INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1416-1430

CYBER SECURITY: THE FUTURE OF CYBER WARFARE

Anjali Jain[1], Achman Saxena[2], Anshul Bhatt[3], Dr. Deepshikha Aggarwal[4]

[1,2,3]Jagan Institute of Management, Institutional Area, Sector - 5, Rohini, Delhi – 110085, India.

[4]Guide: Jagan Institute of Management, Institutional Area, Sector - 5, Rohini, Delhi – 110085, India.

ABSTRACT

Cyber Security plays an important role in the field of information technology. Securing the information have become one of the biggest challenges in the present day. Whenever we think about the cyber security the first thing that comes to our mind is 'cyber crimes' which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cybercrimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies. It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security.

Keywords: Cyber Security, Cybercrime, Cyber Ethics, Social Media, Cloud Computing, Android Apps.

1. INTRODUCTION

Today Internet is the fastest growing infrastructure in everyday life. In today's technical environment many latest technologies are changing the face of the mankind. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence these days cybercrimes are increasing day by day. Today more than 60 percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. Hence cyber security has become a latest issue

Even the latest technologies like cloud computing, mobile computing etc. also needs high level of security. Since these technologies hold some important info. regarding a person their security has become a must thing. Enhancing cyber security and protecting critical information infrastructures are essential toeach nation's security and economic wellbeing.

Making the Internet safer has become integral to the development of new services as well as governmental policy. The fight against cybercrime needs a comprehensive and a safer approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cyber-crime effectively. Today many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of some important information. Every individual must also be trained on this cyber security and save themselves from these increasing cyber crimes

Cyber-attack is now an international concern that hacks the system, and other security attacks could endanger the global economy. Therefore, we protect sensitive information from high profile security breaches.

Furthermore, as the volume of cyber-attacks grows, companies and organizations deal with information related to security, health, or financial records, need to use strong cybersecurity measures and processes to protect their sensitive and personal information.

CYBER SECURITY

Privacy and security of the data will always be top security measures that any organization takes care. We are presently living in a world where all the information is maintained in a digital or a cyber form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. Not only social networking but also during bank transactions a person must take all the required security measures.

Incidents	Jan- June 2012	Jan- June 2013	% Increase/ (decrease)
Fraud	2439	2490	2
Intrusion	2203	1726	(22)
Spam	291	614	111
Malicious code	353	442	25
Cyber Harassment	173	233	35
Content related	10	42	320
Intrusion Attempts	55	24	(56)

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1416-1430

Denial of services	12	10	(17)
Vulnerability reports	45	11	(76)
Total	5581	5592	

echnology and healthcare executives nationwide, Silicon Valley Bank found that companies believe cyber-attacks are a serious threat to both their data and their business continuity.

- 98% of companies are maintaining or increasing their cyber security resources and of those, half are increasing resources devoted to online attacks this year
- The majority of companies are preparing for when, not if, cyber- attacks occur
- Only one-third are completely confident in the security of their information and even less confident about the security measures of their business partners.

There will be new attacks on Android operating system-based devices, but it will not be on massive scale. The fact tablets share the same operating system as smart phones means they will be soon targeted by the same malware as those platforms. The number of malware specimens for Macs would continue to grow, though much less than in the case of PCs. Windows 8 will allow users to develop applications for virtually any device (PCs, tablets and smart phones) running Windows 8, so it will be possible to develop malicious applications like those for Android, hence these are some of the predicted trends in cyber security.

Table 1

The above Comparison of Cyber Security Incidents reported to Cyber999 in Malaysia from January– June 2012 and 2013 clearly exhibits the cyber security threats. As crime is increasing even the security measures are also increasing. According to the survey of U.S.

Cloud Computing and its Services

These days all small, medium and large companies are slowly adopting cloud services. In other words, the world is slowly moving towards the clouds. This latest trend presents a big challenge for cyber security, as traffic can go around traditional points of inspection. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve in order to prevent the loss of valuable information. Though cloud services are developing their own models still a lot of issues are being brought up about their security. Cloud may provide immense opportunities but it should always be noted that as the cloud evolves so as its security concerns increase.

APT's and Targeted attacks

APT (Advanced Persistent Threat) is a whole new level of cybercrime ware. For years network security capabilities such as web filtering or IPS have played a key part in identifying such targeted attacks (mostly after the initial compromise). As attackers grow bolder and employ more vague techniques, network security must integrate with other security services in order to detect attacks. Hence one must improve our security techniques in order to prevent more threats coming in the future.

Mobile Networks

Today we are able to connect to anyone in any part of the world. But for these mobile network's security is a very big concern. These days firewalls and other security measures are becoming porous as people are using devices such as tablets, phones, PC's etc. all of which again require extra securities apart from those present in the applications used. We must always think about the security issues of these mobile networks.

Further mobile networks are highly prone to these cybercrimes So, a lot of care must be taken in case of their security issues.IPv6: New internet protocol

IPv6 is the new Internet protocol which is replacing IPv4 (the older version), which has been a backbone of our networks in general and the Internet at large. Protecting IPv6 is not just a question of porting IPv4 capabilities. While IPv6 is a wholesale replacement in making more IP addresses available, there are some very fundamental changes to the protocol which need to be considered in security policy. Hence it is always better to switch to IPv6 as soon as possible in order to reduce the risks regarding cybercrime.

Encryption of the code

Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it. In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with th use of an encryption key, which specifies how the message is to be encoded. Encryption at a very beginning evel protects data privacy and its integrity.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1416-1430

But more use of encryption brings more challenges in cyber security. Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercoms etc. Hence by encrypting the code one can know if there is any leakage of information.

Cyber Security Elements

The cybersecurity field can be broken down into several different sections, the coordination of which within the organization is crucial to the success of a cybersecurity program.

These sections include the following:

- Application security
- Information or data security
- Network security
- Disaster recovery and business continuity planning
- Operational security
- Cloud security
- Critical infrastructure security
- Physical security
- End-user education

Maintaining cybersecurity in a constantly evolving threat landscape is a challenge for all organizations. Traditional reactive approaches, in which resources were put toward protecting systems against the biggest known threats while lesser-known threats were undefended, are no longer a sufficient tactic. To keep up with changing security risks, a more proactive and adaptive approach is necessary. Several key cybersecurity advisory organizations offer guidance. For example, the National Institute of Standards and Technology (NIST) recommends adopting continuous monitoring and real-time assessments as part of a risk assessment framework to defend against known and unknown threats.

Challenges

Cybersecurity is continually challenged by hackers, data loss, privacy, risk management and changing cybersecurity strategies. And the number of cyberattacks isn't expected to decrease anytime soon. Moreover, increased entry points for attacks, such as the internet of things and the growing attack surface, increase the need to secure networks and devices.

The following major challenges must be continuously addressed.

Evolving threats

One of the most problematic elements of cybersecurity is the evolving nature of security risks.

As new technologies emerge and as technology is used in new or different ways, new attack avenues are developed.

Keeping up with these frequent changes and advances in attacks, as well as updating practices to protect against them, can be challenging. Issues include ensuring all elements of cybersecurity are continually updated to protect against potential vulnerabilities. This can be especially difficult for smaller organizations that don't have adequate staff or in-house resources.

Data deluge

Organizations can gather a lot of potential data on the people who use their services. With more data being collected comes the potential for a cybercriminal to steal personally identifiable information (PII). For example, an organization that stores PII in the cloud could be subject to a ransomware attack

Cybersecurity awareness training

Cybersecurity programs should also address end-user education. Employees can accidentally bring threats and vulnerabilities into the workplace on their laptops or mobile devices. Likewise, they might act imprudently -- for example, clicking links or downloading attachments from phishing emails Regular security awareness training can help employees do their part in keeping their company safe from cyberthreats.

Workforce shortage and skills gap

Another Cybersecurity challenge is a shortage of qualified cybersecurity personnel. As the amount of data collected and used by businesses grows, the need for cybersecurity staff to analyze, manage and respond to incidents also increases. In 2023, cybersecurity association ISC2 estimated the workplace gap between needed cybersecurity jobs and security professionals at 4 million, a 12.6% increase over 2022.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1416-1430

Cyber Security Vendors and Tools

Vendors in the cybersecurity field offer a variety of security products and services that fall into the following categories:

- IAM
- Firewalls
- Endpoint protection
- Antimalware and antivirus
- Intrusion prevention systems and detection systems
- Data loss prevention
- Endpoint detection and response
- Security information and event management
- Encryption
- Vulnerability scanners
- Virtual private networks
- Cloud workload protection platform
- Cloud access security broker

Examples of cybersecurity vendors include the following:

- Check Point Software
- Cisco
- Code42 Software Inc
- CrowdStrike
- FireEye
- Fortinet
- IBM
- Imperva
- KnowBe4, Inc
- McAfee
- Microsoft
- Palo Alto Networks
- Rapid7
- Cyber Attacks

Cyberattacks can target a wide range of victims from individual users to enterprises or even governments. When targeting businesses or other organizations, the hacker's goal is usually to access sensitive and valuable company resources, such as intellectual property (IP), customer data or payment details.

Malware, Denial of Service, Phishing, Spooling, code injection attacks. Malware

Malware or malicious software — is any program or code that is created with the intent to do harm to a computer, network or server. Malware is the most common type of cyberattack, mostly because this term encompasses many subsets such as ransomware, trojans, spyware, viruses, worms, keyloggers, bots, crypto jacking, and any other type of malware attack that leverages software in a malicious way.

- **Denial-of-Service Attacks**

  In a DoS attack, users are unable to perform routine and necessary tasks, such as accessing email, websites, online accounts or other resources that are operated by a compromised computer or network. While most DoS attacks do not result in lost data and are typically resolved without paying a ransom, they cost the organization time, money and other resources in order to restore critical business operations.

- **Phishing**

  Phishing is a type of cyberattack that uses email, SMS, phone, social media, and social engineering techniques

  It is used to entice a victim to share sensitive information such as passwords or account numbers or to download

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1416-1430

a malicious file that will install viruses on their computer or phone.

- **Spoofing**

  Spoofing is a technique through which a cybercriminal disguises themselves as a known or trusted source. In so doing, the adversary is able to engage with the target and access their systems or devices with the ultimate goal of stealing information, extorting money or installing malware or other harmful software on the device.

- **Code Injection Attacks**

  Code injection attacks consist of an attacker injecting malicious code into a vulnerable computer or network to change its course of action.

- **Cyber Security Threats**

  Malicious Software

  A computer user can be forced sometimes to download a software onto a computer that is of malicious intent. Such software comes in many forms, such as viruses, Trojan horses, and worms.

VIRUS- It is the type of malicious software that, when executed replicates itself by modifying other computer programs. Computer viruses causes economic damage due to system failure, corrupting data,increasing maintenance cost etc.

TROJAN HORSE- A TROJAN HORSE, commonly known as a Trojan. **It is a name for malicious software that tends to be harmless, so that a user by will allows it to be downloaded onto the computer.**

Trojan allow an attacker to hack user's personal information such as banking information, email passwords, personal identity. It also affects other devices connected to the network.

1 Virus

➢ **Malware**

MALWARE is a term short for malicious software, used to destroy computer operation, gather very sensitive information, or gain access to private computer systems.

A computer worm is a standalone malware computer program that replicates itself in order to spread to another computer. Many worms are designed only to spread, and do not attempt to change the systems they pass through.

Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency. The term malware is sometimes used for bad malware and unintentionally harmful software.

2 Internet Security Products

- **ANTIVIRUS**

  Antivirus software and internet security programs are able to project a programmable device from attack by detecting and eliminating the viruses. Antivirus software was used in the early years of internet but now with the development several free security applications are available on internet.

- **PASSWORD MANAGERS**

  The password managers is a software application that is used to store and organize the passwords. Password managers usually store passwords encrypted, requiring the person to create a master password; a single, ideally a very strong password which allows the user access to their entire password database.

- **SECURITY SUITS**

  The security suits contain the suits of firewalls, anti-virus, anti-spyware and many more. They also give the theft protection, portable storage device safety check, private internet browsing or make security related decisions and are free of charge.

- **Security Tokens**

  Some online sites offer the users the ability to use the six-digit code which randomly changes after every 30-60 seconds on a security token. The keys on the token have built computations and manipulated numbers based on the current time built into the device. This means that after every thirty seconds there is only a certain sequence of numbers possible which would be correct to access to the online account.

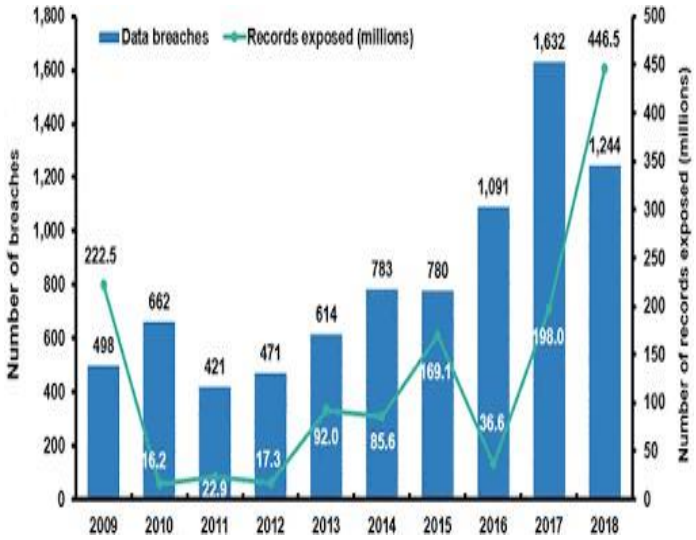
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1416-1430



Worldwide cybersecurity spending is estimated to pass $133 billion by 2020.

1. In 2019, over 4 billion records were exposed due to data breaches.
2. Every 39 seconds a hacker attack occurs, which averages out to be around 2244 times in a single day.
3. By 2020, 83% of enterprise workloads will be transferred to the cloud.
4. 94% of malware attacks are delivered to their target via email.
5. On average, the cost of a ransomware attack comes out to $133,000 for businesses.
6. Of all data breach victims, 43% are small businesses.
7. During 2018, most cybercrimes were directed at the banking industry, incurring a cost of over $18 million.
8. It is estimated that the damage caused by cybercrime is going to hit $6 trillion a year by 2021.
9. Data breaches on average cost $3.9 million.

Impact of COVID-19 on Cyber Security

The COVID-19 pandemic has had significant impacts on cybersecurity across various sectors.

Some key ways that affected Cybersecurity:

1. Increased Cyber Threats- Cybercriminals have exploited the chaos and uncertainty surrounding the pandemic to launch various cyberattacks. Phishing attacks malware campaigns, and ransomware attacks have surged often using COVID-19-related themes to lure victims

2. **Remote Work Challenges**:

With the rapid shift to remote work, organizations faced challenges in securing remote access and ensuring the cybersecurity of home networks and devices. This has led to an increase in vulnerabilities and potential entry points for cyberattacks.

3. Healthcare Sector Targeted:

The healthcare sector has been particularly targeted during the pandemic. Cybercriminals have launched attacks on hospitals, medical research facilities, and pharmaceutical companies, aiming to disrupt operations or steal sensitive data related to COVID-19 research and patient information.

4. Supply Chain Disruptions:

The pandemic has disrupted global supply chains, impacting the availability of hardware, software, and cybersecurity services. This disruption has affected organizations' ability to implement robust cybersecurity measures and updates.

5. Increased Demand for Cybersecurity Solutions:

The heightened threat landscape and the shift to remote work have led to increased demand for cybersecurity solutions and services. Organizations are investing in technologies such as endpoint security, cloud security, and virtual private networks (VPNs) to bolster their defenses.

6. Regulatory Changes:

Regulatory bodies have responded to the cybersecurity challenges posed by the pandemic by introducing new guidelines and regulations. These measures aim to enhance cybersecurity resilience and protect sensitive data, particularly in critical sectors such as healthcare and finance.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1416-1430

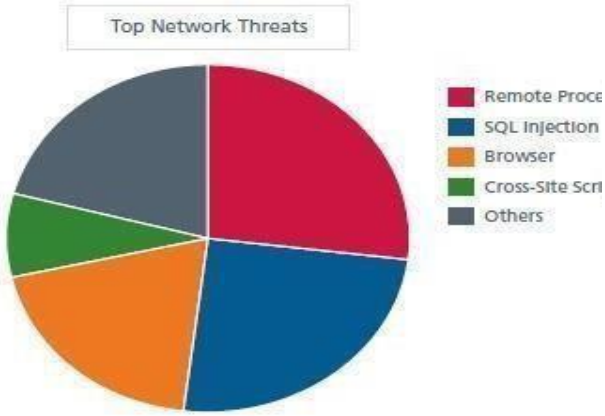
2. METHODOLOGY

The methodology of cybersecurity involves a systematic approach to protecting computer systems, networks, and data from unauthorized access, attacks, and other security threats.

It typically consists of the following key steps:

1. **Risk Assessment:**

   Identify and assess potential risks and vulnerabilities to determine the level of security required. This involves analyzing the value of assets, p o t e n t i a l t h r e a t s , a n d t h e likelihood of attacks or incidents.



   The above pie chart shows about the major threats for networks and cyber security.

2. **Security Policy Development:** Establish a comprehensive security policy that outlines the organization's goals, guidelines, and procedures for ensuring information security. This policy should align with industry standards and regulatory requirements.
3. **Access Control:**

   Implement mechanisms to control and restrict access to systems, networks, and data.

   This includes authentication mechanisms such as passwords, biometrics, and two- factor authentication, as well as authorization controls to grant appropriate access privileges to users.
4. **Security Awareness and Training:** Educate employees and users about security best practices, potential risks, and their responsibilities in maintaining a secure environment Regular training sessions can help raise awareness and reduce the likelihood of human error- related security incidents.
5. **Vulnerability Management:**

   Regularly scan systems and networks for vulnerabilities, such as outdated software, misconfigurations, or unpatched vulnerabilities. Vulnerability assessments and penetration testing can help identify weaknesses and address them before they are exploited.
6. **Threat Detection and Monitoring:**

   deploy prevention systems (IDPS), firewalls, antivirus software, and security information and event management (SIEM) solutions, to monitor network traffic, detect suspicious activities, and respond to security incidents in real-time.
7. **Incident Response:**

   Develop an incident response plan that outlines the steps to be taken in the event of a security breach or incident. This plan should include procedures for containment, eradication, recovery, and post-incident analysis to minimize damage and learn from the incident.
8. **Continuous Improvement:**

   Regularly review and update security measures, policies, and procedures based on emerging threats, technological advancements, and lessons learned from incidents. Implementing a cycle of continuous improvement helps ensure that cybersecurity practices remain effective and up-to-date.
9. **Compliance and Regulation:** Comply withrelevant laws, regulations, and industry standards pertaining to cybersecurity, such as the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), or ISO/IEC 27001. Regular audits and assessments can help ensure adherence to these requirements.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

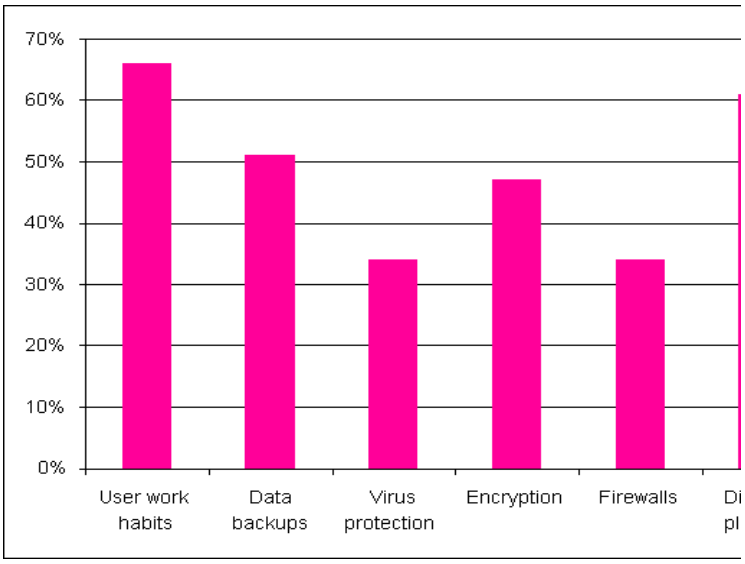
www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1416-1430

10. **Security Culture:** Foster a security- conscious culture within the organization, where security is considered a priority at all levels. This includes promoting a sense of responsibility, accountability, and vigilance among employees and stakeholder.
11. **Security Policy Development:** Establish a comprehensive security policy that outlines the organization's goals, guidelines, and procedures for ensuring information security. This policy should align with industry standards and regulatory requirements.
12. **Access Control:** Implement mechanisms to control and restrict access to systems, networks, and data. This includes authentication mechanisms such as passwords, biometrics, and two-factor authentication, as well as authorization controls to grant appropriate access privileges to users.
13. **Security Awareness and Training:** Educate employees and users about security best practices, potential risks, and their responsibilities in maintaining a secure environment. Regular training sessions can help raise awareness and reduce the likelihood of human error security incidents.
14. **Vulnerability Management:** Regularly scan systems and networks for vulnerabilities, such as outdated software, misconfigurations, or unpatched vulnerabilities. Vulnerability assessments and penetration testing can help identify weaknesses and address them before they are exploited.
15. **Threat Detection and Monitoring:** Deploy security tools and systems, such as intrusion detection and prevention systems (IDPS), firewalls, antivirus software, and security information and event management (SIEM) solutions, to monitor network traffic, detect suspicious activities, and respond to security incidents in real-time.
16. **Incident Response:**

    Develop an incident response plan that outlines the steps to be taken in the event of a security breach or incident. This plan should include procedures for containment, eradication, recovery, and post-incident analysis to minimize damage and learn from the incident.
17. **Continuous Improvement:** Regularly review and update security measures, policies, and procedures based on emerging threats, technological advancements, and lessons learned from incidents. Implementing a cycle of continuous improvement helps ensure that cybersecurity practices remain effective and up-to-date.
18. **Compliance and Regulation:** Comply with relevant laws, regulations, and industry standards pertaining to cybersecurity, such as the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), or ISO/IEC 27001. Regular audits and assessments can help ensure adherence to these requirements.
19. **Security Culture:** Foster a security- conscious culture within the organization, where security is considered a priority at all levels. This includes promoting a sense of responsibility, accountability, and vigilance among employees and stakeholders. It's important to note that cybersecurity is an ongoing process and requires a holistic approach that combines technical measures, policies, and user awareness.

Organizations must adapt their methodologies to address new and evolving threats in the ever-changing landscape of cybersecurity.



INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1416-1430

3. BACKGROUND STUDY

The study of cybercrime, also known as cybercriminalistics or cybercriminal, involves understanding various aspects of criminal activities committed using computer networks, the internet, and digital technologies. It encompasses the analysis, prevention, investigation, and prosecution of cyber-related offenses.

Here's a background study of cybercrime:

1. **Definition:**

   Cybercrime refers to criminal activities that involve computers, networks, or digital devices as either the target or the tool of the crime. It encompasses a wide range of offenses, including hacking, identity theft, online fraud, data breaches, malware distribution, cyberstalking, and more.

2. **Evolution of Cybercrime:**

   Cybercrime has evolved alongside advancements in technology and the widespread use of the internet. It has become more sophisticated, organized, and pervasive, with criminals leveraging various techniques to exploit vulnerabilities and target individuals, businesses, and even governments.

3. **Types of Cybercrime:**

   Cybercrime can be categorized into various types based on the nature of the offense.

Some common types include:

1. **Hacking and Unauthorized Access:** Gaining unauthorized access to computer systems or networks to steal data, disrupt services, or cause damage.
2. **Identity Theft:** Illegally obtaining and using someone's personal information, such as social security numbers or financial details, for fraudulent purposes.
3. **Phishing and Social Engineering:** Using deceptive techniques, often through email or other communication channels, to trick individuals into revealing sensitive information or performing harmful actions.
4. **Online Fraud:** Engaging in fraudulent activities, such as online scams, fake auctions, or credit card fraud, to deceive victims and unlawfully obtain money or goods.
5. **Malware and Ransomware:** Distributing malicious software or encrypting files on victims' devices and demanding ransom payments to restore access or prevent data leaks.
6. **Cyberstalking and Harassment:** Engaging in persistent, unwanted online behavior to intimidate, harass, or threaten individuals.
7. **Data Breaches:** Unauthorized access, theft, or disclosure of sensitive information stored by organizations or individuals.
8. **Cyberterrorism:** Using technology to disrupt critical infrastructure, cause fear, or coerce governments or organizations for political or ideological purposes.

- **Impact and Consequences** Cybercrime has significant societal and economic impacts. It can result in financial losses, reputational damage, privacy breaches, and psychological harm to individuals and organizations. Furthermore, cybercriminals can exploit stolen data for further criminal activities or sell it on the dark web, perpetuating the cycle of cybercrime.
- **Prevention and Investigation** Combating cybercrime requires a multi- faceted approach involving prevention, detection, and investigation. This includes implementing robust cybersecurity measures, educating individuals and organizations about online threats, developing effective legislation, fostering international cooperation, and training law enforcement agencies in digital forensics and cybercrime investigation techniques.
- **Legal Framework:** Countries around the world have developed legislation and frameworks to address cybercrime. Examples include the United States' Computer Fraud and Abuse Act (CFAA), the European Union's General Data Protection Regulation (GDPR), and the Council of Europe's Budapest Convention on Cybercrime. These laws aim to provide a legal basis for prosecuting cybercriminals and facilitating international cooperation in combating cyber threats.
- **Emerging Challenges:** As technology continues to advance, new challenges in cybercrime emerge. These include the rise of artificial intelligence (AI) and machine learning- based attacks, the Internet of Things (IoT) vulnerabilities, the exploitation of cryptocurrencies for illicit activities, and the growing sophistication of cybercriminals using advanced evasion techniques.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1416-1430

The study of cybercrime is a dynamic and evolving field that requires interdisciplinary knowledge in computer science, law, criminology, psychology, and cybersecurity. Researchers, law enforcement agencies, and cybersecurity professionals continuously work.

- **Domains of Cyber Security Domain 1: Security Management**

Security management involves people and processes.

It includes:

- Risk assessment and drawing methods to fight against these risks.
- Ensuring security functions align with businesses operations and processes
- Having management procedures and processes in place
- User security awareness training
- Domain 2: Identity and Access

Management

Also known as IAM, Identity and Access Management enables the processes, systems, and procedures to handle authentication, assign characters, and manage access control. Each user and system are assigned unique names and there is a method in place for users to prove their identity.

Domain 3: Security Engineering Security engineering includes network security and computer operations security.

It involves:

- Firewalls
- Router and Switch Security
- Email Filtering
- Vulnerability Scanning
- Intrusion Detection and Prevention System
- Host-based Security Tools

Domain 4: Business Continuity Business continuity is all about attempting to restore business operations after a catastrophic event like a natural disaster. It involves disaster recovery and business continuity plans and procedures that need to be periodically reviewed.

Understanding the functions of the organization can help introduce certain systems to ensure quick and effective solutions with as little loss of data as possible.

Domain 5: Compliance

Compliance plays a crucial role in security management by ensuring that an organization has appropriate security controls. Additionally, it is also essential to be in line with the legislation and regulations that are applicable to the organization.

Compliance involves understanding and implementing regulations, internal audits, and third-party domains.

Domain 6: Cryptography

Cryptography protects the CIA and non- repudiation of information. It is in conjunction with compliance and security management

Domain 7: Physical Security

Physical security is the control that is applied to the physical hardware that one is concerned with. Some examples of physical security can be ensuring security guards at every entrance, the right fencing at entry and exit points, a secure data center that allows physical access to only authorized individuals, etc.

Cyber Security Professionals

Cyber Security Analyst

Cyber Security Analysts are responsible for planning, designing, and implementing security measures and controls. They are in charge of monitoring the security access as well as conducting internal and external audits to ensure that no potential threats to the network security exist.

Following are some of the other job responsibilities of a Cyber Security Analyst:

- Risk analysis
- Vulnerability testing

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1416-1430

- Security assessments
- Network management
- Employee capacity building
- Building awareness on best practices

According to Indeed, the average annual salary of a Cyber Security Analyst is ₹768346 in India and can go up to a few crores depending on the performance and outcome delivery. There are over 2,000 Cyber Security Analyst jobs listed in India on LinkedIn.

Chief Information Security Officer Appointing a Chief Information Security Officer has become a growing trend in businesses. Given the increasing threats to cyber security in this exponential growing global economy, it is only natural to designate a CISO that can align the cyber security plan with the vision, technology, and operations of the business.

The CISO has a standard process of identification, development, implementation, and maintenance of organizational processes to avoid any kind of security breach. They are in charge of drafting and reviewing the security policies and risk mitigation plans of a company.

A CISO earns an average salary of a whopping ₹2,240,648 per year as per PayScale and can go even up to ₹40,000,000 p.a. LinkedIn has listed 300+ job openings for CISO professionals in India.

4. NETWORK SECURITY ENGINEER

The Network Security Engineer is there to ensure the operational smoothness of a business.

The main responsibilities of this job are:

- Identifying vulnerabilities
- Overseeing the maintenance of firewalls, network monitoring tools, VPNs, routers, switches
- System maintenance
- Improving automation

According to Glassdoor, a Network Security Engineer earns about ₹696,250 p.a. as the average annual salary in India. There are over 2,000 Network Security Engineer jobs available in India according to LinkedIn.

Cyber Security Manager

The Cyber Security Manager manages the security protocols of an organization.

They are involved with the strategizing processes for the improvement of data and network security. These managers handle an entire team of IT professionals who work day and night to optimize the data management and security protocols and systems.

Cyber Security Managers perform crucial research when it comes to the latest cyber threat trends that drive the drafting of security policies in a company.

The average compensation of Cyber Security Managers is about ₹2,195,801 p.a. Salaries are subject to increase depending on performance. Over 1,000 Cyber Security Manager jobs are listed on LinkedIn in India.

Security Architect

Security Architects design the complete network and computer security architecture. They plan and design the different elements that are involved in security. Security Architects are instrumental when it comes to recommending changes, security policies, and protocols.

- **Skills to Become a Cybersecurity Professional**
  - **Technical Skills**

- Most firms look for cyber security professionals who possess one or more of the following technical skills:
- Networking and System Administration
- IoT
- Operating Systems and Virtual Machines
- Cryptography
- Virtualization Network Services and Security

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1416-1430

- Network Security Control
- Coding
- Cloud Security
- Windows Server
- Soft Skills

Although soft skills may not seem as important as domain knowledge, given the widening scope of cyber security, businesses are on the constant lookout for professionals with dynamic skills.

The following basic soft skills can come in handy for anyone looking to build a career in cyber security.

- Curiosity and inquisitiveness
- Business acumen
- Adaptability
- Interpersonal and communication skills
- Passion

Some additional skills that are required in cyber security are risk analysis, information security, security incident handling & response, security audit, and laws and regulations.

5. FUTURE SCOPE

The future scope of cybersecurity is expected to be significant as technology continues to advance and cyber threats become more sophisticated. Here are some key areas that are likely to shape the future of cybersecurity:

Artificial Intelligence (AI) and Machine Learning

AI and ML technologies have the potential to revolutionize cybersecurity. They can be used to detect and respond to threats in real-time, identify patterns and anomalies in large data sets, and automate security operations, making it easier to defend against evolving threats.

Internet of Things (IoT) Security:

With the rapid proliferation of IoT devices, securing the vast networks they create will be a crucial challenge.

Protecting IoT devices, data, and the networks they connect to will require robust security measures and protocols to prevent unauthorized access, data breaches, and the compromise of critical systems.

Cloud Security:

As organizations increasingly migrate their data and infrastructure to the cloud, securing cloud environments becomes paramount. New security models and tools are emerging to address the unique challenges associated with cloud security, including data protection, access control, and visibility across distributed cloud environments.

Mobile Security:

With the widespread use of smartphones and mobile devices, securing mobile platforms and applications will be crucial. Mobile security will encompass protecting data, preventing unauthorized access, and securing mobile payment transactions and communication channels.

Blockchain Security:

Blockchain technology offers decentralized and tamper-proof data storage, but it is not immune to security risks. Future cybersecurity efforts will focus on ensuring the integrity and confidentiality of blockchain networks, securing smart contracts, and preventing attacks such as 51% attacks and double-spending.

Quantum Computing and Post- Quantum Cryptography:

The advent of quantum computing poses a significant threat to existing encryption algorithms. Post-quantum cryptography research aims to develop new cryptographic algorithms resistant to quantum attacks. As quantum computing advances, organizations will need to upgrade their cryptographic system to maintain secure communications.

Threat Intelligence and Analytics:

Cybersecurity professionals will increasingly rely on advanced threat intelligence platforms and analytics tools to gather real-time information about emerging threats It analyzes large volumes of data for identifying patterns, and make informed decisions to mitigate risks.

Cybersecurity Regulations and Compliance:

Governments and regulatory bodies worldwide are recognizing the importance of cybersecurity and implementing

regulations and compliance standards. This trend is likely to continue, resulting in increased demand for cybersecurity professionals with expertise in compliance and risk management.

Overall, the future of cybersecurity will require continuous innovation, collaboration between industry, academia, and governments, and a proactive approach to stay ahead of emerging threats. Organizations will need to invest in skilled cybersecurity professionals, robust security technologies, and comprehensive risk management strategies to protect their digital assets.

As newer technologies evolve, they can be applied to cybersecurity to advance security practices. Some recent technology trends in cybersecurity include the following:

Security automation through AI:

While AI and machine learning can aid attackers, they can also be used to automate cybersecurity tasks. AI is useful for analyzing large data volumes to identify patterns and for making predictions on potential threats. AI tools can also suggest possible fixes for vulnerabilities and identify patterns of unusual behavior.

Zero-trust architecture:

Zero-trust principles assume that no users or devices should be considered trustworthy without verification.

Implementing a zero-trust approach can reduce both the frequency and severity of cybersecurity incidents, along with other zero-trust benefits architecture.

Behavioral biometrics:

This cybersecurity method uses machine learning to analyze user behavior. It can detect patterns in the way users interact with their devices to identify potential threats, such as if someone else has access to their account.

Continued improvements in response capabilities:

Organizations must be continually prepared to respond to large-scale ransomware attacks so they can properly respond to a threat without paying any ransom and without losing any critical data.

- **Probable future of cyber security:**
- Contribution of Machine learning and AI
- Quantum computing raises the capacity of hackers and defenders.
- Obsolete technologies impact cybersecurity after each upgrade.
- Nature of cybersecurity threats.
- Nature of cybersecurity practice.

Fields and Scope in Cyber Security

Governance

This is the Right Path for the ones who is passionate into Laws and Regulations, Auditing, Supervisory Procedures, Reports and scorecards, Guidelines, Policy, procedures, standards, Compliances and Enforcement. They are the guys who decide the standards and set of rules and procedures to work.

- **Threat Intelligence:**

  They are the guys who possess Internal and external threats to an organization, with rule sets and intelligence sharing.

- **Security Operation:**

  This domain Mostly works in a defensive perspective like Vulnerability Management, Recovery, SOC, Incident Response, Detection, Protection, Active Defense, Data Leakage, Investigation, and Forensics also fall under this category of Domain.

- **Career Development:**

  Human Resourcing and Development of the Organization Comes under this Domain to Undertake Training, Peer Groups, Self-Study, Conferences, Certification.

- **User Education:**

  Training and creating awareness of New skills and Threats to the employees and users of the organizations.

- **Framework and Standards:**

  This domain gives your life in Determining and Implementing Standards in an organization like ISO, COBIT, NIST, SANS

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1416-1430

- **CYBER ETHICS**

  Cyber ethics are nothing but the code of the internet. When we practice these cyber ethics there are good chances of us using the internet in a proper and safer way.

  The below are a few of them:

- DO use the Internet to communicate and interact with other people at anywhere and anytime**.**

  Email and instant messaging make it easy to stay in touch with friends and family members, communicate with work colleagues, and share ideas and information with people across town or halfway around the world.

- Don't be a bully on the Internet. Do not call people names, lie about them, send embarrassing pictures of them, or do anything else to try to hurt them.
- Internet is considered as world's largest library with information on any topic in any subject area, so using this information in a correct and legal way is always essential.
- Do not operate others accounts using their passwords.
- Never try to send any kind of malware to other's systems and make them corrupt.
- Never share your personal information to anyone as there is a good chance of others misusing it and finally you would end up in a trouble.
- When you're online never pretend to the other person, and never try to create fake accounts on someone else as it would land you as well as the other person into trouble.
- Always adhere to copyrighted information and download games or videos only if they are permissible.

The above are a few cyber ethics one must follow while using the internet. We are always thought proper rules from out very early stages.

Functions of Cyber Ethics:

- **Cyber Bullying:**

  Cyberbullying is a form of bullying carried out via internet technology such as social media where individuals are mocked on their physical appearance, lifestyle, preferences, etc. The teenage generation or say youngsters are the major victims of this form of cyber ethic breach. Cyberbullying affects the emotional ethics of individuals and can cause mental disturbance to individuals.

- **Hacking:**

  Stealing a user's personal or organizational information without authorized permission is not considered a good practice. It is one of the riskiest cyber breaches to data leak. Data leak includes passing of sensitive information such as passwords, bank details of the user to a third- party user who is not authorized to access the information.

- **Copywriting:**

  Claiming of another individual as one's own is another type of cyber ethic breach that must be eradicated. Never engage in copywriting another person's content or document and claim as it is your own.

  It leads to a serious problem called plagiarism, which is a punishable offense and considered a legal crime. It is always advisable to follow general cybernetics, while using the internet or say any kind of technology.

  A proper code of conduct must be followed while using cyber technology. Cybernetics if not used wisely can lead to serious situations. Social and legal laws are defined to use cyber technology wisely. In extreme cases, legal action can be taken if there is a violation of cyber ethics.

6. CONCLUSION

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cybercrime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cybercrimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space.

cybersecurity is a critical aspect of our digital world, safeguarding individuals, organizations, and nations from malicious cyber threats. As technology continues to advance, the importance of robust cybersecurity measures cannot

be overstated. Effective cybersecurity requires a multi- faceted approach, involving technological solutions, robust policies and regulations, continuous education and training, and collaboration between various stakeholders. It's not merely about installing antivirus software or implementing firewalls but also about fostering a culture of cybersecurity awareness and resilience.

The consequences of neglecting cybersecurity can be severe, ranging from financial losses and reputational damage to national security threats and even loss of life in extreme cases. Therefore, investing in cybersecurity is not just an option but a necessity in today's interconnected world.

The evolution of cyber threats demands continuous adaptation and innovation in cybersecurity strategies. As cybercriminals become more sophisticated, cybersecurity measures must keep pace, utilizing advanced technologies like artificial intelligence and machine learning to detect and mitigate threats effectively.

In essence, cybersecurity is everyone's responsibility, from individual users to large corporations and government agencies. By prioritizing cybersecurity and adopting a proactive approach, we can collectively mitigate cyber risks and ensure a safer and more secure digital future for all.

7. REFERENCES

[1] A Sophos Article 04. 12v1.dNA, eight trends changing network security by James Lyne.

[2] Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole.

[3] Computer Security Practices in Non- Profit Organizations – A Net Action Report by Audrie Krause.

[4] A Cybersecurity Agenda for the 45th President. (2017, January

[5] Retrieved from https://www.csis.org/news/cyberssecurity - agenda-45th-president

[6] An Examination of the Cybersecurity Labor Market. Retrieved from http://www.rand.org/content/dam/ rand/pubs/research reports/RR40 0/RR430/RANDRR430.pdf

[7] Apprenticeship USA Investments. (2017, June 22). Received from https://www.dol.gov/featured/appr entices hip/grants