**COMPUTER ENGINEERING**

**Title of Micro-Project:** Measures to be taken for ensuring cyber security.

## GROUP MEMBERS

|  |  |  |
| --- | --- | --- |
| **ROLL NO** | **CLASS** | **NAME OF MEMBER** |
| 3111 | CO6I | Shreyash Kotain |
| 3112 | CO6I | Darshana Kure |
| 3113 | CO6I | Sahil Mhatre |
| 3114 | CO6I | Omkar Moolya |
| 3115 | CO6I | Aman Pandey |
| 3116 | CO6I | Priyanka Patil |
| 3117 | CO6I | Heramb Pawar |
| 3118 | CO6I | Aditya Raut |
| 3119 | CO6I | Pawan Salve |
| 3120 | CO6I | Ameya Sawant |

**Guide Name**: - Mr. Pramod Patil

Part A Plan

**Title of Micro-Project:** Measures to be taken for ensuring cyber security.

## Brief description: -

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

# Cyber security is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices

* For an effective cyber security, an organization needs to coordinate its efforts throughout its entire information system.

## Aim of Micro-Project: -

The Micro-Project Aims To: -

* Study the importance of cyber security.
* Study the features of cyber security.
* Study the types of cyber security.
* Study the advantages of cyber security.

## Action Plan: -

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr No** | **Detail of Activities** | **Plan**  **Start date** | **Plan end date** | **Name of Team Members** |
| 1 | Group formed according to roll no & group leaders were elected also detailed information on micro project was given |  |  | Heramb Pawar |
| 2 | Finalization of micro project as well as detailed discussion regarding topic |  |  | Ameya Sawant |
| 3 | Planning of micro-project regarding, resources, software used, submission date and completing part a plan of micro  – project |  |  | Darshana Kure |
| 4 | Complete analysis of design part of micro-project & distribution of module among group members |  |  | Priyanka Patil |
| 5 | Getting it finalized by the guide |  |  | Pavan Salve |
| 6 | Implementation of Project report |  |  | Sahil Mhatre |
| 7 | Presentation of 1st part of micro-project Infront of guide by each group member and Preparing of part b plan for micro- project |  |  | Aman Pandey |
| 8 | Submission of micro-project |  |  | Heramb Pawar |

**Resources used: -**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr No** | **Name of Resources Required** | **Specification** | **Quantity** | **Remarks** |
| 1 | Computer | **Processor-**Amd **Hard Disk-**2 Tb **Ram-**16gb **Operating System-** Windows 10 Pro | 1  1  1  1 | Hardware used |
| 2 | Microsoft word | MS office 2010 | -- | Software used |

**PART B**

**Aim of The Project**: Measures to be taken for ensuring cyber security.

## Brief description: -

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

# Cyber security is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices

* For an effective cyber security, an organization needs to coordinate its efforts throughout its entire information system.

## Aim of Micro-Project: -

The Micro-Project Aims To: -

* Study the importance of cyber security.
* Study the features of cyber security.
* Study the types of cyber security.
* Study the advantages of cyber security.

## Course Outcome Integrated:

1. Able to understand the importance of cyber security.
2. Recognize security flaws and use alternative solutions to solve Cybersecurity problems.

## Actual Procedure Followed:

* 1. **Group Formation: -** Management studies include the activities of setting the strategy of an organization and coordinating the efforts of its employees (or of volunteers) to accomplish its objectives through the application of available resources, such as financial, natural, technological, and human resources. The basic aim of micro- project is to accelerate the attainment of the various outcomes in the course. In the first 2 weeks of April the subject was introduced. The syllabus as well as details of micro-project were discussed. A group of 10 members was formed and the group leaders were selected. The schedule of plan “a”,” b” & “presentation of micro-project” were finalized. The various micro-project topics related to subject were discussed our guide gave us the opportunity to select the topic of our choice.
  2. **Finalization of Micro-Project: -** After attending the lectures for 2 weeks. We selected the topic for micro-project. We discussed the topic with our guide regarding the concept which we are going to apply in the project. We individually tried to explain the basic platform of project.
  3. **Planning: -** After finalization of the project we started working on the project. We started the planning phase. We discussed among ourselves regarding the resources such as software requirements. In this week we completed ‘part a plan’ of the micro-project which is nothing but an initial description about the project. We submitted it to the guide.
  4. **Module Distribution &Analysis Part: -** Once the planning was over regarding resources, etc. We finalized the module which we will be writing. According to members we distributed the modules. We started the analysis of project.
  5. **Design Part: -** In this part we focused on designing the structure of the project. We planned to apply some formatting to give an attractive look to the structure.
  6. **Implementation: -** In the week we actually started the technical phase. In this phase we technically applied the formatting as decided. Each member was designing project modules which were assigned to them. Finally, the project was within the schedule time.
  7. **Presentation: -** In this week we had to present the micro-project. Each member of group presented their own parts with confidence in front of guide. He asked us various queries regarding the topics. We explained him about the various components of the project. He asked us to do some changes regarding some topics.
  8. **Submission: -** This week was submission week. We submitted our project along with ‘part a & b plan’ to the guide. We also submitted the hard copies and soft copies of project to the guide.

## Actual Resources Used:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr No** | **Name of Resources Required** | **Specification** | **Quantity** | **Remarks** |
| 1 | Computer | **Processor-**Amd **Hard Disk-**2 Tb **Ram-**16gb **Operating System-** Windows 10 Pro | 1  1  1  1 | Hardware used |
| 2 | Microsoft word | MS office 2010 | -- | Software used |

Measures to be taken for ensuring cyber security

# Abstract

Cyber security are techniques generally set forth in published materials that attempt to safeguard the cyber environment of a user or organization. It manages the set of techniques used to save the integrity of networks, programs and data from unauthorized access. It refers to the body of technologies, processes, and is also known as information technology security. The field is of growing importance due to increasing reliance on computer systems, including smart phones, televisions and the various tiny devices that constitute the Internet of Things.

# INTRODUCTION

The internet has made the world smaller in many ways but it has also opened us up to influences, that have never before been so varied and so challenging. As fast as security grew, the hacking world grew faster. There are two ways of looking at the issue of cyber security. One is that the companies that provide cloud computing do that so these companies will be extremely well secured with the latest in cutting edge encryption technology.

**WHAT IS CYBER SECURITY?**

It’s being protected by internet-connected systems, including hardware, software and data, from cyberattacks. In a computing context, security comprises cyber security and physical security both are used by enterprises to avoid unauthorized access to data center and other computerized systems. The security, which is designed to maintain the confidentiality, integrity and availability of data, is a subset of cyber security.

# WHY DO WE NEED CYBER SECURITY?

The range of operations of cyber security involves protecting information and systems from major cyber threats. These threats take many forms. As a result, keeping pace with cyber security strategy and operations can be a challenge, particularly in government and enterprise networks , in their most innovative form, cyber threats often take aim at secret, political and military assets of a nation, or its people. Some of the common threats are:

* **Cyber terrorism**: It is the innovative use of information technology by terrorist group for their further political agenda. It took the form of attacks on networks, computer systems and telecommunication infrastructures.
* **Cyber warfare:** It involves nation-states using information technology to go through some another nation’s networks to cause damage. In US and many other nations. People live in society, cyber warfare has been acknowledged as the fifth domain of warfare. Cyber warfare attacks are primarily executed by hackers who are well-trained in use of computer networks, and operate under the favorable and support of nation- states. Rather than closing a target’s key networks, a cyber-warfare attack may force to put into a situation into networks to compromise valuable data, degrade communications, impair infrastructural services as transportation and medical services, or interrupt commerce.
* **Cyber siphonage**: It is the practice of using information technology to obtain secret operation without permission from its owners or holders. It is the most often used to gain strategic, economic, military advantage, and is conducted using cracking techniques and malware.

**Measures to Ensure Cyber Security:**

## Maintain an Accurate Inventory of Control System Devices and Eliminate Any Exposure of this Equipment to External Networks:

Never allow any machine on the control network to talk directly to a machine on the business network or on the Internet. Although some organizations’ industrial control systems may not directly face the Internet, a connection still exists if those systems are connected to a part of the network – such as the corporate side – that has a communications channel to external (non-trusted) resources (i.e., to the Internet).

Organizations may not realize this connection exists, but a persistent cyber threat actor can find such pathways and use them to access and exploit industrial control systems to attempt to create a physical consequence. Therefore, organizations are encouraged to conduct thorough assessments of their systems, including the corporate enterprise segments, to determine where pathways exist.

Any channels between devices on the control system and equipment on other networks should be eliminated to reduce network vulnerabilities

* 1. ICS-ALERT-12-046-01A Increasing Threat to Industrial Control Systems (ICS-CERT)
  2. ICS-ALERT-11-343-01A Control System Internet Accessibility (ICS-CERT)
  3. Targeted Cyber Intrusion Detection and Mitigation Strategies (ICS-CERT)

## Implement Network Segmentation and Apply Firewalls:

Network segmentation entails classifying and categorizing IT assets, data, and personnel into specific groups, and then restricting access to these groups. By placing resources into different areas of a network, a compromise of one device or sector cannot translate into the exploitation of the entire system.

Otherwise, cyber threat actors would be able to exploit any vulnerability within an organization’s system – the “weakest chain in the link” – to gain entry and move laterally throughout a network and access sensitive equipment and data. Given the rise of the “Internet of Things” – whereby many previously non-Internet connected devices, such as video cameras, are now linked to systems and the web – the importance of segmenting networks is greater than ever.

Access to network areas can be restricted by isolating them entirely from one another, which is optimal in the case of industrial control systems (as described in recommendation or by implementing firewalls. A firewall is a software program or hardware device that filters the inbound and outbound traffic between different parts of a network or between a network and the Internet. For connections that face the Internet, a firewall can be set up to filter incoming and outgoing information. By reducing the number of pathways into and within your networks and by implementing security protocols on the pathways that do exist, it is much more difficult for a threat to enter your system and gain access to other areas.

Creating network boundaries and segments empowers an organization to enforce both detective and protective controls within its infrastructure. The capability to monitor, restrict, and govern communication flows yields to a practical capability to baseline network traffic (especially traffic traversing a network boundary), and identify anomalous or suspicious communication flows.

These boundaries also provide a means to practically detect potential lateral movement, network foot printing and enumeration, and device communications attempting to traverse from one zone to another.

* Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies (ICS-CERT)
* Why You Need to Segment Your Network for Security (CSO)
* Firewall Deployment for SCADA and Process Control Networks (UK Centre for the Protection of National Infrastructure via ICS-CERT)
* Beginners Guide to Firewalls: A Non-Technical Guide (MS-ISAC)
* Guide to Industrial Control Systems Security – Special Publication 800-82 (NIST)
* Guidelines for Application Whitelisting in Industrial Control Systems (ICS- CERT)

## Use Secure Remote Access Methods:

The ability to remotely connect to a network has added a great deal of convenience for end users, but a secure access method, such as a Virtual Private Network (VPN), should be used if remote access is required. A VPN is an encrypted data channel for securely sending and receiving data via public IT infrastructure (such as the Internet). Through a VPN, users are able to remotely access internal resources like files, printers, databases, or websites as if directly connected to the network. This remote access can further be hardened by reducing the number of Internet Protocol (IP) addresses that can access it by utilizing network devices and/or firewalls to specific IP addresses and/or ranges and from within the U.S. Note that a VPN is only as secure as the devices connected to it. A laptop computer infected with malware can introduce those vulnerabilities into the network, leading to additional infections and negating the security of the VPN.

* 1. Configuring and Managing Remote Access for Industrial Control Systems (ICS-CERT)
  2. Extending Your Business Network through a Virtual Private Network (SANS Institute)
  3. Virtual Private Networking: An Overview (Microsoft)

## Establish Role-Based Access Controls and Implement System Logging:

Role-based access control grants or denies access to network resources based on job functions. This limits the ability of individual users – or attackers – to reach files or parts of the system they shouldn’t access. For example, SCADA system operators likely do not need access to the billing department or certain administrative files. Therefore, define the permissions based on the level of access each job function needs to perform its duties, and work with human resources to implement standard operating procedures to remove network access of former employees and contractors. In addition, limiting employee permissions through role-based access controls can facilitate tracking network intrusions or suspicious activities during an audit.

Implementing a logging capability allows for the monitoring of system activity. This enables organizations to conduct thorough root cause analyses to find the sources of issues in the system, which may have been the activities of an employee or an outsider. Monitoring network traffic also allows organizations to determine if a user is making unauthorized actions or if an outsider is in the system, which provides an opportunity to intervene before problems are manifested.

* 1. Role Based Access Control and Role Based Security (NIST)
  2. An Introduction to Role Based Access Control (NIST)
  3. Extending Role Based Access Control (SANS Institute)
  4. Targeted Cyber Intrusion Detection and Mitigation Strategies (ICS-CERT)

## Use Only Strong Passwords, Change Default Passwords, and Consider Other Access Controls:

Use strong passwords to keep your systems and information secure, and have different passwords for different accounts. Hackers can use readily available software tools to try millions of character combinations to attempt an unauthorized login – this is called a “brute force attack.” Passwords should have at least eight characters, but longer passwords are stronger, because of the greater number of characters to guess. Also, include uppercase and lowercase letters, numerals, and special characters. Change all default passwords upon installation of new software, particularly for administrator accounts and control system devices, and regularly thereafter. Implement other password security features, such as an account lock-out that activates when too many incorrect passwords have been entered. Organizations may also consider requiring multi-factor authentication, which entails users verifying their identities – via codes sent to devices they previously registered – whenever they attempt to sign-in.

* 1. Choosing and Protecting Passwords (US-CERT)
  2. Supplementing Passwords (US-CERT)
  3. Strong Passwords (Microsoft)

## Maintain Awareness of Vulnerabilities and Implement Necessary Patches and Updates:

Most vendors work diligently to develop patches for identified vulnerabilities. But even after patches and updates have been released, many systems remain vulnerable because organizations are either unaware of or choose to not implement these fixes. In its 2016 Data Breach Investigations Report, Verizon found that in most industries, three quarters of incidents and breaches are covered by only three patterns. For utilities, these patterns were cyber espionage, crimeware, and denial of service. Among its recommendations, understanding the building blocks of an attack (e.g., a kill chain) can help construct defenses and detect a breach. Effective patching can also stop a large portion of attacks considering the top 10 cyber vulnerabilities accounted for 85% of successfully exploited traffic.

Cisco’s 2016 Annual Security Report stated that security professionals must rethink their defense strategies as cyber criminals have refined their infrastructures to carry out attacks in more efficient and profitable ways. The report also covered global threat intelligence and insights on possible future criminal behavior, ransomware, risks of aging IT infrastructure, and geopolitical concerns for internet governance.

To protect one’s organization from these opportunistic attacks, a system of monitoring for and applying system patches and updates should be implemented. Water ISAC regularly posts information on vulnerabilities and patches, which it receives from its partners at the U.S. Department of Homeland Security’s ICS-CERT and United States Computer Emergency Readiness Team (US- CERT), other ISACs, and cybersecurity firms, among others. Where possible, organizations should also consider setting systems and software to auto-update to avoid missing critical updates. These updates are designed to fix known vulnerabilities and are encouraged for any Internet-connected device.

* 1. Recommended Practice for Patch Management of Control Systems (ICS- CERT)
  2. Software Update Management Guidelines (Microsoft)
  3. Index of Advisories by Vendor (ICS-CERT)
  4. Top 30 Targeted High-risk Vulnerabilities (US-CERT)

## Develop and Enforce Policies on Mobile Devices:

The proliferation of laptops, tablets, smartphones, and other mobile devices in the workplace presents significant security challenges. The mobile nature of these devices means they are potentially exposed to external, compromised applications and networks and malicious actors. Further contributing to this challenge is the increasing trend of organizations allowing employees to use their personal electronic devices for work purposes, known as the “Bring Your Own Device (BYOD)” phenomenon.

Therefore, it’s important to develop policies on the reasonable limits of mobile devices in your office and on your networks. These measures should be strictly enforced for all employees, as well as for contractors. Devices should also be password protected to ensure only authorized users can log-in. Otherwise, an unauthorized user can gain access to restricted networks and files using an authorized user’s device. Similarly, employees should avoid or be cautious about using devices that do not belong to them as they cannot be sure these are properly protected or comply with established policy. Such devices may actually be infected, and using them could put the information and networks you access at risk.

* 1. Cybersecurity for Electronic Devices (US-CERT)
  2. Guidelines on Cell Phone and PDA Security (NIST)
  3. Guidelines for Managing the Security of Mobile Devices on the Enterprise (NIST)
  4. Guide to Enterprise Telework, Remote Access, and BYOD Security (NIST)
  5. User’s Guide to Telework and BYOD Security (NIST)
  6. Bring Your Own Device (BYOD) Design Considerations Guide (Microsoft)

## Implement an Employee Cybersecurity Training Program:

Cybersecurity for critical infrastructure sectors that operate industrial control systems, such as the water and wastewater sector, is extremely important given that these systems are increasingly being targeted. When employees aren’t involved in cybersecurity, not only can vulnerabilities and threats go unnoticed but the employees themselves can become conduits through which attacks are executed. Therefore, employees should receive initial and periodic cybersecurity training, helping to maintain the security of the organization as a whole.

While cybersecurity is an expansive field, there are certain topics that should be emphasized for general awareness. One such topic is social engineering, which continues to be a popular means for cyber criminals to prey upon unsuspecting employees. These methods involve emails (“phishing”), phone calls, or other types of personal interactions in which malicious actors attempt to entice employees into providing sensitive personal or corporate information, such as account passwords or details about information technology infrastructure.

Alternatively, these actors might attempt to make employees perform specific actions, such as pay for alleged services, download infected attachments, or visit malicious websites. Unsolicited emails, phone calls, and other correspondence from unknown senders should be viewed with particular caution.

Among the key points in Booz Allen Hamilton’s Industrial Cybersecurity Threat Briefing for 2016, one-third of ICS operators around the world were breached in 2015 and spear phishing was the primary method of attack. In spear phishing incidents, the vulnerabilities were the users who were comprised through social engineering. According to its survey, the water and dam’s sectors totaled 31 incidents in 2015. The primary threats included nation-states (specifically China, Russia, North Korea, and Iran), ransomware targeting ICS operators, the sale of access to SCADA systems as a service, freely available attack resources, attacks against the supply chain, and improper access control. The briefing included detailed descriptions of incidents per sector, and mitigation practices.

Training should also incorporate the importance of smart Internet browsing practices. Visiting suspicious websites may expose users to infection by malware embedded on the site (a “drive-by-download” attack). Even legitimate websites, as well as the files on them, may be compromised. Cyber attackers employ a variation of this type of tactic, a “watering-hole” attack, to target the employees of a company they know will visit the website. Therefore, caution should be exercised no matter where a user navigates and the materials that are downloaded.

* Avoiding Social Engineering and Phishing Attacks (US-CERT)
* Recognizing and Avoiding Email Scams (US-CERT)
* Securing Your Web Browser (US-CERT)
* Preparing for Cyber Incident Analysis (ICS-CERT)
* Best Practices for Dealing with Phishing and Ransomware (Osterman Research)
* Five Tips to Help Execute an Employee Training Program (Help Net Security)

## Involve Executives in Cybersecurity:

Despite the continued proliferation of cyber threats and the far- reaching effects cyberattacks can have, researchers have found that organizational leaders often lack sufficient awareness of cybersecurity threats and needs. Cyphort and the Ponemon Institute published a study in March 2016 titled The State of Malware Detection and Prevention that identified serious challenges organizations face in preventing and detecting cyberattacks and prioritizing and investigating malware alerts. Only 36 percent of respondents say IT security and others who are responsible for security have the necessary information to make the C-suite aware of advanced threats. The report also notes that 34% of respondents say C-level executives are never updated on security incidents.

While organizations are increasingly elevating cybersecurity to the executive level by adding the role of Chief Information Security Officer (CISO), many organizations remain unprepared for cyber threats. IBM’s paper, Securing the C- Suite, surveyed 700 executives worldwide to assess non-technical executives’ understanding of cyber threats. According to the results, there are four signs that an organization is not prepared for cybersecurity threats. These involve the misidentification of the actual threats, the lack of a chief information security officer (CISO), not including all C-suite members in cybersecurity planning, and a reluctance to share information about cybersecurity threats with external organizations.

* 1. Cybersecurity Questions for CEOs (US-CERT)
  2. ICS Cybersecurity for the C-Level (ICS-CERT)

1. **Measures for Detecting Compromises and Develop a Cybersecurity Incident Response Plan:**

Despite the many preventative measure’s organizations implement, many still experience compromises. Indeed, many cybersecurity experts have noted that experiencing a compromise is not really a question of “if,” but more of a question of “when.” When a compromise occurs, the organizations that fare the best will be those that quickly detect the issue and have a plan in place to respond.

Implementing such measures as intrusion detection systems (IDSs) and intrusion prevention systems (IPSs), anti-virus software, and logs (previously described in recommendation 4) can help to detect compromises in their earliest stages. Most IDSs and IPSs use signatures to detect port scans, malware, and other abnormal network communications. New viruses are discovered every day, and anti-virus programs are oftentimes set to automatically update themselves to look for the latest threat signatures. Still, administrators should not rely solely on anti-virus software for detecting infections. Logs from firewalls, intrusion detection and prevention sensors, and servers should be monitored for signs of infections.

Incident response plans are a critical yet underutilized component of emergency preparedness and resilience. An effective cybersecurity response plan will limit damage, increase the confidence of partners and customers, and reduce recovery time and costs. Plans should include measures for reacting to destructive malware in an ICS environment. In such situations, organizations should be prepared to “island” their ICS environments by disconnecting from non-ICS networks. They should also be capable of going to “manual operations” if network conditions impact visibility from the SCADA system, or if malware potentially renders control devices inoperable via an automated means.

Rather than being developed by a single entity, the plan should be a product of collaboration between all departments that would be stakeholders in a cybersecurity incident. This will ensure a cooperative and unified response that leverages all of an organization’s resources to the greatest extent possible. For enhanced responsive capability in the event of a cybersecurity incident, organizations should consider forming a Computer Security Incident Response Team (CSIRT).

This task is not complete once the plan has been developed; it needs to be operationalized as well. It is critical that plans be routinely reviewed and updated to ensure they remain relevant and useable for when they are actually needed. Furthermore, to truly understand their cybersecurity incident response plan, organizations must practice them through regular exercises. This will ensure that all stakeholders understand the procedures that would be implemented in the event of a significant cyber disruption or breach, enabling a more effective and efficient response.

* Malware Threats and Mitigation Strategies (US-CERT)
* Developing an ICS Cybersecurity Incident Response Capability (ICS-CERT)
* Nine Steps for A Successful Incident Response Plan (CSO Online)
* Ten Steps to Planning an Effective Cyber-Incident Response (Harvard Business Review)
* Create a CSIRT (CERT)
* Best Practices for Continuity of Operations (ICS-CERT)
* Five Useful Tips to Build a Successful and Mature Security Operations Center (IBM)
* How Incident Response Fails in ICS Networks (Dark Reading)

**References:**

We do have used a few references during the process of building our project. The references used are from Websites, Books etc.

The references used are:

## Websites:

1: [www.waterisac.org](http://www.waterisac.org/)

2: [www.en.wikipedia.org](http://www.en.wikipedia.org/wiki/Operating)

3: [www.tutorialspoint.com](http://www.tutorialspoint.com/)

## Reference Books:

1: Security engineering.

2: Cybersecurity.

## Skill Developed/Learning Out of This Micro Project:

* Since we worked in a group, we developed the skill of ‘TEAMWORK’ in us.
* We learnt in brief about concept, purpose, importance of cyber security.

**Conclusion**

* + Cybersecurity or information technology security is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. Cyber security is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of