links, manually look up the organization's or person's official contact details. You can determine whether the email is authentic or a phishing effort by getting in touch with them through a reliable and trusted channel, such their official website or customer care hotline.

Additionally, it is vital to use caution while downloading attachments from emails or clicking on links inside them. Before clicking on a hyperlink, hover over it to see the exact URL. Avoid clicking if the URL appears suspicious or differs from the desired location. To be sure you are accessing the right and legitimate website, manually type the website's address into your browser. Likewise, be wary with email attachments, especially those coming from unexpected or shady sources. The malware or ransomware that malicious attachments carry has the potential to infect your machine or network. Always run a trustworthy antivirus programme before opening an attachment.

Strong spam filters and email filtering systems should be used to further improve email security. These programmes can recognise and reject phishing emails, stopping them from getting to your mailbox. Spam filters use a variety of methods, such as email content analysis, sender reputation checks, and knowledge of known phishing patterns, to find and quarantine problematic emails. The likelihood of becoming a victim of phishing attacks can be considerably decreased by turning on these filters and consistently updating the security settings in your email client.

Another essential component of email security is educating yourself and your staff about phishing dangers and appropriate practises. To increase understanding of typical phishing techniques, how to spot phishing emails, and the significance of keeping a security-conscious mindset, hold frequent training sessions. Inform staff members of the dangers of clicking on untrusted links or sending confidential information through email. You can enable people to be proactive in defending themselves and their organisations against phishing attempts by developing a culture of cybersecurity knowledge.

Keep your email client and operating system updated with the most recent security patches and upgrades as well. Software makers frequently provide updates to fix flaws and bolster security protections. You can lessen the chance of being exploited by attackers who aim to exploit known vulnerabilities by rapidly installing these updates.

In conclusion, a multi-layered strategy is needed for email security and phishing assault defence. You may dramatically lower your chance of falling for phishing scams by being watchful, checking the legitimacy of emails, being cautious when clicking links or opening files, putting effective spam filters in place, and educating both yourself and your staff.

Web/Internet Security:

As we navigate the online world, web and internet security is essential in protecting our personal and sensitive data. Understanding the fundamentals of web security and putting them into practise are crucial for protecting ourselves and our digital assets considering the growing reliance on web-based services and the persistent threat of cyberattacks.

Encrypted secure communication is one of the core components of web security. Data transmission between your device and a website is encrypted to prevent unauthorised parties from deciphering it. Encryption is made possible, and a secure connection is established between your browser and the website you are browsing using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocols. This stops criminals from intercepting and tampering with your data, including login passwords, financial information, or personal information, while it is in transit.

Look for the padlock icon in the browser's address bar or a URL that begins with "https://" rather than "http://" to tell if a website is utilising encryption. A secure connection is indicated

by the "s" in "https". When entering sensitive information on websites without the necessary encryption safeguards in place, extreme caution must be taken.

The usage of strong and distinctive passwords is a crucial component of web security. Brute-force assaults, where automated systems repeatedly try various combinations to crack passwords, are susceptible to weak passwords. It is crucial to make complicated passwords that combine uppercase and lowercase letters, numbers, and special characters to reduce this risk. Avoid using words or phrases that are simple to guess, such as names, dates of birth, or frequent expressions. To prevent a single compromised password from allowing unauthorised access to various platforms, it is also essential to use different passwords for each online account.

Multi-factor authentication (MFA) implementation boosts web services' security. MFA requires users to submit extra credentials in addition to a password, such as a fingerprint, a special code transmitted to a mobile device, or a security key. Even if an attacker is successful in getting your password, they would still require the second factor to access the system. Enabling MFA whenever it is possible greatly improves security and makes it more difficult for unauthorised users to access your accounts.

To fix vulnerabilities and defend against new threats, operating systems and web browsers constantly publish security updates and patches. To take advantage of the most recent security improvements, it's critical to keep your operating systems, plugins, and browsers up to date. Bug fixes, security patches, and enhancements to reduce known vulnerabilities are frequently included in these updates. Set up your devices to automatically install updates or manually check for newer versions on a regular basis.

The use of caution when downloading files or clicking on links is a crucial component of web security. Internet users frequently fall victim to phishing assaults, in which attackers pretend to be reliable organisations to deceive people into disclosing personal information. Be wary of unexpected or suspicious emails, instant messages, or pop-up windows that request personal information from you in exchange for your clicking on a link. Before clicking on links, hover over them to see a preview of the URL. Avoid clicking on links that appear dubious or lead to locations other than what you were expecting. Additionally, be careful when downloading files from unreliable websites or when opening attachments from unknown senders because they can be infected with malware or viruses that jeopardise the security of your device.

Consider using a virtual private network (VPN) when using the internet, especially when using open Wi-Fi networks, to further increase web security. Your internet traffic is encrypted using a VPN, making it more challenging for outsiders to eavesdrop on or monitor your online activities. Particularly when accessing sensitive information or making financial transactions online, it gives an added degree of privacy and protection.

In conclusion, online and internet security are essential for safeguarding our private information in a world that is becoming more and more digital. By being aware of and using security precautions like encryption, strong passwords, multi-factor authentication, updated software, being cautious when opening links or downloading files, etc…

Social Media Usage:

Social media is now an essential component of our daily lives in today's connected society. However, it's critical to be aware of any security risks related to using social media. Maintaining security awareness while using social media platforms is crucial due to the rising frequency of cyber threats and the possibility for privacy violations.

The most important thing to remember is to exercise caution while posting material to social media. You run the danger of identity theft or targeted attacks if you share too many personal details. Posting private information like your whole birthdate, home address, phone number, or financial information is not advised. Real-time location disclosures should be used with caution as they can expose you to physical security threats. This information can be used by cybercriminals to pose as you or launch specialised attacks. Review your privacy settings on social networking networks frequently, and only allow select friends or contacts to see your personal information.

It is crucial to exercise caution when it comes to the connections you form on social media. Accepting friend requests from people you don't know or trust, or engaging with them, should be avoided. False profiles are frequently created by scammers and malicious individuals to collect personal data or trick people into clicking on harmful links. Examine a person's profile and shared connections before connecting with them to see if they are real. It's wise to err on the side of caution and refrain from engaging with strangers if something sounds suspicious.

Being careful with everything you connect with on social media is a crucial component of security awareness. When clicking on links shared on social media, exercise caution, especially if they seem suspect or originate from unreliable sources. These links could direct you to harmful websites or start the download of malware onto your computer. Never click on links without first hovering over them to see the URL. You should also exercise caution while downloading or opening attachments shared on social media because they can be infected with malware or viruses.

It's crucial to keep up a secure and distinctive password for your social media accounts. Avoid using passwords that are simple to guess and avoid using the same password on multiple platforms. Update your passwords frequently and think about using a password manager to manage and store them safely. Your social network accounts are more secure when you use multi-factor authentication (MFA). By turning on MFA, you make sure that even if someone gets hold of your password, they still need the extra authentication factor to log in.

Understanding the dangers of social engineering attacks is essential. Cybercriminals employ the technique of social engineering to trick others into disclosing private information or taking specific activities. To trick users, they may pose as reputable companies, groups, or brands. Be wary of unsolicited emails or phone calls asking for personal information, especially if they seem to be coming from a reputable source. If in doubt, independently confirm the request's validity through a dependable and verified means.

Review the terms of service and privacy policies of the social networking sites you use on a regular basis. Recognise the processes used for gathering, storing, and sharing personal data. Avoid giving applications or other third-party services connected to your social media accounts any access they do not need. Examine and eliminate any unneeded or pointless apps that may have access to your personal information on a regular basis.

Ethical Hacking as a career

The field of ethical hacking, sometimes referred to as penetration testing or white-hat hacking, is referred to as hacking as a career. Cybersecurity experts known as ethical hackers are permitted to evaluate the security of computer systems, networks, and apps with the aim of spotting vulnerabilities and potential weak points. They assist organisations in strengthening their security defences by using ethical and legal hacking techniques and

processes. Ethical hacking is basically evaluating the security state of a system within an organisation, authorised persons employ hacking tools and techniques. Penetration testers and security consultants, commonly referred to as ethical hackers, simulate actual cyberattacks to find flaws and make security-improvement suggestions.

Ethical hackers operate inside the law, securing the necessary approval from the company to test its systems. To make sure that their acts are legal and beneficial, they abide by rigid rules of engagement and ethical standards. To find flaws in computer systems, networks, and applications, ethical hackers use a variety of tools and approaches. They examine system configurations, do network scans, review code, and make an effort to exploit vulnerabilities in order to gauge the impact. After vulnerabilities are found, ethical hackers produce a thorough report detailing their findings. They offer suggestions to the organisation on how to strengthen their security defences and address the weaknesses. This can entail recommending security updates, configuration modifications, or other security measures.

The several types of ethical hacking include web application testing, network security evaluation, wireless network evaluation, social engineering, and more. Each section focuses on a different facet of cybersecurity and calls for specialised training. Before hostile hackers may take advantage of vulnerabilities, ethical hacking helps organisations find and fix them. Ethical hackers help to build security defences and protect sensitive data by simulating actual attack situations. Organisations frequently deal with industry standards and legal regulations connected to cybersecurity. By locating security flaws and putting the required controls in place, ethical hacking can assist organisations in complying with regulatory requirements. By proactively correcting weaknesses, it also aids in risk management. By offering important insights into the organization's security posture, ethical hackers help incident response operations. Their analyses can aid organisations in better comprehending the effects of future attacks and developing efficient reaction strategies. Ethical hacking is a continual process that encourages constant development of a company's security procedures. Organisations may maintain an adaptive and strong security posture by conducting regular assessments and penetration testing. Through its ability to assist organisations in proactively identifying and addressing vulnerabilities, ethical hacking plays a significant role in the cybersecurity landscape. It lets businesses to safeguard their digital assets, uphold customer confidence, and remain resilient in the face of changing cyberthreats.

Certificates required as an Ethical Hacker

Certificates serve as a form of professional validation and show that a person has a specific amount of knowledge and skill in ethical hacking. They act as verifiable proof of the hacker's abilities and credentials. Additionally, they are frequently acknowledged and regarded within the cybersecurity sector. They provide evidence that the ethical hacker has satisfied particular criteria established by respectable institutions or certification authorities, which raises the legitimacy of their skills. Clients and organisations may be assured by certificates that an ethical hacker has the skills and knowledge required to carry out their tasks. Clients frequently search for people who possess recognised credentials when employing ethical hackers or using their services to make sure they are working with a qualified expert. The participation of qualified experts may be required by compliance

requirements and laws in specific sectors or for particular types of activities. For instance, organisations may be obliged to work with certified ethical hackers to satisfy requirements while undertaking security assessments or audits for regulatory compliance purposes.

An ethical hacker's professional chances and possibilities can be improved by certificates. As it displays their dedication to continued professional development and keeping up with the most recent industry practises and techniques, many organisations prefer hiring certified individuals. Ethical hackers must go through difficult training and testing procedures to get certified. Through this process, they obtain a thorough understanding of ethical hacking methodology, tools, and best practises in addition to expanding their knowledge and learning new skills. Access to professional groups and networks is frequently included with certifications, enabling ethical hackers to network with colleagues, exchange experiences, and pick the brains of subject-matter experts. These communities offer continuing assistance, information exchange, and chances for career advancement.

Some of the certificated that are required as an ethical hacker include:

1. **Certified Ethical Hacker (CEH):**
   The International Council of E-Commerce Consultants (EC-Council) offers the Certified Ethical Hacker (CEH) certification, which is one of the most well-known qualifications for ethical hacking. It certifies the skills and knowledge required to discover vulnerabilities and conduct penetration testing. CEH covers a wide range of issues, including reconnaissance, scanning, enumeration, system hacking, and ethical hacking methods.
2. **Offensive Security Certified Professional (OSCP):**
   Offered by Offensive Security, the Offensive Security Certified Professional (OSCP) certification emphasises practical, hands-on penetration testing abilities. Candidates for the certification must successfully identify vulnerabilities in systems and exploit them in a controlled setting through a rigorous 24-hour practical exam. The OSCP places a strong emphasis on practical applications and promotes innovative thinking to address security issues.
3. **Certified Information Systems Security Professional (CISSP):**
   The (ISC)^2 certification, Certified Information Systems Security Professional (CISSP), is extensive and covers a variety of information security topics. CISSP offers a strong foundation in security concepts, risk management, and security governance, despite not being exclusively focused on ethical hacking. It is well-known in the field and appropriate for experts who want to focus on a wider range of security domains.
4. **Certified Penetration Testing Professional (CPENT):**
   The CPENT certification is offered by EC-Council and is created exclusively for penetration testers. Advanced penetration testing procedures, network pivoting, post-exploitation methods, and report writing are all validated by CPENT. It places a strong emphasis on practical knowledge and gives professionals the tools they need to carry out challenging penetration examinations.
5. **GIAC Penetration Tester (GPEN):**
   The Global Information Assurance Certification (GIAC) offers the GIAC Penetration Tester (GPEN) certification, which certifies the abilities needed to carry out penetration testing and vulnerability assessments. GPEN encompasses

exploitation techniques, post-exploitation techniques, scanning and enumeration, and reconnaissance. The certification places a strong emphasis on comprehending vulnerabilities and evaluating risks from the standpoint of an attacker.

6. **Certified Security Analyst (ECSA):**
   The CEH certification is the foundation for the Certified Security Analyst (ECSA) certification, which is offered by EC-Council. The ECSA emphasises actual proficiency with penetration testing techniques and equipment. Network scanning, vulnerability analysis, system hacking, web application penetration testing, and report authoring are just a few of the topics it covers. ECSA is meant to give professionals the practical skills they need for productive penetration testing projects.
7. **Certified Secure Computer User (CSCU):**
   Offered by EC-Council, the Certified Secure Computer User (CSCU) certification is a fundamental credential for people who desire to develop a basic grasp of cybersecurity and ethical hacking. Operating system security, digital information protection, virus awareness, and fundamental network security concepts are all covered by CSCU. For individuals who are new to the field of ethical hacking, it is a good place to start.
8. **Certified Web Application Penetration Tester (CWAPT):**
   Web application security and penetration testing are the main areas of concentration for the Certified Web Application Penetration Tester (CWAPT) certification, which is offered by EC-Council. CWAPT certifies knowledge of web application vulnerabilities such injection attacks, cross-site scripting (XSS), and unsafe direct object references. It covers testing techniques, equipment, and industry standards for online applications.
9. **Certified Information Security Manager (CISM):**
   Although not exclusively focused on ethical hacking, the Certified Information Security Manager (CISM) certification, provided by ISACA, is well-known in the information security industry. The CISM certifies knowledge of managing, creating, and directing an organization's information security programme. It addresses issues including information security management systems (ISMS), incident response, governance, and risk management.
10. **Certified Wireless Security Professional (CWSP):**
    The CWSP certification, offered by CWNP, focuses on protecting wireless networks. It covers subjects like secure network design, encryption protocols, authentication methods, and wireless network vulnerabilities. CWSP is beneficial for people interested in wireless security and ethical hacking since it gives experts the abilities needed to examine and safeguard wireless networks in an efficient manner.
11. **Certified Network Forensics Examiner (CNFE):**
    Mile2 offers the Certified Network Forensics Examiner (CNFE) certification for individuals with a focus on network forensics. CNFE encompasses subjects including packet analysis, network traffic capture, intrusion detection and prevention, and incident response, while it is not just concerned with ethical

hacking. It gives experts the tools they need to look into and evaluate network-based security issues.

EXPERIMENTAL INVESTIGATIONS

Recent Cyber Attacks in the past years

Telecom and BPO Companies Attack by SIM Swapping Hackers

(June 2022) "Scattered Spider"

The attackers gained initial access to the target by carrying out various methods of social engineering like phone calls and telegram messages in attempts of impersonating an IT personnel. These are to trick the victims into unintentionally leaking their credentials or installing remote monitoring tools into the target environment. The victims were also tricked into sharing their OTPs or were subjected to prompt bombing which is another social engineering technique that is applied to gain access to a specific network by tricking the victim. Similarly, many other attacks were launched on victims including using stolen credentials to authenticate to the organization's Azure tenant, exploitation of bugs, access gain to multi-factor authentication console and enrolling the attacker's own devices to them, etc. After the initial access, reconnaissance of various environments is conducted. Additional tools that might be required to exfiltrated VPN and other software were downloaded for further access.

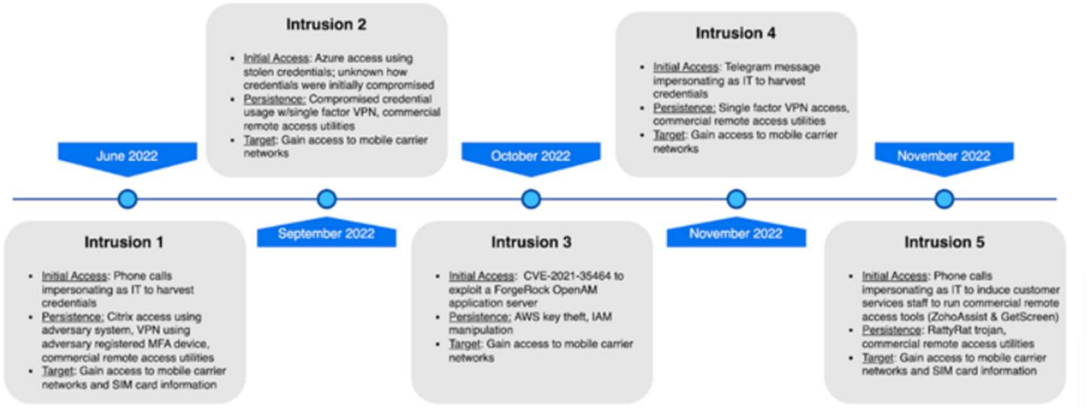

Fig 1.2. Telecom and BPO attacks Intrusion Timeline

Muddled Libra: Targets BPO Sector with Advanced Social Engineering

(Late 2022)

0ktapus phishing kit, a package that offered a prebuilt hosting framework and bundled templates to perform phishing attacks more efficiently. This was first released and came to be known in August 2022 while smishing attacks were launched against almost 100 organizations. The SIM swapping attacks from the previous article also happened in around the same period and seemed to have connections. Multiple groups started using the phishing kit to establish initial access and steal data. This attack is signified with the use of stolen data and compromised

infrastructure to launch attacks and targeting victims. Hence this group proved to be a significant threat to organizations even with good cyber defenses.

Camaro Dragon Hackers Strike with USB-Driven Self-Propagating Malware

(Early 2023)

A new strain of self-propagating malware was released that spreads through compromised USB drives. It is said to have started in a healthcare institution in Europe where an employee injected an infected USB drive that led to the spread of the infection to the institution's systems. The malware creates manipulates the files in the system, creating hidden folders. The primary payload of this drive is WispRider. It communicates with a remote server and tries to compromise any new USB drives that might be introduced into the system.

Twitter hacked; 200 million user email addresses leaked.

(December 2023)

A data collection auction containing more than 200 million Twitter profiles started on December 4th, 2023 for eight credits. The stolen data was made available in a 59 GB RAR bundle. The vulnerable API was compromised by the scrapers using earlier data harvesting. Users of Twitter should be aware of targeted phishing scam attempts. However, on November 27th, 2022, the collection became available for free. In November, it appeared that a second data dossier, purportedly holding information on 17 million people, was moving covertly. The vast data sets of scraped Twitter user accounts have been sold and shared by threat actors.

Tallahassee Memorial Hospital Cyber Attack

(January 2023)

A cyber-attack, that occurred in late January 2023 led Tallahassee Memorial Healthcare (TMH), a nonprofit health organization that serves patients in North Florida and South Georgia, to function for almost two weeks using emergency downtime protocols. The inquiry revealed that between January 26 and February 2, unauthorized users gained access to TMH's computers and exfiltrated material. Names, Social Security numbers, medical record and patient account numbers, addresses, dates of birth, insurance details, dates of services, treatment plans, diagnoses, visit notes, medication details, and physician names were all included in the stolen data. Affected patients at Tallahassee Memorial Hospital were provided free credit monitoring and identity theft prevention services after being made aware of the compromise on March 31. The hospital said that it did not think the cyberattack had any effect on how patients were treated.

Hotel Marriot breach

(2018)

Late in 2018, the Marriott hotel chain revealed that one of its reservation systems had been breached, allowing the attackers to steal hundreds of millions of client details, including credit card and passport numbers. Although Marriott has not yet provided the complete timing or technical details of the attack, what is known about it provides valuable information about the current threat environment and provides guidance for other businesses on how to stay safe. When a security tool detected an unexpected database query, Marriott initially realized they had been hacked. Analysis swiftly revealed that although the database query was performed by a user with administrator credentials, that user was not the one who did it; instead, someone else had managed to take control of that account.

Four SSRF Vulnerabilities in Azure Cloud Services

(2020)

Four Azure services were found vulnerable to SSRF: Azure API Management, Azure Functions, Azure Machine Learning and Azure Digital Twins. The Azure SSRF vulnerabilities allowed an attacker to scan local ports, find new services, endpoints, and files – providing valuable information on possibly vulnerable servers and services to exploit for initial entry and the location of potential information to target. The recently identified Azure SSRF flaws made it possible for an attacker to scan local ports, identify new services, endpoints, and files, giving them important information about potentially susceptible servers and services to use as a backdoor and the location of potential target information.

Scar Cruft Hackers Exploit Ably Service for Stealthy Wiretapping Attacks

ScarCruft, a North Korean threat actor, has been seen employing malware that steals data and includes previously unreported eavesdropping capabilities, as well as a backdoor made in Golang that takes use of the Ably real-time messaging service. The threat actor used the Ably service to send commands through the Golang backdoor. A GitHub repository held the API key value needed for command transmission. Although the gang has used a variety of different bespoke tools to gather sensitive information, their attack chains involve the use of spear-phishing lures to deploy RokRAT.

Twitter Hacker Sentenced to 5 Years in Prison for $120,000 Crypto Scam

(July 2020)

A British national who participated in the significant Twitter hack in July 2020 was given a five-year jail term in the United States. Joseph A little more than a month after entering a guilty plea to the criminal offences, James O'Connor (aka PlugwalkJoe), 24, was given the term on Friday in the Southern District of New York. His arrest took place in July 2021 in Spain. The infamous Twitter security breach gave the defendant and his accomplices access to Twitter's backend tools without authorization, which they used to take control of 130 well-known accounts and run a cryptocurrency fraud that brought in around $120,000 in unlawful gains.

Shields Health Care Group Data Breach

(April 2023)

The Shields Health Care Group, a supplier of medical services with a Massachusetts address, experienced the biggest data breach in April 2023. Near the end of the month, reports surfaced that a cybercriminal had accessed the organization's networks without authorization and had taken 2.3 million people's personal data with them. According to reports, the thieves had access to private information for two weeks, including patient Social Security numbers, dates of birth, home addresses, healthcare provider information, and medical histories.

Kubernetes Clusters Hacked

Two potential sites of attack were used: vulnerable images and PostgreSQL servers that were not properly setup. The goal of the assault is to mine cryptocurrencies and earn money. Kubernetes cluster security is a difficult task that must be finished. In order to get early access to Kubernetes systems, the threat actors behind the Kinsing Crypto Jacking operation have been seen leveraging unsecured and improperly configured PostgreSQL servers. Kinsing virus was created using Golang, a high-level programming language intended for creating cloud native apps. It is constructed with Go 1.13.6. This virus primarily targets Linux installations in order to mine cryptocurrencies. Once the virus has been successfully installed and is functioning on the victim's PC, the goal shifts to infiltrating additional computers.

PayPal Accounts Breached in large-scale Credential Stuffing Attack

(December 2022)

The company discovered the credential stuffing attack took steps to mitigate it, but it also launched an internal investigation to determine how the hackers gained access to the accounts. PayPal finished its investigation on December 20, 2022, and found that legitimate login information was used by unauthorized third parties to access the accounts. The electronic payment system asserts that there was no system breach, and there is no proof that the user credentials were taken directly from the users. 34,942 of PayPal's users have been impacted by the incident, according to the company's data breach reports. Hackers gained access to the complete names, birthdates, postal addresses, social security numbers, and unique tax identification numbers of account holders for the two days. On PayPal accounts, you may also see transaction histories, associated credit or debit card information, and information on PayPal invoices. According to PayPal, it acted swiftly to restrict the hackers' access to the system and reset the passwords of the accounts that were proven to have been compromised. The warning further states that no transactions from the compromised PayPal accounts have been attempted or successfully completed by the attackers.

Uber Blames LAPSUS$ Hacking Group for Security Breach

(September 2022)

When the City of London Police made the decision to detain seven people between the ages of 16 and 21 for their claimed ties to the group, the financially driven extortionist gang was struck a devastating blow in March 2022. Two of the young people are accused of fraud A hack into Rockstar Games over the weekend has also been attributed to the 18-year-old hacker known as Tea Pot, who is also responsible for the Uber attack. The company, which has its headquarters in Singapore, reported that at least two of Uber's staff members in Indonesia and Brazil had Raccoon and Vidar information-stealing viruses. The attacker subsequently made many attempts to access the contractor's Uber account, according to the business. "Each time, the contractor got a request for two-factor login approval, which at first prevented access. But eventually, the contractor gave in, and the attacker was able to log in. After establishing a footing, the thief allegedly gained access to the accounts of additional workers, giving the malevolent individual enhanced access to "several internal systems" like Google Workspace and Slack.

Cisco Hacked by Yanluowang Ransomware Gang

(August 2022)

On May 24, 2022, networking equipment giant Cisco acknowledged that it had been the target of a cyberattack after the attackers gained access to a worker's personal Google account, which had passwords synchronized from their online browser. According to a thorough report by Cisco Talos, the first access to the Cisco VPN was obtained through the successful hack of a Cisco employee's personal Google account. "The user had stored their Cisco login information in their browser and enabled password syncing via Google Chrome, enabling that information to synchronize to their Google account." The information was released while cybercriminals connected to the Yanluowang ransomware group posted a list of the compromised files on their data dump website on August 10.

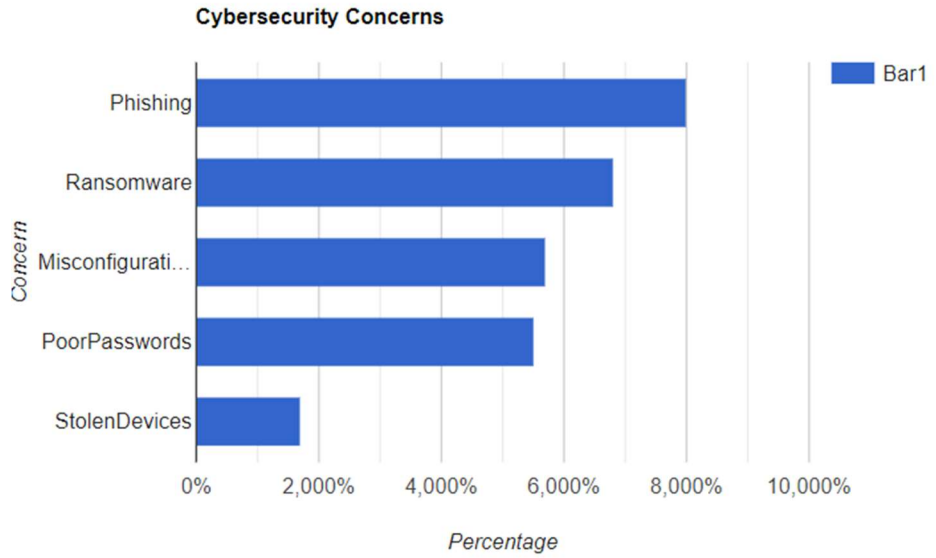

Fig 1.3. Cybersecurity Concern Analytics

APPLICATIONS

Cybersecurity, cybercrime, and cyberattack awareness can greatly help people in their daily lives and businesses in a variety of ways.

For individuals:

1. Protection of Personal Information: People are better able to appreciate the value of protecting their personal information when they are aware of cybersecurity and cybercrime. Armed with this information, users may create secure passwords, enable two-factor authentication, stay away from dubious links and attachments, and access secure online services. People can lessen their risk of becoming a victim of identity theft, financial fraud, or other personal data breaches by exercising vigilance and caution.
2. Attacks on social engineering are preventable because they rely on tricking people into disclosing sensitive information or taking activities that jeopardise security, including phishing or impersonation frauds. Understanding these strategies enables people to spot and defend against such attacks. They are able to see warning signs in dubious emails, calls, or online inquiries and can avoid giving out sensitive information or clicking on harmful sites.
3. Safe Online Shopping and Financial Transactions: Being aware of cyber dangers can assist people in making educated decisions while conducting online business. People can safeguard their financial information and prevent falling victim to scams by recognising secure website signs (such as HTTPS and lock symbols), confirming the legality of e-commerce platforms, and using secure payment methods.
4. Protection Against Malware and Ransomware: Malware and ransomware are serious online threats that can attack mobile and computer systems, encrypt files, and demand a fee to decrypt them. Understanding these hazards makes people realise how important it is to use reliable antivirus software, update software frequently, and stay away from dubious downloads and websites. This knowledge aids in avoiding infections and possible data loss.
5. Enhanced Data Privacy: People are more likely to preserve their privacy when they are aware of cybersecurity issues. People can better keep control over their personal data if they are aware of the significance of data privacy settings on social media platforms, the dangers of oversharing personal information, and the significance of reading and understanding privacy regulations.
6. Protecting Personal Devices: By being aware of cybersecurity issues, people may safeguard their computers, cell phones, and tablets. People can reduce the risk of device compromise and unauthorised access to their personal information by being aware of the hazards connected with public Wi-Fi networks, using safe surfing techniques, and frequently updating device software.
7. Cybersecurity awareness provides parents and guardians with information on how to keep their children safe online. They can instruct their kids on how to behave safely online, the dangers of providing personal information, and the necessity of reporting any questionable activity. Children can be shielded from predators, unsuitable information, and cyberbullying by having a safe environment online thanks to awareness.

8. Protecting Against Social Media Threats: By being more cyber-aware, people can better comprehend the dangers posed by social media platforms. They can take security steps, manage their privacy settings, restrict the sharing of personal information, and refrain from accepting requests from shady or unauthorised accounts. Identity theft, social engineering attempts, and cyberstalking are less likely as a result.

For businesses:

1. Strengthened Security Measures: Companies that are more security conscious and educate their personnel about potential dangers and recommended practises tend to have stronger security measures. As a result, strong security mechanisms including firewalls, intrusion detection systems, encryption protocols, and access controls are put in place. When it comes to spotting and reporting potential security breaches, employees take a proactive role in defence.

2. Improved Incident Response: Companies can build effective incident response procedures with the support of cybersecurity knowledge. Employees that are knowledgeable about typical attack routes, phishing tricks, and indicators of a potential breach can report instances to the proper channels right once. This makes it possible for businesses to react quickly, lessen losses, and lessen the effects of cyberattacks.

3. Sensitive Data Protection: Companies can secure their sensitive data by being aware of cyberthreats. Employees can handle sensitive information more responsibly if they are aware of the value of data classification, secure data storage, and secure data transport methods. Data breaches, unauthorised access, and data loss are less likely as a result.

For companies:

1. Enhanced Cybersecurity Awareness Programmes: These programmes give staff members the instruction and information they need to identify and respond to potential cyber-attacks. Employees are kept up to date on new threats, best practises, and their roles and responsibilities in maintaining a secure work environment through regular training sessions, workshops, and awareness campaigns.
2. Protection of Intellectual Property and Trade Secrets: Companies may protect their intellectual property, trade secrets, and confidential information by becoming more knowledgeable about cybersecurity. Companies may safeguard their priceless assets from theft or unauthorised disclosure by teaching staff about the value of intellectual property, the dangers of data breaches, and the significance of effective access controls and encryption.
3. Protection of Reputation and Trust: A cybersecurity event may have a negative impact on a company's standing with clients and undermine their trust. The knowledge of cyber dangers motivates businesses to prioritise cybersecurity, put in place effective security measures, and show a dedication to protecting consumer data. Companies may uphold their reputation and inspire confidence in their stakeholders by maintaining a robust security posture.

4. Compliance with Data Protection rules: Companies can maintain compliance with pertinent data protection rules, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA), by being aware of cybersecurity and privacy standards. Companies can assure the legal and moral treatment of personal data, avoiding legal repercussions and financial penalties, by knowing the demands and obligations imposed by these standards.

In conclusion, a person's ability to protect their personal information, avoid online fraud, and uphold a secure online presence is empowered by cybersecurity awareness. As a result of increased awareness, businesses may take stronger security precautions, respond to incidents better, and protect sensitive data, eventually protecting their reputation and adhering to legal requirements.

RESULTS & CONCLUSIONS

A thorough strategy that incorporates technological controls, best practises, policies, and a strong security culture inside an organisation is needed to ensure cybersecurity. Here are some strategies for preserving our safety and privacy:

Strong Passwords and Authentication: As we saw previously, it is strongly advised to use strong, one-of-a-kind passwords for all accounts and systems. By demanding additional verification beyond passwords, multi-factor authentication (MFA) implementation offers an additional degree of protection. Employees should be taught the proper password practises, which include avoiding obvious or simple passwords and updating them frequently.

Risk Assessment and Management: Regular risk assessments to find vulnerabilities, threats, and possible effects on your systems, networks, and data are necessary for risk management. Prioritise risks based on their likelihood and possible impact, and create a risk management strategy to effectively handle them. As the threat landscape changes, make sure to maintain continual monitoring and update risk assessments.

Firewall and Network Security: To monitor and manage incoming and outgoing network traffic, deploy, and maintain firewalls, intrusion detection systems, and other network security measures. Firewall rules should be regularly reviewed and updated to reflect evolving business demands and security requirements.

Regular Software upgrades and Patch Management: We can fail to keep all software, operating systems, and apps current with the most recent security patches and upgrades. However, it is crucial to make sure that all the software is current and that the system is impenetrable by hackers or other attackers. When practicable, enabling automated updates can provide prompt protection against known vulnerabilities.

Secure Data handling and backup: To prevent unauthorised access, encrypt sensitive data both in transit and at rest. To guarantee that data can be restored in the case of a breach, a data loss disaster, or even during DOS assaults, implement frequent data backup practises. Processes for data restoration should be tested routinely to ensure their efficacy.

Penetration testing and periodic security audits: Perform routine security audits to assess the efficacy of security controls, policies, and processes. Conduct penetration testing to find systems' and networks' flaws and vulnerabilities so that they may be quickly fixed.

FUTURE SCOPE

Cybersecurity is a vast and evolving field and relies more on the growing technology. There are various enhancements and growths that can be done in this field including the growing sophistication of cyber threats. Prediction and detection of threat can be done using artificial intelligence and machine learning techniques. These systems can go through and analyse huge amounts of data and identify patterns and hence, help detecting any possible attacks. Machine learning algorithms can accurately detect intrusions and even in behavioural analytics. Further data security has to be ensured especially in those organisations that use cloud services for data storage. Data encryption and real-time threat monitoring can be developed and paid more attention to.

Internet of Things is one of the growing fields of technology that are implemented almost everywhere. Securing the data and the interconnected network of devices. Development of robust security frameworks and device authentication protocols for IoT environments can be focused on in the future. It can also be used in enhancement of blockchain security and cryptocurrency wallet protection. It must ensure privacy of the transaction. Analytica on cybersecurity can help identifying and predicting attacks and threats that are most likely to occur. More sophisticated tools and techniques can be used in ethical hacking and red teams. The field of cybersecurity must be able to adapt to new and growing technologies and environments and must be able to protect the data and privacy of the users even with the advanced technologies and software. Hence, future of cybersecurity is vast and can keep growing as it has a wide range of opportunities and paths of development and is of at most importance for any organization or even an individual.

References

- https://blog.usecure.io/5-ways-your-users-can-stay-safe-when-using-public-wifi#:~:text=Use%20a%20VPN%20(virtual%20private%20network)%20when%20you%20use%20public%20WiFi&text=A%20virtual%20private%20network%20will,before%20connecting%20to%20the%20internet.
- https://blog.symquest.com/steps-to-implement-a-cyber-security-awareness-training-program-at-your-company
- https://portswigger.net/web-security/sql-injection
- https://www.byos.io/blog/denial-of-service-attack-prevention#:~:text=IP%20blocking%20%2D%20Blocking%20traffic%20from,DoS%20attack%20from%20overwhelming%20it.
- https://blog.usecure.io/7-key-steps-to-implement-security-awareness-training
- https://clouddocs.f5.com/training/community/firewall/html/class2/dns4.html
- https://www.kelsercorp.com/blog/cybersecurity-training-must-haves#:~:text=The%203%20non%2Dnegotiable%20elements,that%20a%20human%20firewall%20provides.

- https://thehackernews.com/2023/06/twitter-hacker-sentenced-to-5-years-in.html
- https://thehackernews.com/2022/09/uber-blames-lapsus-hacking-group-for.html
- https://thehackernews.com/2022/08/cisco-confirms-its-been-hacked-by.html