**SEMINAR REPORT**

**ON**

**Cyber Security**

**Submitted to**

**Rashtrasant Tukadoji Maharaj Nagpur University,**

**NAGPUR**

In partial fulfillment of the requirement of

**M.Sc. – (Computer Science) Semester-II Examination**

Submitted by

**Pranay Vijay Shahare**

**Under the Guidance of**

**Dr. V. C. Pande**

Assistant Professor

**Department of Computer Science**

**DEPARTMENT OF COMPUTER SCIENCE**

**Shri Shivaji Education Society Amravati’s**

**SCIENCE COLLEGE**

**Congress Nagar, Nagpur-440012.**

**2020-2021**

Department of Computer Science

Shri Shivaji Education Society Amravati’s,

Science College, Congress Nagar, Nagpur.

**CERTIFICATE**

This is to certify that **Pranay Vijay Shahare** have successfully prepared the seminar report entitled **Cyber Security** under my guidance towards the partial fulfillment of the requirement of  **M.Sc. – (Computer Science) Semester-II Examination** submitted to **Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur** during the academic year 2020-21.

**Place:** Nagpur Seminar Guide

**Date: 27-07-2021 Dr. V. C. Pande**

Assistant Professor

Department of Computer Science

**INDEX**

|  |  |  |
| --- | --- | --- |
| **Sr. No.** | **Name of the Topics** | **Page No.** |
| 1. | Introduction | 1 |
| 2. | Objectives | 2 |
| 3. | Features | 2 |
| 4. | Implementation | 4 |
| 5. | Advantages and Disadvantages | 5 |
| 6. | Conclusion | 6 |
| 7. | Future Scope | 6 |
| 8. | References | 7 |

**1. INTRODUCTION**

Cybersecurity is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc."

Cybersecurity is the protection of Internet-connected systems, including hardware, software, and data from cyber attacks. It is made up of two words one is cyber and other is security. Cyber is related to the technology which contains systems, network and programs or data. Whereas security related to the protection which includes systems security, network security and application and information security.

It is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access. It may also be referred to as information technology security.

We can also define cybersecurity as the set of principles and practices designed to protect our computing resources and online information against threats. Due to the heavy dependency on computers in a modern industry that store and transmit an abundance of confidential and essential information about the people, cybersecurity is a critical function and needed insurance of many businesses.

**Why is cybersecurity important?**

Because, We live in a digital era which understands that our private information is more vulnerable than ever before. We all live in a world which is networked together, from internet banking to government infrastructure, where data is stored on computers and other devices. A portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Cyber-attack is now an international concern and has given many concerns that hacks and other security attacks could endanger the global economy. Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cybersecurity describes to protect that information and the systems used to process or store it. As the volume of cyber-attacks grows, companies and organizations, especially those that deal information related to national security, health, or financial records, need to take steps to protect their sensitive business and personal information.

**2. OBJECTIVE**

To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT systems and transaction in cyberspace and thus enhance adoption of IT in all sectors.

To create an assurance framework for design of security policies.

To strengthen the regulatory framework for ensuring a secure cyberspace ecosystem.

The objective of cybersecurity is to protect information from being stolen, compromised or attacked. Cybersecurity can. be measured by at least one of three goals.

1. **Confidentiality -**  Keeping sensitive information private. Encryption services can protect your data at rest or in transit and prevent unauthorized access to protected data.
2. **Integrity –** It is the consistency of data, networks, and systems. This includes mitigation and proactive measures to restrict unapproved changes, while also having the ability to recover data that has been lost or compromised.
3. **Availability –** It refers to authorized user that can freely access the systems, networks and data needed to perform their daily tasks,. Resolving hardware and software conflicts, along with regular maintenance is crucial to keep systems up and available.

* Analyze the threats and vulnerabilities in information systems and find ways to resolve them.
* Troubleshoot threats using secure enterprise architecture.
* Apply business security awareness using strategic management and resource optimization.
* Create an effective defense in cyber-related attacks and threats.

**3. FEATURES**

1. Coverage that includes major threat vectors such as email and web security (38%). Any security researcher will tell you that at least 90% of cyber attacks emanate from phishing emails, malicious attachments, or weaponized URLs. A cybersecurity platform must apply filters and monitoring to these common threat vectors for blocking malware and providing visibility into anomalous, suspicious, and malicious behaviors.
2. Central management across all products and services (33%). In this instance, central management means configuration management and policy management, along with common administration and reporting. Cybersecurity technology platform management provides an aggregated alternative to the current situation where organizations operate endpoint security management, network security management, malware sandboxing management, etc.
3. Capabilities across threat prevention, detection, and response (31%). CISOs want their security technologies to block the majority of attacks with detection efficacy in excess of 95%. When attacks circumvent security controls, they want their cybersecurity technology platforms to track anomalous behaviors across the kill chain (or the MITRE ATT&CK framework), provide aggregated alerts that string together all the suspicious breadcrumbs, and provide functions to terminate processes, quarantine systems, or rollback configurations to a known trusted state.
4. Coverage that spans endpoints, networks, servers, and cloud-based workloads (27%). This one is sort of self-explanatory. Today’s enterprises feature Balkanized endpoint, network, server, and cloud-workload protection tools don’t talk to each other. Enterprise organizations want tightly integrated tools that span their IT infrastructure and work together as security force multipliers.
5. Cloud-based backend services — i.e. analytics, threat intelligence, signature/rules distribution, etc. (26%). Think of the cloud as the backend brains of a cybersecurity technology platform. Cloud-based services will aggregate suspicious behaviors across customers, run these behaviors through advanced and constantly improving machine learning algorithms, track the latest threat intelligence, and provide customized analytics and threat intelligence curation for specific customers, and industries, etc. In this way, all customers benefit from universal and customized services
6. Openness — i.e. open APIs, developer support, ecosystem partners, etc. (22%). Even the best cybersecurity technology platforms won’t offer exhaustive security coverage. Therefore, security platforms must be fitted with APIs for third-party technology integration and developer support. This will also encourage the network effect where cybersecurity technology platform users share development best practices and homegrown software amongst the community.
7. A combination of tightly coupled products and services — i.e. products and managed service options offering central command-and-control (20%). Given the global cybersecurity skills shortage, organizations will pick and choose which security technologies they run in house and which they outsource to managed security service providers. Leading cybersecurity technology platforms will enable seamless interoperability across any product and managed services mix.
8. A platform that is offered in multiple deployment options — i.e. on premises, cloud delivered, hybrid, etc. (18%). Large organizations tend to use hybrid technology deployments, running security appliances at corporate headquarters while opting for cloud based security proxy services to support remote offices and mobile workers. Cybersecurity technology platforms will offer this hybrid support across all security controls (regardless of form factor) with a central management plane.

**4. IMPLEMENTATION**

Cybersecurity is designed to provide multiple layers of protection across all of the computers, networks, and programs used by a business. In order to create a unified defence against potential cyberattacks, it is important that the business, employees, processes, and technology are designed to work seamlessly together. Cybersecurity systems that function properly will be able to detect, investigate, and resolve potential weaknesses and vulnerabilities in the system before they can be exploited by a hacker or malicious software.

**Types of Cybersecurity:**

The different types of cybersecurity include:

**Application Security**:- Application security is the implementation of various defence within business software and services to protect against a range of different threats. This type of cybersecurity requires the design of secure applications to minimize unauthorized access and modification.

**Data Security**:- Data security involves implementing strong data storage systems that are specifically designed to secure information while it is being stored and while it is in transit.

**Network Security**:- Network security focuses on protecting a business from both external and internal threats by implementing hardware and software systems that are specifically designed to protect a business’ network and infrastructure from misuse, disruptions, and unauthorized access.

**Mobile Security**:- Businesses that use mobile devices, such as cell phones, laptops, and tablets, should use mobile security measures to protect the information that is being stored on those devices from a range of different threats

**Cloud Security**:- Most cloud applications and system—AWS, Google, Microsoft, etc.—use cloud security measures to protect users against various threats.

**Cyber Security Techniques:**

**Access Control and Password Security:-** The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security.

**Authentication of Data:-** The documents that we receive must always be authenticated be before downloading that is it should be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the anti virus software present in the devices. Thus a good anti virus software is also essential to protect the devices from viruses.

**Malware Scanner:-** This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

**Anti-virus Software:-** Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An anti virus software is a must and basic necessity for every system.

**5. ADVANTAGES AND DISADVANTAGES**

**ADVANTAGES**

1. Protects system against viruses, worms, spyware and other unwanted programs.
2. Protection against data from theft.
3. Protects the computer from being hacked.
4. Minimizes computer freezing and crashes.
5. Gives privacy to user.

**DISADVANTAGES**

1. Firewalls can be difficult to configure correctly.
2. Incorrectly configured firewalls may block users from performing certain actions on the Internet, until the firewall configured correctly.
3. Makes the system slower than before.
4. Need to keep updating the new software in order to keep security up to date.
5. Could be costly for average user.

**6. CONCLUSION**

More highly skilled workers in cybersecurity roles would help the nation respond more robustly to the cybersecurity problems it faces. All organizations need to understand their threat environment and the risks they face, address their cybersecurity problems, and hire the most appropriate people to do that work

In today’s world, cyber security is a crucial part of any business. We must understand the importance of annual assessments and following good cyber guidelines. We must understand.

**7. FUTURE SCOPE**

* The National Association of Software and Services Companies (NASSCOM) has estimated that India alone will need about 1 million cybersecurity professionals by the end of 2020 to tackle cybercrime dangers. This has serious implications for the economy at large.
* Cyber Security is an essential component of any company or enterprise across the world, hence the scope of Cyber Security is immense.
* Cyber Security is the technology, process, and practice, designed to protect devices, programs, and data from damages, attacks, and other unauthorized access. Cyber Security is also known as Information Technology Security, focuses on protecting computers, applications, systems and networks from unauthorized access, change, or destruction. The former components are the basic components of any company hence you can imagine what would the scope of cybersecurity be like.
* Many authorized institutions, like the military, government agencies, financial institutions, Banking Sector, etc. have confidential information that is stored on computers and transmitted to networks. With growing cyber-attacks, it has become necessary to protect this sensitive data and personal information. Thousands and millions of Cyber Security professionals will be required to do so.

**8. 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 Organisations – A NetAction Report by Audrie Krause.
4. A Look back on Cyber Security 2012 by Luis corrons – Panda Labs. CIO Asia, September 3rd, H1 2013: Cyber security in malasia by Avanthi Kumar.

.