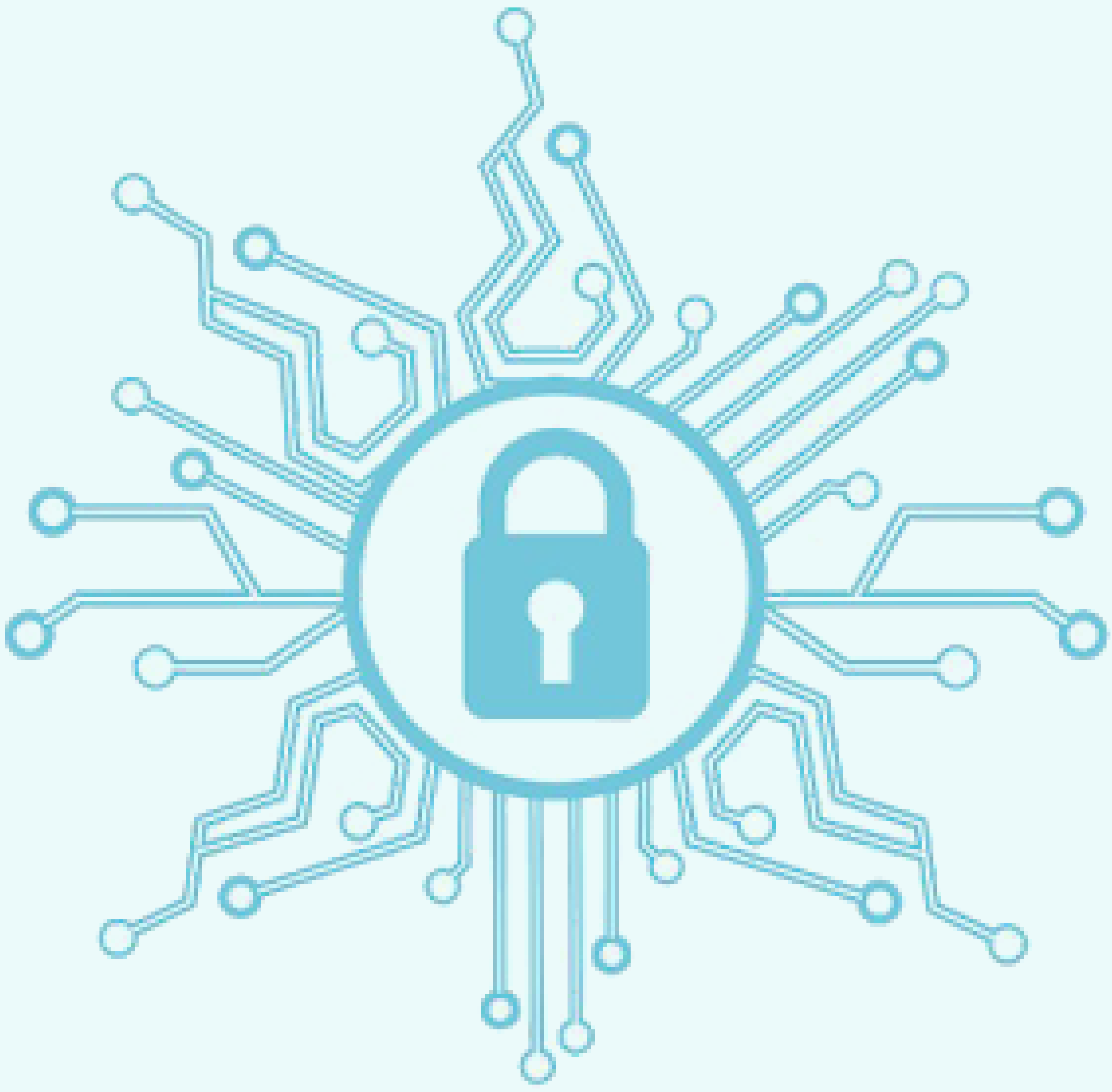
AICTE CYBERSECURITY STRATEGY FOR HIGHER EDUCATION INSTITUTES

All India Council for Technical Education
AICTE
योगः कर्मसु कौशलम्

Table of content



ALL INDIA COUNCIL FOR TECHNICAL EDUCATION

(A Statuary Body of the Govt. of India)
Ministry of Education, Govt of India

AICTE CYBERSECURITY STRATEGY FOR HIGHER EDUCATION INSTITUTES

1. Vision

India is steadily becoming a technology powerhouse, 34% of India's population comprises millennials, Indian millennials, and Gen Z are the brightest spots among their global peers. As the job market shifts dramatically, and technology skills become central to every job, it was imperative for our education modules to adopt a new way of communication, business, and living.

A secure digital India is capable of advancing India's economic prosperity and national security through innovative cybersecurity education, training, and awareness on a higher education level that addresses the full spectrum of cybersecurity.

Higher education institutions possess massive amounts of data and face a constant deluge of cyberattacks, including personal information about students, faculty, staff, intellectual property, research data, innovation data, and donors, making them tempting targets for hackers and other digital criminals. The cyberattack risk increases with the emphasis on openness and collegiality that colleges and universities cultivate, challenging them to develop and enforce methods to protect vital data.

For the Indian context, cybersecurity at the national level is a complex concept with various dimensions. Each dimension can be addressed by prioritizing the most important objectives.

Perhaps even more significant than potential financial losses, cyber-attacks pose a grave threat to a university's reputation and the safety of its students.

India's National Cyber Security Strategy for Higher Education 2020 is being formulated to shape the next generation of the country's security posture in cyberspace, we must embrace this opportunity to move beyond perimeter-based, reactive, threat-centric approaches in favor of behavior-centric methods that put human nature at the forefront of cyber defenses.

Mission

To enhance the overall cybersecurity posture of Higher Education of India.

Goals

- Create Dynamic Cybersecurity policies for students and institutes
- Translate policy statements into an action plan
- Raise National awareness about risks in Cyberspace
- Create Nationwide students and faculty cybersecurity experts

Section 1. Create Dynamic Cybersecurity policies for students and institutes

User accounts and Administration

(a) Students and faculty should use their own accounts and maintain cyber sanitization as per Institutes instructions.

(b) Maintain required account management policies and should not tamper with their own requirements.

(c) Students should inform institutes about any type of misconfiguration found in their accounts. Teachers should also follow the same.

(c) Students should inform institutes about any type of misconfiguration found in their accounts. Teachers should also follow the same.

(d) Students and teachers should maintain their entry/exit information correctly.

(e) Students and faculty should not make any type of user account bypassing techniques and follow all rules as per IT Act 2000.

(f) Students and faculty should follow every instruction of institutes about their user account management.

3. ACADEMIC POLICY AND STRATEGY OF CYBERSECURITY AND MANAGEMENT

General user accounts

(a) General purpose users should access their accounts as per instruction of faculty.

(b) Users should not try to install unwanted software/programs without prior permission of Institutes/faculty.

(c) Users should accept time to time policy implementations and follow the rules as per the guidance of faculty.

(d) Students/teachers should not use these accounts for social media/personal purposes.

(e) Students/teachers should not save unwanted images and files in this account.

(f) Students/teachers should not access other data with the help of these accounts.

Special user accounts

(a) Students should not access this account without prior permission of faculty.

(b) Any discrepancy in these accounts should be treated as a punishable offense.

(c) Credentials of these accounts should be kept with the lab in charge.

(d) Passwords of these accounts should be changed periodically.

Physical Security

(a) Users should maintain the physical security of the system.

(b) Users and lab assistants should monitor the lab and its premises from time to time.

(c) They should make a close watching procedure on CCTV cameras and should maintain CCTV cameras in good working conditions.

(d) Lab in-Charges should ensure security management of entrance and exit of lab premises.

(e) Lab in-Charges should keep the necessary records of lab timing and asset management.

Password handling

(a) Password records should be maintained.

(b) Password policy should be implemented fortnightly.

(c) Passwords of each account should be kept in common records on different pages.

User and access rights assignment

(a) Administrator accounts should be maintained by Institutes.

(b) Administrators should implement security policies as per requirement.

(c) Administrator should audit all computers and keep records.

(d) Access to information and information processing facilities shall be provided after due process of identification, authentication, and authorization. Access to information assets shall be controlled.

(e) The access to information and Information Systems shall be according to the principles of least privilege and "need to know basis" to authorized users.

(f) Access to information and Information systems shall be regulated using unique User IDs, Users access to information assets shall be reviewed at regular intervals. Format procedures for user access management shall be documented and communicated.

Unauthorized Data

Unauthorized data like personal documents, presentations, multimedia files, etc. will not be stored within the official system or hosted on official websites.

3.1 DATA SECURITY

Database Administrator

A database administrator will be nominated by the institution who will be responsible for all database functions and manages the user authorized list and deals with the management of all the data stored in the database. No default roles will be commenced.

Data Classifications

(a) Restricted Data: Information should be classified as Restricted when the unauthorized disclosure, alteration, or destruction of that data could cause a significant level of risk to the University or its affiliates.

(b) Private Data: Data should be classified as Private when the unauthorized disclosure, alteration, or destruction of that data could result in a moderate level of risk to the University or its affiliates.

(c) Public Data: Data will be classified as Public when the unauthorized disclosure, alteration, or destruction of that data would result in little or no risk to the University and its affiliates. Examples of Public data include press releases, course information, and research publications. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

Multi-Level Authentication

The process by which more than one factor of authentication is needed to verify the identity of a client requesting access to resources. There are three common factors of authentication: something you know (e.g. password, pin, etc.), something you have (e.g. smart card, digital certificate, etc.), and something you are (e.g. fingerprint, retinal pattern, etc.). Use of single-factor authentication (username and password combination) is sufficient, even if multiple level authentication is required.

Failed Login attempts

Logs for all successful/failed login attempts will be maintained and reviewed regularly. Account lockout policy should be configured for locking the user account after 5 failed attempts by the user.

Privileged Users

Users who can alter the configuration of the system, specifically, the security configuration. This definition is intentionally vague to allow the flexibility to accommodate varying systems and authentication mechanisms. In a traditional Microsoft Windows environment, members of the Local Administrators, Domain Administrators, and Enterprise Administrators groups would all be considered to have privileged access. In a traditional UNIX or Linux environment, users with root-level access, or the ability to do would be considered to have privileged access. In an application environment, users with 'super-user' or system administrator roles and responsibilities would be considered to have privileged access.

Software Configuration and Change Control

(a) All changes in hardware, software, and their configuration will be analyzed, approved, and carried out in a controlled manner under supervision.

(b) System formatting, Recovery, Repair and Restore permission from appropriate authority must be taken in prior to format, recovery, repair, or restoration of information system assets including computers and laptops, external storage disks, etc.

Data Security and ownership backup

Ownership of data stored within the database will rest with the database administrator and the security of the data will be ensured by the database administrator. There may be instances where the application is able to generate information of much higher significance than the information fed to the database. Responsibility for the security of any such information prepared by collating base data will be of the authorized user who is authorized to access the collated/aggregated information. Backup of data will be taken and tested regularly as per the backup policy of the establishment and criticality of the information.

3.2 NETWORK AND COMMUNICATION SECURITY

Rules to access both internal and external network servers/resources:

(a) Use of network services and its resources will be formulated by the head of the Cyber team and national IT security policy. The policy clears the methodology that users must follow to access authorized networks and resources.

(b) Equipment like network devices and terminals will be configured to automatically identify the device on a network. Devices must confirm its identity to complete the handshake with network devices.

(c) Usage of third-party applications for remote access on a network, like zoom meetings, Teams, Webex, and VNC should be avoided on official networks.

d) Routing restrictions must follow within the network connections to secure the valuable information of the college/university.

(e) Device management on a network like a switch, Medium Access Control MAC, and IP binding must be implemented and minimize the usage of ports within the network switches deployed over a network.

Remote access to a network

Remote access to the sources on the LAN side of the network of any institution will only be permitted for pre-designed and authorized users only. The privileges granted for remote access need to be restricted. Permission for such remote access, if required, will be given by specified authorities.

File Transfer Protocol (FTP)

Users of insecure FTP services are not recommended. However, the use of secure FTP services may be configured using network technologies like secure socket layer/transport layer security (SSL/TLS) protocols.

Mobile Phone Usage

(a) Mobile /Smart Phones and smartwatches /wearable devices with data connectivity are prone to be exploited for exfiltration /siphoning of information of remote locations/ servers without the knowledge of the user. Moreover, mobile phones with GPS facilities can be tracked in real time without the knowledge of the user.

(b) The risk posed by mobile phones is proportional to the various advanced features integrated within the device. Inbuilt features like camera, data storage capability (fixed and removable), Bluetooth, NFC, infrared port, Wi-Fi, and GPS cannot be completely disabled and pose a threat to data and location security.

3.3 SECURITY ZONE ASSIGNMENT

Hardware and Software Asset Protection and Management

(a) Hardware Protection and Management:

(i) Management of IT Assets: Glossary of IT hardware and peripherals will be managed and protected by Cybersecurity officers and Network Administrators who are appointed and elected by governing bodies of a college or university at all levels. Usage and Accountability of IT assets, logbooks will be maintained by college

(ii) Data drain and destruction: Damaged optical media, tapes, hard disks System logs, printouts, printer ribbons, printer cartridges should be destroyed in a secure manner. Records will be kept for the equipment by the college/university.

(iii) Backup of Important Information/Data: Secure data, data backup, and the system should be taken timely. Backup data to be stored in a fire and waterproof container or a safe and safeguard against natural disasters.

(b) Software Protection and Management: -

(i) Only licensed versions of OS (Windows/ Linux application) and custom software (MS Office, Adobe) should be used. Users should not install any OS other than provided by the Administrator and the administrator ensures the hardening of computers and servers. Dual boot and virtualized OS installation are strictly prohibited.

(ii) Application software should be licensed and should be periodically checked by the administrator and issuing authority.

(iii) Software patch management of OS, security software, applications, web browsers, is one of the best protection methods against malware and other online threats. User/system administrators should check periodically whether all softwares are regularly updated with genuine patches.

(iv) Pirated Software: Since pirated software is embedded with malicious codes and cannot be updated, the use of pirated unlicensed /cracked software is strictly prohibited within the official system.

Server Room Protection

(a) Multi-level authentication including biometric authentication to restrict access by unauthorized personnel. Two-factor authentication is required for PCs handling important data.

(b) Features like camera Wi-Fi, voice recording, Bluetooth, GPS, and geotagging must be disabled on all official devices like computers, Laptops, and Tablets. Cordless mouse, Keyboard, and presenters are, however, allowed to be used.

Power Damage Prevention

Power loss can lead to vital data loss and in some cases, it may even lead to system crash/failure. So, IT equipment should be protected from power failures and other disruptions. Standby arrangements, in terms of uninterrupted power supply and backup power, shall be used.

Storage Media

Strict control is required to be exercised in the use of mass storage devices such as CD/DVD writers and Ethernet-based hard drives/ Network Attached Storage (NAS) Drives. Explicit authority to specified persons must be issued for usage of these devices and a periodic check of accounting procedure should be undertaken. Cybersecurity audits must ensure a comprehensive check of all related security aspects.

3.4 SECURITY AUDIT AND INCIDENT HANDLING

Security Audit:

(a) Cyber Security Audits will be forced at all educational institutions to ensure and follow cybersecurity policies and advisories issued by AICTE and National IT security policy. AICTE nominated a Chief Security Audit Officer (CSAO) and a team of members to conduct an audit periodically as per the advisory.

(b) Audit will be conducted by institutions, colleges/universities four times in a year. Chief Security Audit Officer (CSAO) is responsible for periodically reviewing/arranging to review the levels of information and cybersecurity and its implementation across colleges /universities and institutions. The internal audit team may obtain the necessary support from the Information Security Team to carry out the audit work.

How to Manage the Response to an Information Security Incident

To ensure effective management of information and cybersecurity incidents, including responding to a cyber crisis, and preservation of digital evidence.

(a) A formal information and cyber incident management shall be established to discover, record, respond to escalate and prevent information security events and weakness effectively

(b) A Cyber Security Cell shall be established to monitor the critical IT infrastructure and information systems of institutions to provide analysis, intelligence, and response for different information and cybersecurity threats to the latest projects and classified documents of institutions. Monitoring of threats shall also consider threat intelligence and advisories.

(c) All users of information systems including suppliers shall report any security breach or attempt to breach and security weakness in information systems to a designated authority.

(d) Cyber crisis Management Plan shall be designated and implemented for an effective response to cyber crisis incidents. Only Authorized officials shall report information on cyber security incidents to outside authorities when such reporting is required to comply with legal, statutory, regulatory requirements.

Breach of Physical Security

(a) Access security such as access cards, biometric access devices, controlled entry points, and manned reception will be used to establish secure entry.

(b) Protection from environmental threats: precautions against fire accidents, lightning, and all other types of natural or man-made disasters will be taken, all data processing facilities and complexes shall be equipped with proper firefighting systems, automatic smoke detectors, and temperature monitoring sensors to prevent

Section 2: Translate policy statements into action

4. Threats

A large variety of cyber threats, aimed at obtaining confidential information, pose great threats to data users. Chief Information Security Officers (CISOs) are responsible for protecting, securing, and storing gigantic amounts of data, including financial aid applications, sensitive research information, intellectual property, information within online learning portals, operational data, and more. It is recommended that CISOs work closely with cybersecurity teams on the internal and external levels to prevent, protect, mitigate, respond to, and recover from the vanity of cyber threats to networks and systems.

(a) Denial of Service (DoS): During the DoS attacks, individuals who are normally granted access to systems or networks are suddenly denied the ability to view data or systems. This can include emails, Websites, learning accounts, etc.

(b) Malware: When an unrequested software is installed on an individual's computer or on a server; its access(unauthorized) will be restricted causing a system crash, it can be considered malware. As recent events have shown, these malware threats are often used as a means to steal information and to commit fraud, including extortion.

(c) Phishing: When it comes to cybersecurity, research shows that the most common threat to everyday Internet users is actually one of the oldest types-phishing (INFOSEC Institute, n.d.), which occurs when attempts at obtaining PII are made by malicious individuals or groups (USCERT, n.d.). Phishing victims are targeted via unscrupulous email messages that hyperlink to fraudulent Websites via which users are prompted to disclose PII such as addresses, usernames, and passwords. Implementing cybersecurity training and emphasizing individual preparedness are the best defense against phishing attacks, as they target individuals in many cases.

(d) Spear Phishing Attacks:
Spear phishing is an email aimed at a particular individual or organization, desiring unauthorized access to crucial information. These hacks are not executed by random attackers but are most likely done by individuals out for trade secrets, financial gain, or military intelligence.

Spear phishing emails appear to originate from an individual within the recipient's own organization or someone the target knows personally. Quite often, government-sponsored hacktivists and hackers perform these activities. Cybercriminals also carry out these attacks with the aim of reselling confidential data to private companies and governments. These attackers employ social engineering and individually-designed approaches to effectively personalize websites and messages.

Useful Link: https://phoenixnap.com/blog/what-is-spear-phishing-definition-prevention

Ransomware:

Ransomware blocks access to a victim's data, typically threatening to delete it if a ransom is paid. There is no guarantee that paying a ransom will regain access to the data. Ransomware is often carried out via a Trojan delivering a payload disguised as a legitimate file.

Useful Link: https://phoenixnap.com/blog/preventing-detecting-ransomware-attacks

SQL Injection:

SQL injection, also known as SQLI, is a kind of attack that employs malicious code to manipulate backend databases to access information that was not intended for display. This may include numerous items including private customer details, user lists, or sensitive company data.

SQLI can have devastating effects on a business. A successful SQLI attack can cause deletion of entire tables, unauthorized viewing of user lists, and in some cases, the attacker can gain administrative access to a database. These can be highly detrimental to a business. When calculating the probable cost of SQLI, you need to consider the loss of customer trust in case personal information like addresses, credit card details, and phone numbers are stolen.

Although SQLI can be used to attack any SQL database, the culprits often target websites.

Useful Link: https://phoenixnap.com/blog/what-is-sql-injection-attack-prevent

Password Attack:

A password attack simply means an attempt to decrypt or obtain a user's password with illegal intentions.

Crackers can use password sniffers, dictionary attacks, and cracking programs in password attacks. There are few defense mechanisms against password attacks, but usually, the remedy is inculcating a password policy that includes a minimum length, frequent changes, and unrecognizable words.

Password attacks are often carried out by recovering passwords stored or exported through a computer system. The password recovery is usually done by continuously guessing the password through a computer algorithm. The computer tries several combinations until it successfully discovers the password.

Eavesdropping Attack:

Eavesdropping attacks start with the interception of network traffic.

An Eavesdropping breach, also known as snooping or sniffing, is a network security attack where an individual tries to steal the information that smartphones, computers and other digital devices send or receive. This hack capitalizes on unsecured network transmissions to access the data being transmitted. Eavesdropping is challenging to detect since it doesn't cause abnormal data transmissions.

These attacks target weakened transmissions between the client and server that enables the attacker to receive network transmissions. An attacker can install network monitors such as sniffers on a server or computer to perform an eavesdropping attack and intercept data as it is being transmitted. Any device within the transmitting and receiving network is a vulnerability point, including the terminal and initial devices themselves. One way to protect against these attacks is knowing what devices are connected to a particular network and what software is run on these devices.

Birthday attack:

The birthday attack is a statistical phenomenon that simplifies the brute-forcing of one-way hashes. It is based on the birthday paradox that states that for a 50 percent chance that someone shares your birthday in any room, you need 253 individuals in the room. However, for a chance higher than 50 percent, you only require 23 people. This probability works because these matches depend on pairs. If you choose yourself as one of the pairs, you only need 253 people to get the required number of 253 pairs. However, if you just need matches that don't include you, you only need 23 people to create 253 pairs when cross-matching with each other. Thus, 253 is the number you need to acquire a 50 percent probability of a birthday match in a room.

Brute-Force and Dictionary Network Attacks

Dictionary and brute-force attacks are networking attacks whereby the attacker attempts to log into a user's account by systematically checking and trying all possible passwords until finding the correct one.

The simplest method to attack is through the front door since you must have a way of logging in. If you have the required credentials, you can gain entry as a regular user without creating suspicious logs, needing an unpatched entry, or tripping IDS signatures. If you have a system's credentials, your life is even simplified since attackers don't have these luxuries.

The term brute-force means overpowering the system through repetition. When hacking passwords, brute force requires dictionary software that combines dictionary words with thousands of different variations. It is a slower and less glamorous process. These attacks start with simple letters such as "a" and then move to full words such as "snoop" or "snoopy."

Brute-force dictionary attacks can make 100 to 1000 attempts per minute. After several hours or days, brute-force attacks can eventually crack any password. Brute force attacks reiterate the importance of password best practices, especially on critical resources such as network switches, routers, and servers.
Learn more about Brute Force attacks.

4.1 Insider Threats:

Not every network attack is performed by someone outside an organization.

Inside attacks are malicious attacks performed on a computer system or network by an individual authorized to access the system. Insiders that carry out these attacks have the edge over external attackers since they have authorized system access. They may also understand the system policies and network architecture. Furthermore, there is less security against insider attacks since most organizations focus on defending against external attacks.

Insider threats can affect all elements of computer security and range from injecting Trojan viruses to stealing sensitive data from a network or system. The attackers may also affect the system availability by overloading the network or computer processing capacity or computer storage, resulting in system crashes.

Man-in-the-Middle (MITM) Attacks:

Man-in-the-middle (MITM) attacks are a type of cybersecurity breach that allows an attacker to eavesdrop a communication between two entities. The attack occurs between two legitimate communicating parties, enabling the attacker to intercept communication they should otherwise not be able to access. Thus the name "man-in-the-middle." The attacker "listens" to the conversation by intercepting the public key message transmission and retransmits the message while interchanging the requested key with his own.

The two parties seem to communicate as usual, without knowing the message sender is an unknown perpetrator trying to modify and access the message before it is transmitted to the receiver. Thus, the intruder controls the whole communication.

AI-Powered Attacks:

The concept of a computer program learning by itself, building knowledge, and getting more sophisticated may be scary.

Artificial intelligence can be easily dismissed as another tech buzzword. However, it is already being employed in everyday applications through an algorithmic process referred to as machine learning. Machine learning software is aimed at training a computer to perform particular tasks on its own. They are taught to accomplish tasks by doing them repeatedly while learning about certain obstacles that could hinder them.

AI can be used to hack into many systems including autonomous vehicles and drones, converting them into potential weapons. AI makes cyber-attacks such as identity theft, password cracking, and denial-of-service attacks, automated, more powerful, and efficient. It can also be used to kill or injure people, steal money, or cause emotional harm. Larger attacks can as well be used to affect national security, shut down hospitals, and cut power supplies to entire regions.

When facing cyber threats, cybersecurity mitigation and response teams identify risks and cyber threat areas; protect and implement safeguards; detect cybersecurity threats; respond to a potential incident or threat; and recover and restore capabilities. In the following sections, we will overview how to incorporate these guidelines into the preparation (prevention, protection, and mitigation), response, and recovery processes.

4.2 Preparing for Threats:

Preparing for cyber threats involves the implementation of a variety of prevention, protection, and mitigation strategies for use by students, faculty, and staff. It is a continuous process that requires CISOs, cybersecurity staff, and emergency management teams to constantly monitor new and emerging technologies, trends, and Information security techniques. The following are some steps that IHEs can take to prepare for cyber threats that may impact higher ed networks and systems.

Securely store data: As described in the previous section, most cyber-attacks and threats target data, which is why cybersecurity, emergency management, and IT staff; administrative and financial aid staff; and faculty and students must all take steps to secure data that, if breached, cloud negatively impact an IHE's reputation, operations, and/or finances. A major element of secure data storage involves the performance of regular data backups. Even if a cyber attacker is successful in retrieving data, data backups can help cybersecurity teams "go back in time" in order to help confirm which systems, applications, etc. were compromised, which will in turn help IHE administrative staff communicate pertinent information to those affected.

Create access control lists and firewalls: Controlling access is a great mitigation technique to use in the open BYOE environment on campuses, and it is one that many institutions are already using. Accessing control lists and firewalls make it easier for IT and cybersecurity staff when they are providing user and/or investigative support before, during, and after a data breach. It is recommended that lists are reviewed on a regular basis to ensure they do not include staff who have transitioned out of positions and to add new staff joining.

Develop policies on secure deployment, maintenance, and responsible/acceptance There are a lot of players in higher ed cybersecurity prevention, protection, and mitigation. They include IT staff, emergency management teams, cybersecurity professionals, as well as faculty, students, and visitors. Policies that clearly outline what to do and what not to do when performing specific actions can help prevent cyber-attacks. For example, IT staff should understand Federal, state, and local regulations related to ensuring information security, privacy, and the secure storage of PII before being assigned to support deployment and/or maintenance teams. Those regulations, along with procedures related to secure deployment and maintenance, can be included in policies outlined in a Cybersecurity Annex within higher ed emergency operations plans (EOPs). Furthermore, it is recommended that existing faculty, students, and visitors receive regular notifications and reminders related to responsible cyber use and that responsible use policy are shared in the orientation packets of new faculty, staff, and students.

security, privacy, and the secure storage of PII before being assigned to support deployment and/or maintenance teams. Those regulations, along with procedures related to secure deployment and maintenance, can be included in policies outlined in a Cybersecurity Annex within higher ed emergency operations plans (EOPs). Furthermore, it is recommended that existing faculty, students, and visitors receive regular notifications and reminders related to responsible cyber use and that responsible use policy are shared in the orientation packets of new faculty, staff, and students.

Monitor network carefully: With the recent proliferation of cyber attacks and threats, network monitoring has likely become a regular activity within THE IT departments, performing vulnerability scan may be one technique that IHE IT and cybersecurity staff use to assess risk and to develop courses of action to thwart potential attacks. Depending on an IHE's size and on how connected its individual department and school network are, network monitoring can be a time-consuming task that requires support from outside sources, such as data security firms. Consider consulting neighbouring IHRs, or IHEs within cybersecurity networks, to get input on which data security firms provide the best support.

4.3 Recovering from Threats:

The recovery process for a cyber incident should be focused on people, policies, and technology. When designing plans for recovery, if operating systems have been disabled, either as a result of a cyber attack and/or a protective measure, IT staff will need to work to restore technology capabilities. They will also need to notify the people impacted, including faculty, staff, and students, about contingency plans that will be in place until capabilities are restored. Lastly, cybersecurity and emergency management teams should take steps to review, revise, train, and continually remind key stakeholders on policies that may be implemented to prevent future attacks.

Understand the Situation:

During this step in the planning process, higher ed IT, cybersecurity, and emergency management teams should ensure they understand potential cyber threats that may impact their Cyber community. Once potential threats are identified, planning teams should assess the cyber risk to their networks and systems, and from there, identify the cyber vulnerabilities.

Plan Preparation, Review, and Approval:

When finalizing the Cybersecurity Annex, it is recommended that higher ed IT, cybersecurity, and emergency management teams address how the annex connects to state, county, and/or municipal plans. The annex may also identify a chain of command for before, during, and after an incident, as well as roles, responsibilities, and contact information for key stakeholders in prevention, protection, mitigation, response, and recovery.

5. Plan Implementation and Maintenance:

Once the plan is finalized, it is important for CSE to train stakeholders. In this case, stakeholders include faculty and staff (IT, emergency management, academic, research, administrative, etc.), students, and visitors. Consider conducting emergency drills and exercises related to cybersecurity that involve these key stockholders, as well as other partners who will support the CSE in the event of a cyber-incident. After drills and exercises are complete and after actual cyber incidents, CSE should prepare after-action reviews in order to identify lessons learned and implement corrective actions.

Dos and Don'ts

(a) A genuine operating system is recommended with regular updates.

(b) Latest updated version of antivirus aids in protecting the computer from Cyber-threats.

(c) A personal computer needs to have good malware, anti-spyware. The recommended downloads are Malware byte, Super AntiSpyWare, and useful cleaners.

(d) Use strong power on password, Admin password, and user login password. An alphanumeric password with special characters will be helpful. Changing them regularly minimizes the risk of Cyber-threats.

(e) Never Click on attachments of email that you are not sure of. Think before you click.

(f) Work on sandbox which is an important security technique that isolates programs, preventing malicious or malfunctioning programs from damaging or snooping on the rest of your computer.

(g) Always backup your data on an external Hard Disk Drive.
(h) Format your personal computer regularly.
(i) Always save the passwords in a coded format.
(j) Use secure erase software for deleting files.
(k) Do not access, store, share, manipulate official data on the personal computer.

(l) Firewall or IP Tables must be configured on every system and kept on at all times.
Guidelines for the operating system used on residential internet computer (Window or Linux)
(i) Keep WiFi /Bluetooth service disabled (when not in use)
(ii) Disable all default and manual shared drives and folders.
(iii) Provide minimum rights to the user account.
(iv) Enable security features of windows like firewall, security policies.
(v) Disable Guest account.

(n) Do not download any unwanted software, clear scrutiny is recommended before any download.
o) To safeguard against fake/malicious applications/software used to compromise and extract information from the internet computers, all software/ applications like browsers, antivirus software, etc to be downloaded directly from OEM (Original Equipment Manu-facturers) website or a licensed version of the same be procured.

(p) Configure your modem and Wi-Fi devices. Always change the default password.
(q) Smartphones are also vulnerable to cyber-threats and must be configured for their secure use.
(s) Change your email password regularly.
(t) Use secure browsers like updated versions of Chrome and Firefox for surfing. Configure web browser as under:-
(i) Disable window pop-up functionality.
(ii) Disable Java runtime support.
(iii) Disable ActiveX Support.
(iv) Disable all multimedia and auto-play/auto-execute extensions.
(v) Prevent the storage of non-secure cookies.
(vi) Ensure that the downloads cannot be automatically run from the browser.
(u) Most of the Smartphones allow for locking the screen by means of a security PIN. This is a good practice for preventing unauthorized access to the device if left unattended or lost.
(v) Data, if stored on the device must be encrypted.
(w) Do-not install untrusted applications. Always check for the permissions requested by the application. Do not install the application if suspicious permissions are requested by it.
(x) Install an updated internet protection suite (a combination of antivirus and firewall).

(y) Sanitise all data by carrying out a virus scan before it is downloaded.

(z) Do-not turn on geotagging and location service. It is strongly suggested to minimize the use of Location service.

(aa) Do not click on a link /photo sent by a stranger.

(ab) Do not use unknown Wi-Fi in public places like airports, railway stations, bus stops, shopping complexes, etc.

(ac) Old smartphones are to be disposed of in a secure manner.

(ad) Do not make smartphone devices as storage for personal data.

(ae) Note down the IMEI (International Mobile Equipment Identity) number of the smartphone in a safe location.

(af) It is a good practice to use cloud storage for backup of the smartphones and systems in a secure manner.

(ag) Trusted gaming sources ensure network security and control.

(ah) Emails from an unknown source or originator to be ignored or authentically confirmed before accessing.

(ai) Report any suspected E-mails/ Messages and Pop-ups.

Section 3. Raise National awareness about risks in Cyberspace

Earlier the contact with the world was limited by physical boundaries and to the closed communities and cultures. The reach of cyberspace is ubiquitous. It has connected people across the globe. It has revolutionized the way people think and work in a global environment. However, this has also increased the space and scope of anti-social and criminal elements. Now they can operate at a global scale. They can operate from safe havens and target the vulnerable sections of our society especially our children and people in distress.

In order to raise the National awareness about risks in cyberspace we can have followed in place

1. Children below the age of 18 years should be given access to the Internet and Social Media only under supervision.

2. Our media and Journalists play a vital role in making people aware of the happening around the world. They should report cybercrimes in daily news hours.

3. Cinema and media should also be encouraged to make TV/web series on cybercrime. Doordarshan can play a stellar role due to its vast network and deeper reach in the hinterland of our country.

4. There should be a pool of cybersecurity instructors who can further spread awareness amongst children and other people on various aspects of cybersecurity. These instructors should be recruited in schools like PT instructors. AICTE can play a vital role by listing the qualifications/skillsets required by the cybersecurity instructors.

ROLES AND RESPONSIBILITIES

1.1 Role of the Board / Management

1.2 Role of the Principal / Vice-chancellor / Director

1.3 Role of Staff

1.4 Role of Parents

Create Dynamic Cybersecurity policies for students and institutes

7. Student Network Policies

1.Social Engineering Awareness Policy

1. Overview

The Social Engineering Awareness Policy bundle is a collection of policies and guidelines for employees of AICTE. This Employee Front Desk Communication Policy is part of the Social Engineering Awareness Policy bundle.

In order to protect AICTE's assets, all employees need to defend the integrity and confidentiality of AICTE's resources.

2. Purpose

This policy has two purposes:

2.1 To make employees aware that (a) fraudulent social engineering attacks occur, and (b) there are procedures that employees can use to detect attacks.

2.1.0 Employees are made aware of techniques used for such attacks, and they are given standard procedures to respond to attacks.

2.1.1 Employees know who to contact in these circumstances.

2.1.2 Employees recognize they are an important part of AICTE’s security. The integrity of an employee is the best line of defense for protecting sensitive information regarding AICTE’s resources.

2.2 To create specific procedures for employees to follow to help them make the best choice when:

2.2.0 Someone is contacting the employee - via phone, in person, email, fax or online - and elusively trying to collect AICTE’s sensitive information.

2.2.1 The employee is being “socially pressured” or “socially encouraged or tricked” into sharing sensitive data.

3. Scope

Includes all employees of AICTE, including temporary contractors or part-time employees participating with help desk customer service.

4. Policy

4.1 Sensitive information of AICTE will not be shared with an unauthorized individual if he/she uses words and/ or techniques such as the following:

4.1.1 An “urgent matter”

4.1.2 A “forgotten password”

4.1.3 A “computer virus emergency”

4.1.4 Any form of intimidation from “higher level management”

4.1.5 Any “name dropping” by the individual which gives the appearance that it is coming from legitimate and authorized personnel.

4.1.6 The requester requires release of information that will reveal passwords, model, serial number, or brand or quantity of AICTE resources.

4.1.7 The techniques are used by an unknown (not promptly verifiable) individual via phone, email, online, fax, or in person.

4.1.8 The techniques are used by a person that declares to be "affiliated" with AICTE such as a sub-contractor.

4.1.9 The techniques are used by an individual that says he/she is a reporter for a well-known press editor or TV or radio company.

4.1.10 The requester is using ego and vanity seducing methods, for example, rewarding the front desk employee with compliments about his/her intelligence, capabilities, or making inappropriate greetings (coming from a stranger).

4.2 Action

4.2.1 All persons described in section 3.0 MUST attend the security awareness training within 30 days from the date of employment and every 6 months thereafter.

4.2.2 If one or more circumstances described in section 4.0 is detected by a person described in section 3.0, then the identity of the requester MUST be verified before continuing the conversation or replying to email, fax, or online.

4.2.3 If the identity of the requester described in section 5.1.1 CANNOT be promptly verified, the person MUST immediately contact his/her supervisor or direct manager.

4.2.4 If the supervisor or manager is not available, that person MUST contact the security personnel.

4.2.5 If the security personnel is not available, the person described in section 3.0 MUST immediately drop the conversation, email, online chat with the requester, and report the episode to his/her supervisor before the end of the business day.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.