International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST523102121

Upcoming Threats in Cyber-Security

Shruti Sudhir Shinde[1], Gauri Ansurkar[2]

[1]Keraleeya Samajam's Model College, Khambalpada Road, Thakurli, Dombivli (East), Maharashtra, India

[2]Assistant Professor, Keraleeya Samajam's Model College, Khambalpada Road, Thakurli, Dombivli (East), Maharashtra, India

ARTICLEINFO

Article History:

Accepted: 05 April 2023
Published: 27 April 2023

Publication Issue
Volume 10, Issue 2
March-April-2023

Page Number
806-816

ABSTRACT

As technology advances rapidly, the cyber-security field is constantly facing new threats. All the world is running over networks. Cyber-security is adapting new changes and grows exponentially with real-time. Cybercriminals are constantly adapting and finding innovative ways to exploit vulnerabilities in networks, systems, and devices. From artificial intelligence (AI)-powered attacks to breaches of supply chains, cyber-security threats are evolving at an unprecedented pace. To protect sensitive data, ensure business continuity, and protect against potential financial and reputational damage as organizations increasingly rely on digital technology to conduct their business. It is important for us to stay vigilant and proactively address these emerging threats. This introduction examines some of the upcoming cyber-security threats that are expected to pose significant challenges in the near future and highlights the need for robust cyber-security measures to effectively mitigate these risks.

Keywords : Cyber-security, networks, vulnerabilities, Cybercriminals, mitigate these risks.

I. INTRODUCTION

As the technology is increasing, networks becomes more vulnerable. Globally, cyber-attacks are happening due to some lack of security in networks. It is becoming major concern. The word is full of data. Organizational data, hospital's data, government data, etc. contains sensitive information. The vulnerabilities in smart electronic devices such as mobile, computers, tabs etc. For example mobile hacking or mobile cybercrimes are also evolving so it becomes important to communicate about mobile security threats and best practices to keep the devices safe. Malware attacks are increasing on network causing errors in hardware devices. Malware entering smartphones and PC's try to disable essential functions and spread the virus leading to an information leak.

Various common on network attacks affect the users' or institutions' network systems, such as denial of service (DoS), distributed denial of service (DDoS), and SQL injection. Thus, cyber-security specialists propose and utilize various types of defensive methods against network attacks, such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPSs). Such defence methods are used to detect or deter unauthorized network attacks that may affect network users in a harmful way. [https://www.mdpi.com/1999-5903/15/2/62]

Day-by-day the branches like Artificial Intelligence (AI), Internet of Things (IoT), Cloud Security, Data Science (DS), and Machine Learning (ML) are expanding with vulnerabilities. For example, ML systems are increasingly trusted in cyber-physical systems. In such a complex physical environment, threats that penetrate vulnerable systems can be harmful. With significant advances in ML technology in network security, new attack surfaces are opening up for attackers. Therefore, IDS is built on top of ML, which can be compromised by building adversarial inputs to ML/DL models such as artificial neural networks (ANNs), deep neural networks (DNNs), and support vectors. Vulnerable to adversary attacks. Machine (SVM), which affects accuracy and robustness. In addition, research also shows that the attacker's samples can impact his ML-based IDS. As a result, ML can also be fooled, which requires some protection mechanism. In addition, communicating over open networks leaves systems vulnerable and gives adversaries a large attack surface.

II. Background

Cyber-security in the past has evolved in tandem with rapid technological progress, from early measures to protect individual computers and networks to more sophisticated strategies to protect complex systems and data. Below is a quick overview of the past of cyber-security and how it works.

a. Early Days: Passwords and Firewalls

In the early days of computing, cyber-security mostly relied on simple measures like passwords and firewalls. Passwords were used to restrict access to individual computers or networks, and firewalls were implemented to create barriers between internal and external networks and filter incoming and outgoing network traffic.

b. Antivirus Software and Intrusion Detection Systems:

The emergence of computer viruses and other forms of malware as a threat has led to the development of antivirus software and intrusion detection systems (IDS). Antivirus software scanned files and programs for known malware signatures, and IDS monitored network traffic for suspicious activity that could indicate an intrusion or attack.

c. Encryption and Secure Communications:

Encryption technology was developed to protect data transmitted over networks and stored on computer systems. Encryption uses algorithms to scramble data so that only authorized parties with the correct decryption key can read the data. Secure communication protocols such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS) have also been developed to protect data transmitted over the Internet.

d. Public Key Infrastructure(PKI):

A Public Key Infrastructure (PKI) was introduced to securely authenticate users and ensure data confidentiality and integrity. PKI uses asymmetric encryption. In this cryptography, the user has a public/private key pair to verify the user's identity and encrypt the data. PKI is commonly used for digital certificates, secure communications, and digital signatures.

e. Security Awareness and Training:

Recognizing that the human element is a key component of cyber-security, security awareness and training programs have become essential.

These programs should educate users on safe computing practices, phishing awareness, password hygiene, and other security best practices to reduce the risks associated with human error and social engineering attacks.

f. Vulnerability Scanning and Patching:

Vulnerability scanning and patching have become common cyber-security practices for identifying and remediating vulnerabilities in software and systems. Vulnerability scans use automated scanning tools to look for known vulnerabilities. Patching uses updates or patches to fix vulnerabilities and improve **SYSTEM** security.

g. Security Standards and Best Practices:

Various security standards and best practices have been developed to help organizations protect their systems and networks. Examples include the ISO/IEC 27001 standard for information security management systems, the NIST Cyber-security Framework, and the Centre for Internet Security (CIS) Critical Security Controls.

In summary, cyber-security in the past has developed a variety of technologies, techniques, and best practices to protect digital systems and data. Cyber-security has evolved from simple measures to complex strategies involving encryption, authentication, patching and incident response, with increasing emphasis on security awareness and training to address human vulnerability.

III.Types of Attacks on Cyber-security:

There're various types of cyber-attacks. DOS, DDOS, SQL injection, phishing etc. these are common attacks. Nowadays, attackers are more intended to create vulnerabilities in data branches like Artificial Intelligence (AI), Machine Learning (ML), Data Science (DS), Internet of Things (IoT) Cloud, cryptocurrency etc.

A. Ransomware-as-a-Service (RaaS) Attacks:

A Ransomware-as-a-Service (RaaS) attack is a type of cyber-attack distributed and operated as a service by malicious actors who rent or sell ransomware to other individuals or groups (commonly called "affiliates"). is. Or "Partner" is called "Customer". With RaaS, even people with limited technical skills can mount ransomware attacks because the service provider handles the technical aspects, such as: B. Creating and maintaining ransomware while partners focus on target selection and ransomware distribution.

Some of the key characteristic of RaaS attacks are service-based model, accessibility, customization, profit sharing, affiliate driven operations. Ransomware-as-a-Service (RaaS) attacks have become a significant threat in the cyber-security landscape, allowing a wider range of actors to participate in ransomware attacks and increasing the overall frequency and scale of such attacks.

B. Deepfake attacks:

Deepfakes, an emergent type of threat falling under the greater and more pervasive umbrella of synthetic media, utilize a form of artificial intelligence/machine learning (AI/ML) to create believable, realistic videos, pictures, audio, and text of events which never happened. A deepfake attack is the exploitation of deep learning-based technologies, such as artificial intelligence (AI) and machine learning (ML), to create and distribute manipulated or fabricated media such as images, videos, audio recordings, and texts. refers to Deepfakes are often created using advanced algorithms that can produce realistic and compelling content that is difficult to distinguish from real media.

The negative impact of deepfake attacks are misinformation and disinformation, Fraud and Social Engineering, privacy and Consent Violations, Political Manipulation, Cyber-security Risks. Deepfake attacks can also pose cyber-security risks, as attackers can use deepfakes to impersonate individuals or gain unauthorized access to systems or accounts.

C. Artificial Intelligence (AI) Attacks:

An artificial intelligence (AI) attack refers to the exploitation of AI technology or the exploitation of vulnerabilities in AI systems that can unauthorized access, manipulate, sabotage, or deceive AI-based systems, data, or processes. As AI technology becomes more prevalent and sophisticated, it can also be used for malicious purposes by malicious actors. Examples of AI attacks includes data poisoning, adversarial attacks, model inversion, generative adversarial network (GAN) attacks, AI-based Social engineering. Adversarial attacks involve manipulating inputs to AI systems in order to deceive them. Data poisoning attacks involve injecting malicious data into the training data used to train AI models. Model inversion attacks involve exploiting the transparency of AI models to infer sensitive information about the training data used to train the models. GANs are a type of AI model used to generate realistic data such as images and videos. GANs are maliciously used to generate fake data such as fake images, videos, and documents for various purposes, such as spreading disinformation, creating fake identities, and generating realistic phishing content. AI can be used to create realistic and compelling social engineering attacks such as voice or text-based chatbots that can impersonate real people, leading to social manipulation, fraud, and deception.

D. Quantum Computing Attacks:

A quantum computing attack uses quantum computing, a state-of-the-art technology that leverages the principles of quantum mechanics, to exploit vulnerabilities in traditional cryptosystems to gain unauthorized access or manipulate data. , to break an encryption algorithm. Quantum computers have the potential to revolutionize computing by solving certain complex problems exponentially faster than classical computers. This includes factoring large numbers, solving the discrete logarithm problem, and performing quantum key distribution. However, this also poses significant risks to traditional cryptographic techniques that rely on the severity of these security issues.

Some examples of quantum computing attacks include:

1. **Quantum Cryptographic Attack:**

Quantum computers have the potential to break many of the traditional cryptography methods commonly used for secure communications and data encryption, such as RSA and ECC (elliptic curve cryptography). Quantum computers can use Shor's algorithm to factorize large numbers that can break the security of many current cryptosystems, as well as to solve the discrete logarithm problem.

2. **Quantum key distribution (QKD) attacks:**

Quantum Key Distribution is a quantum cryptography that uses the principles of quantum mechanics to securely distribute cryptographic keys. However, a quantum computer could potentially launch an attack against his QKD protocol like this: B. Intercept and retransmit attacks that could compromise the security of the key distribution process, photon number splitting attacks, or time shifting attacks.

3. **Quantum brute force attack:**

Quantum computers may be able to perform brute force attacks more efficiently than classical computers using Grover's algorithm, a quantum algorithm for searching unsorted databases. This can accelerate the cracking of symmetric encryption keys or password hashes.

4. **Quantum side-channel attack:**

Quantum computers can also use side-channel attacks to extract information from cryptographic systems. Measure the quantum state of a system, obtain information about cryptographic keys, or exploit quantum leaks from quantum systems.

5. **Quantum Replay Attack:**

Quantum computers potentially exploit the unique properties of quantum systems, such as quantum

entanglement, to allow attackers to capture quantum signals and later replay them to gain unauthorized access or tamper with data.

E. Internet of Things (IoT) Attacks:

An Internet of Things (IoT) attack is an attack that exploits vulnerabilities in IoT devices, networks, or applications to gain unauthorized access, manipulate data, disrupt services, or compromise connected devices or systems. Malicious activity that compromises or compromises the privacy and security of IoT refers to networks of interconnected devices such as smart devices, wearable, sensors, and industrial control systems that communicate and exchange data over the Internet. As the number of IoT devices continues to grow rapidly, so does the potential for IoT attacks.

1. Device Exploitation:

Attackers can exploit vulnerabilities in IoT devices such as: B. Use weak passwords, unpatched software, or insecure communication protocols to gain unauthorized access to the device to control its functionality or steal sensitive data.

2. Eavesdropping and Data Tampering:

Attackers can intercept and manipulate communications between IoT devices, networks, or applications to eavesdrop on sensitive data, modify data, or inject malicious commands or malware to compromise data integrity. They can jeopardize privacy and confidentiality.

3. Physical Attacks:

An attacker can physically manipulate an IoT device. Modify sensors or tamper with firmware or hardware to interfere with their functionality or gain unauthorized access to sensitive information or control systems.

4. Botnets:

Attackers can create botnets, networks of compromised IoT devices, to launch large-scale attacks. Distributed Denial of Service (DDoS) attacks. Overload a system or network with data traffic, causing disruption or loss of service.

5. IoT Protocol Attacks:

Attackers target communication protocols used in IoT networks such as Wi-Fi, Bluetooth, and Zigbee to exploit vulnerabilities, perform man-in-the-middle attacks, and steal data sent between devices or networks. Can be intercepted and manipulated.

F. Cryptocurrency Attacks:

Cryptocurrency attacks refer to malicious activity that uses cryptography for security and targets cryptocurrencies, which are digital or virtual currencies that operate on distributed networks such as blockchains. Cryptocurrencies such as Bitcoin and Ethereum have gained popularity in recent years due to their potential as digital assets and investment opportunities, but they are also vulnerable to various types of attacks.

Examples of cryptocurrency attacks include:

1. **Theft of Cryptocurrency:** Attackers can exploit vulnerabilities in wallets, exchanges, or other cryptocurrency-related software to steal cryptocurrencies from individuals or organizations.

2. Malicious Mining:

Attackers can infect computers and other devices with malware to hijack computing power for cryptocurrency mining without the owner's consent. This increases power consumption, slows down performance, and can damage infected devices.

3. Initial Coin Offering (ICO) Scams:

An ICO is a fundraising activity that launches a new cryptocurrency. An attacker could create a fake his ICO, promise investors a high return, and then disappear with the raised funds without fulfilling the promise, resulting in financial loss for the investor.

4. Pump and Dump Schemes:

In pump-and-dump schemes, attackers manipulate the price of low-volume or low-cap cryptocurrencies by spreading false information to generate hype, lure buyers, and artificially raise prices. Once the price hits a certain level, the attackers sell their holdings, causing the price to crash, causing financial losses to unsuspecting buyers.

5. Fake Cryptocurrency Wallets and Apps:

Attackers can create fake cryptocurrency wallets or apps that impersonate legitimate wallets and distribute them through app stores, social media, or other channels. Unsuspecting users can download and use these fake wallets and apps, allowing their crypto funds to be stolen or compromised.

6. Phishing and Social Engineering Attacks:

Attackers can use phishing and social engineering techniques to trick cryptocurrency users into revealing private keys, wallet credentials, or other sensitive information. This can be done through a fake her website, emails, messages or other forms of communication impersonating a legitimate cryptocurrency platform or entity.

1. Solution on Cyber Threats:

Cyber-security is an ongoing process, and organizations need to continually assess and update their cyber-security measures to adapt to evolving threats and ensure the best possible protection against cyber-attacks. It is important to note that additionally, working with cyber-security experts, staying current on the latest threats and best practices, and maintaining a proactive approach to cyber-security are key to effectively mitigating cyber risk.

1. To reduce the risks associated with deepfake attacks, detect and verify the authenticity of media content, raise awareness of the existence of deepfakes, and use AI and ML technologies responsibly and ethically for promotional purposes. It is important to develop robust techniques for additionally, policymakers, technology developers, and social media platforms must work together to establish policies, regulations, and best practices to counter deepfake attacks and protect individuals and society at large.
2. Containing AI attacks requires robust security practices, such as protecting the data used to train AI models, implementing robust authentication and access controls, detecting and mitigating adversary attacks, and ensuring transparency, accountability, and ethics. Security measures are required using AI technology.
3. Regular security audits, vulnerability assessments, and proactive monitoring of AI systems are also essential to identify and remediate potential vulnerabilities and risks associated with AI deployments. Collaboration among researchers, developers, policy makers, and stakeholders to establish best practices, standards, and regulations to protect against AI attacks and ensure responsible and safe use of AI technology.
4. Defending against quantum computing attacks requires the development and implementation of post-quantum cryptosystems designed to be resistant to quantum attacks. This includes research and deployment of quantum secure cryptographic algorithms such as Lattice-based encryption, code-based encryption, or hash-based encryption. Additionally, secure key distribution can be achieved using implementations of the QKD (Quantum Key Distribution) protocol that are resistant to known quantum attacks.
5. Firms should also plan for quantum readiness by assessing the impact of quantum computing on current cryptosystems and moving to quantum-resistant methods in a timely manner. Collaboration between researchers, policymakers and industry players is essential to stay ahead of quantum computing attacks and ensure the

security of sensitive information in the quantum era.

6. Containing IoT attacks requires implementing strong security measures in all aspects of your IoT deployment. These include using strong authentication and access controls, regularly updating and patching IoT devices and software, encrypting data sent between devices and networks, It includes IoT network segmentation and monitoring for anomalous behaviour and traffic patterns. It's also important to implement security best practices such as least privilege, defence in depth, and regular security audits.
7. Additionally, educating users and stakeholders about IoT security risks and promoting a security-centric mind set in IoT development and deployment can help prevent IoT attacks. Collaboration among manufacturers, vendors, developers, policy makers, and end users is essential to setting industry standards, policies, and regulations to protect IoT devices and networks in the rapidly evolving threat landscape.
8. Containing cryptocurrency attacks requires implementing strong security measures across the cryptocurrency ecosystem. This includes using secure and reputable wallets and exchanges, implementing multi-factor authentication (MFA) for user accounts, updating software and systems with the latest security patches, using strong and unique passwords, using phishing attacks and Includes caution against other social engineering attacks. Regular security audits, vulnerability assessments, and penetration tests also help identify and fix potential vulnerabilities.
9. Implement a logging and monitoring solution to collect and analyse network and system logs in real time. This allows you to quickly detect and respond to security incidents by identifying unusual behaviour and patterns of activity that may indicate cyber-attacks.
10. Collaborate with industry peers, information-sharing firms or organizations, and government agencies to share threat intelligence, best practices, and lessons learned. This gives you valuable insight into emerging threats and keeps you one step ahead of cyber attackers.
11. Implement the principle of least privilege. Users are granted only the minimum level of access required to perform their jobs. Remember that cyber-security is an ongoing process and requires a proactive approach. Evaluate, update and improve security measures on a regular basis to effectively combat future cyber-security threats. Get the latest threats, trends, and best practices from trusted sources, and work with cyber-security experts to tailor your security strategy to your specific needs.

IV. Public Survey:

We first conducted a poll of people through Google form creator and data collection service to acquire information regarding people's awareness.

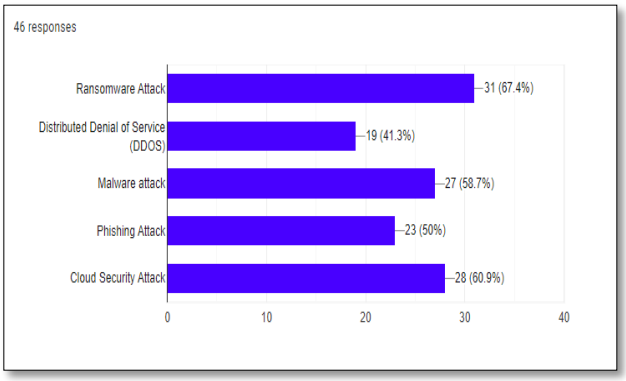
Questionnaire:

1. What do you consider to be biggest upcoming threat in cyber-security world?
2. According to you, why hackers are still successful organisation hack your or any organizational data?
3. How concerned are you about the impact of threats on your personal or professional life in upcoming year?
4. Do you think your data is protected within organization or in day-to-day life?
5. What do you think the option to protect our information against cybersecurity threats?
6. According to you, what measures should be implemented in cyber-threats?

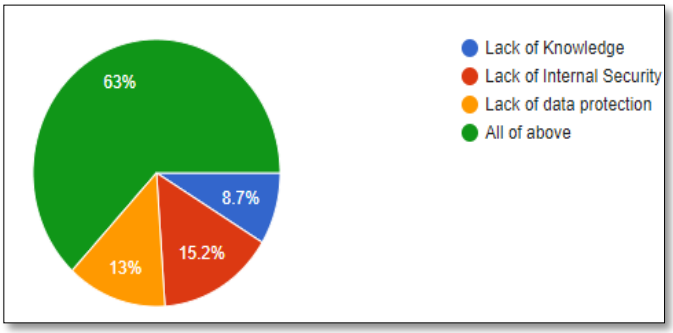
7. Have you or your organization implemented any new cybersecurity technologies or strategies in response to emerging threats?
8. How confident are you in your organization's ability to detect and respond to a cybersecurity incident?
9. What is your or your organization's primary motivation for investing in cybersecurity measures?

V. Results

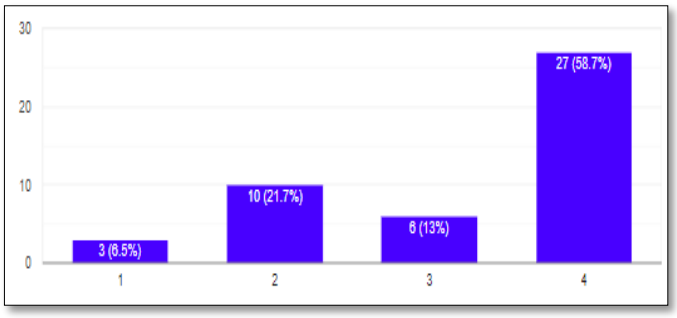
1. What do you consider to be biggest upcoming threat in cyber-security world?



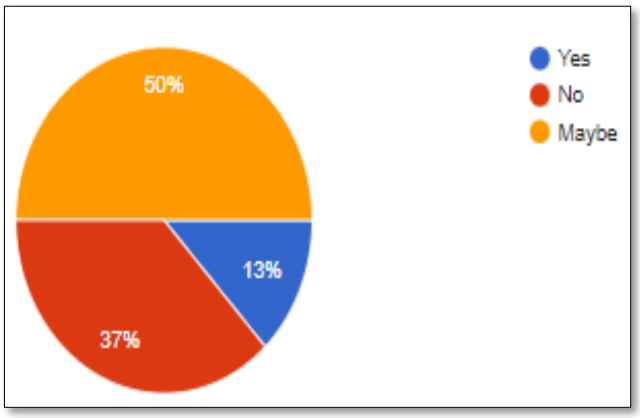
2. According to you, why hackers are still successful organisation hack your or any organizational data?



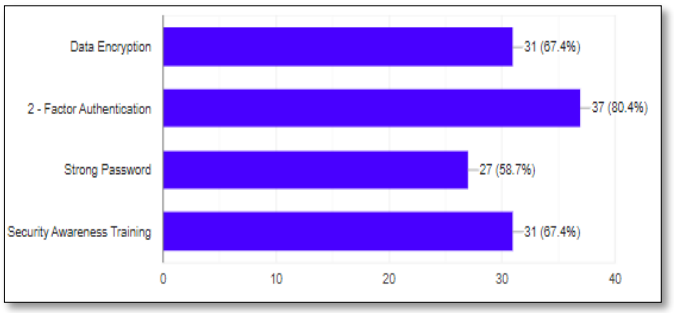
3. How concerned are you about the impact of threats on your personal or professional life in upcoming year?



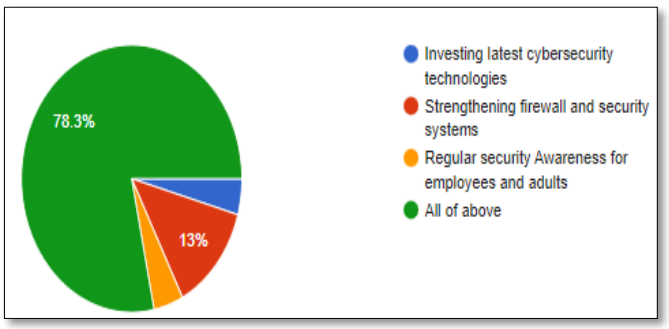
4. Do you think your data is protected within organization or in day-to-day life?



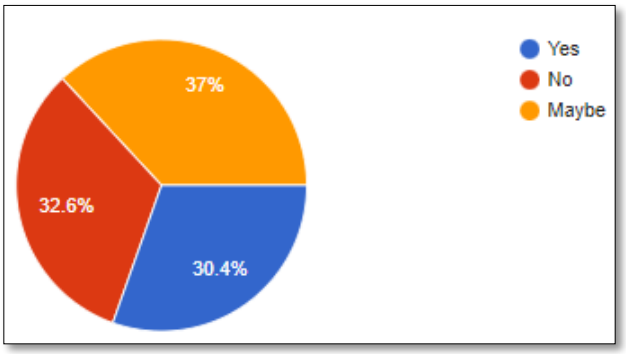
5. What do you think the option to protect our information against cybersecurity threats?



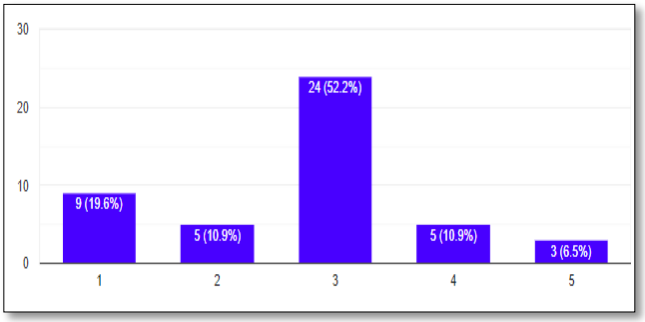
6. According to you, what measures should be implemented in cyber-threats?



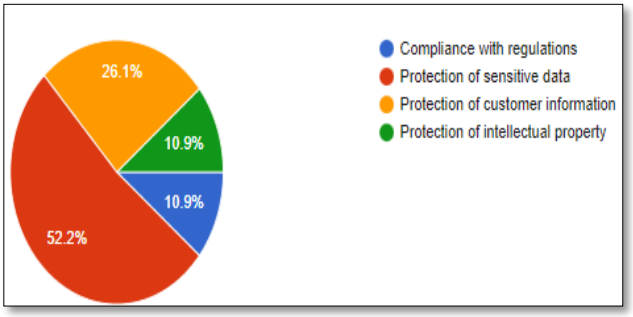
7. Have you or your organization implemented any new cybersecurity technologies or strategies in response to emerging threats?



8. How confident are you in your organization's ability to detect and respond to a cybersecurity incident?



9. What is your or your organization's primary motivation for investing in cybersecurity measures?



1.1 Descriptive Statistics:

Descriptive statistics is means of describing features of a data set by generating summaries about data samples.

Here are some results which will helps us in finding the actual response of people.

Do you think your data is protected within organization or in day-to-day life?	
Mean	1.130434783
Standard Error	0.137643015
Median	1.5
Mode	2
Standard Deviation	0.93354035
Sample Variance	0.871497585
Kurtosis	-1.843005308
Skewness	-0.269795027
Range	2
Minimum	0
Maximum	2
Sum	52
Count	46
Largest(1)	2
Smallest(1)	0
Confidence Level(95.0%)	0.277227264

Have you or your organization implemented any new cybersecurity technologies or strategies in response to emerging threats?	
Mean	1.043478261
Standard Error	0.124164927
Median	1
Mode	2
Standard Deviation	0.842127511
Sample Variance	0.709178744
Kurtosis	-1.594449743
Skewness	-0.084272916
Range	2
Minimum	0
Maximum	2
Sum	48
Count	46
Largest(1)	2
Smallest(1)	0
Confidence Level(95.0%)	0.250081001

VI. Findings

A survey was conducted to know the view of the people about what they think regarding the technology of cybersecurity threats and the solution they have for current threats. So, people gave their opinions on different threats. So, this is what the stats say:

1. First of all 93.5% of responders are in age category of 19-35, 4.3% of 35-60 and 2.2% are from 60 and above age.
2. According from total responses, 67.4% of respondents thinks that ransomeware attack would be the biggest upcoming attack, then 60.9% is for cloud security attack, then 58.7% is for malware attack, then 50% is for phishing attack and 41.3% is for DDOS.
3. According from total responses, 63% of people thinks that the Lack of Knowledge, Lack of Internal Security and Lack of data protection are the reason that the hackers are still successful too hack personal or organizational data.
4. According from total responses, 58.7% of people are most concerned for impact of threats on your personal or professional life in upcoming year.
5. According from total responses, 50% of people thinks data is protected within organization or day-to-day life, 37% of people does not think that their data is protected within organization or day-to-day life, other 13% are still confused.
6. According from total responses, 80.4% of people thinks that the option to protect our information against cybersecurity threats is 2-Factor authentication. Then 67.4% of people thinks for data encryption and security awareness training, then 58.7% is for strong password.
7. According from total responses, 78.3% of respondents thinks investing latest cyber-security technologies, strengthening firewall and security systems and regular security awareness for employees and adults are the measures should be implemented in cyber-threats
8. According from total responses, less organizations have already implemented new cybersecurity technologies or strategies in response to emerging threats.
9. According from total responses, 52.2% of respondents are confident are you in your organization's ability to detect and respond to a cybersecurity incident.
10. According from total responses, 52.2% of people thinks that their organization's primary motivation for investing in cybersecurity measures, then 26.1% is for protection of customer information and 10.9% is for Protection of intellectual property and compliance with regulations

VII. Conclusion

In summary, cybersecurity threats are constantly evolving, posing significant challenges in the future. Due to rapid technological advancement, increasing device connectivity, and increasing reliance on digital systems, several upcoming threats are expected to impact the cybersecurity landscape.

The cybersecurity landscape is complex and ever-changing, and future threats present significant challenges. Organizations and individuals should stay vigilant, stay up-to-date with the latest cybersecurity best practices, and implement robust security measures to protect against these evolving threats. To protect against evolving threats in the cybersecurity environment, it is important to take a proactive, multi-layered approach to cybersecurity, including strong authentication, encryption, regular security audits, and employee training.

VIII. REFERENCES

[1]. https://www.aura.com/learn/emerging-cyber-threats

[2]. https://fieldeffect.com/blog/what-is-the-future-of-cyber-security

[3]. https://www.knowledgehut.com/blog/security/cyber-security-challenges#the-new-challenges-of-cybersecurity-and-solutions-in-2022
[4]. https://www.mdpi.com/1999-5903/15/2/62

Cite this article as :

Shruti Sudhir Shinde, Gauri Ansurkar, "Upcoming Threats in Cyber-Security", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 10 Issue 2, pp. 806-816, March-April 2023. Available at doi : https://doi.org/10.32628/IJSRST523102121
Journal URL : https://ijsrst.com/IJSRST523102121