AMOGHVARTA

ISSN : 2583-3189

Cyber Security & Privacy

ORIGINAL ARTICLE

Author
Dr. Pushpa Ramesh,
Associate Professor,
Head of the Commerce Department,
Mata Gujri Mahavidhyalaya (Autonomus),
Jabapur, Madhya Pradesh, INDIA

Abstract

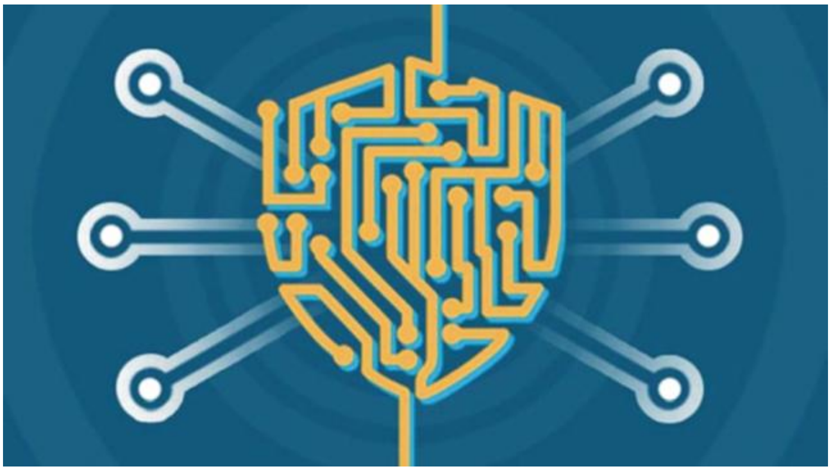
Internet was made as a global network primarily to fulfill military purposes. Thus, it is obvious that the need for protection of data or information existed since the time internet is in use. Now, when it is accessible to almost everyone, criminals have started to use it for their personal goals. Cyber-security is the practice of protecting internet-connected systems including hardware, software and data, networks, and programs from digital attacks.

Keywords

Cyber Security, Cyber Privacy, Internet, Network.

Internet was made as a global network primarily to fulfill military purposes. Thus, it is obvious that the need for protection of data or information existed since the time internet is in use. Now, when it is accessible to almost everyone, criminals have started to use it for their personal goals.

Cyber-security is the practice of protecting internet-connected systems including hardware, software and data, networks, and programs from digital attacks. Cyber attack is aimed at accessing, changing or destroying sensitive information, extorting money from customers, or interrupting ongoing internet processes. In a much broader and technical context, security comprises of both online and physical security. The protection is against unauthorized access to data centers and other computerized systems.

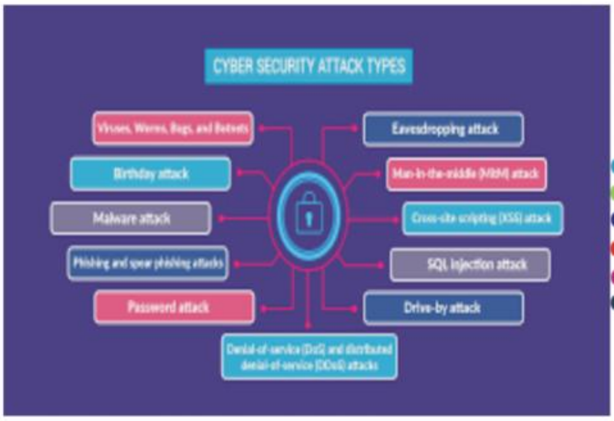


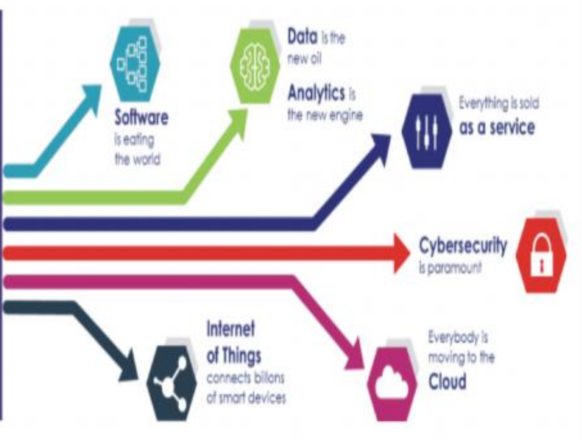
A successful approach to cyber security has multiple protection layers across computers, programs, networks and data that a person intends to keep safe. The people along with the processes and technology belonging to an organization should complement each other in order to create an effective defense mechanism against cyber-attacks.

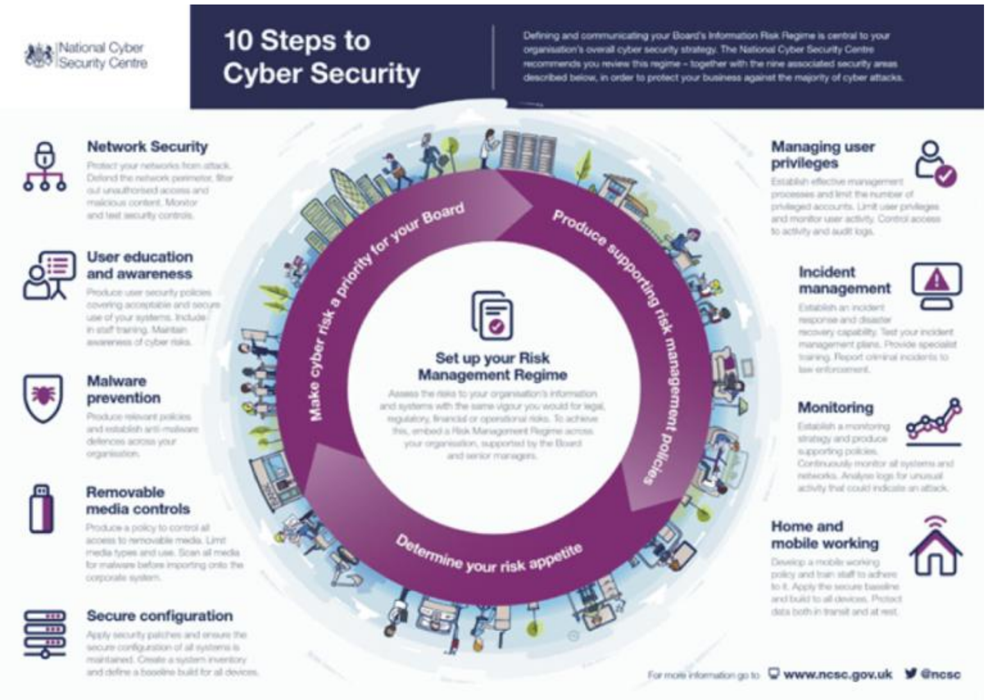
The subset of cyber security is Information security, which is designed to maintain the three triads known as the CIA triad of cyber security viz. a viz., confidentiality, integrity and availability. Cyber security deals with the prevention of issues such as data breaches and identity theft and can also aid in risk management.

Information security, put in short as Infosec, involves the alleviation of information risks in order to safeguard hardware, software and data which can otherwise be gained via unauthorized access or use. It typically consists of prevention of disruption or destruction of information or networks by hackers. The primary goal is to reduce inappropriate disclosure, inspection, deletion, modification of information as well as to decrease adverse aftermath of incidents.

At an individual level, a cyber security attack results in everything from theft of identity, to attempts of breach, to the loss of important data like family photos, which can be used for nasty purposes. To keep our society functioning, it becomes important to safeguard critical infrastructure of hospitals and financial service companies.


CYBER SECURITY ATTACK TYPES
Viruses, Worms, Bugs, and Botnets
Eavesdropping attack
Birthday attack
Man-in-the-middle (MitM) attack
Malware attack
Cross-site scripting (XSS) attack
Phishing and spear phishing attacks
SQL injection attack
Password attack
Drive-by attack
Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks


Software is eating the world
Data is the new oil
Analytics is the new engine
Everything is sold as a service
Cybersecurity is paramount
Internet of Things connects billons of smart devices
Everybody is moving to the Cloud


National Cyber Security Centre
10 Steps to Cyber Security
Make cyber risk a priority for your Board
Produce supporting risk management policies
Determine your risk appetite

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security
Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness
Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention
Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls
Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration
Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Set up your Risk Management Regime
Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

Managing user privileges
Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management
Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring
Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working
Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk @ncsc

The insurance of any form of information in the form of physical or electronic tangible devices, or any data over the internet is done by focusing on the maintenance of a balanced preservation of the CIA triad. This is done while implementing an efficient policy, which should be done without inhibiting organization productivity.

At the heart of Information security lies the CIA triad – confidentiality, integrity, availability – which are the properties of the goals of security. It can be used as a model for creating security measures; and it ensures that the important areas of security are covered.

1. Confidentiality

Confidentiality is like privacy, but never the same. Navigation around technology with the hope of keeping one’s data safe from prying eyes, in times when data can be accessed through illegal means, and be compromised with, is the need of the hour. Any data has access to guaranteed protection with the use of things like access controls, permissions, and key encryption techniques.

Blockchain Technology: A database that maintains a consequently growing list of data, called blocks that are safeguarded from any kind of revision efforts or tampering. It consists of blocks that contain sections of valid and approved transactions. There is a link between the prior block and the current one. The linked blocks form a chain, therefore the blockchain.

It is a come-of-age disruptive technology that revolutionizes the way in which extremely complex audits, dealing with sensitive information like transactions with virtual currencies can be done more securely. The popular Bitcoin platforms are built on the foundational technology of blockchains that organizes data and secures it to reduce the cost and complexity of transactions to a greater extent. Due to its decentralized nature, the elements are transparent to all the individuals who share their information with others in a single block chain. IoT – Internet of things brings along with itself numerous device corruption ways, attacks, as well as internal leaks.

2. Integrity

Prevention of data from being modified completely or partly, as well as being deleted and all this be done in an undetected manner caters to integrity of information. The key element to data integrity is encryption. The goal is to not depend on a ‘third party auditor’ for more reliable data integrity verification, being provided both for the data owners as well as the consumers. In any case of fault is the integrity system, possible ways to revert the harm done should exist.

Spoofing and forgery attacks where impersonation of a device is done in order to gain false access to credentials, is done by creation of IP packets with unreal IP address. This way data is hampered along the way posing threat to integrity.

Use of CONIKS: The end-to-end secure communication between users, without the threat of data being stolen along the way has become a need among technology users. This demand is met by adopting end-to-end encryption. Key management is difficult for a vast majority of users. CONIKS establishes automated trust with untrusted communication providers by having the service provider keep an auditable directory of all its users’ keys.

Valid certification of encryption is done by applying for a rusted CA (Certificate Authority), which is then presented to the browser to authenticate the site.

3. Availability

Any information be available when needed, only to authorized users as per the need is the purpose of the third member of the CIA triad. This is best achieved by rigorously maintaining hardware, performing repairs and by correct functioning of OS environment, free of software conflicts. This also relies on necessary upgrades and updates, to keep systems working reliably. For example, an investment in cloud backup measures in case of power outage, shall ensure availability of data to an organization.

Issues in network forensics & cyber security

Network forensics can be generally defined as the science of discovering and retrieving evident information in a connected environment about a crime in a way which makes it admissible in court.

Different from intrusion detection, all the techniques used for network forensics should satisfy both legal and technical requirements. For example, it is important to guarantee whether the developed network forensic solutions are practical and fast enough to be used in high-speed networks with heterogeneous network architecture and devices. More importantly, they need to satisfy general forensics principles such as the rules of evidence and the criteria for admissibility of novel scientific evidence (such as the Daubert criteria).

The five rules are that evidence must be:

- Admissible - Must be able to be used in court or elsewhere.
- Authentic - The evidence relates to an incident in a relevant way.
- Complete - No tunnel vision, exculpatory evidence for alternative suspects.
- Reliable - No question about authenticity and veracity.
- Believable - Clear, easy to understand, and believable by a jury.

The evidence and the investigative network forensics techniques should satisfy the criteria for admissibility of novel scientific evidence (Daubert v. Merrell):

- Whether the theory or technique has been reliably tested.
- Whether the theory or technique has been subject to peer review and publication.
- What is the known or potential rate of error of the method used?
- Whether the theory or method has been generally accepted by the scientific community.

The investigation of a cyber-crime often involves cases related to homeland security, corporate espionage, child pornography, traditional crime assisted by computer and network technology, employee monitoring, or medical records, where privacy plays an important role.

There are at least three distinct communities within digital forensics: law enforcement, military, and business and industry, each of which has its objectives and priorities. For example, the prosecution is the primary objective of the law enforcement agencies and their practitioners and is often done after the fact. Military operations' primary objective is to guarantee the continuity of services, which often have strict real-time requirements. Business and industry's primary objectives vary significantly, many of which want to guarantee the availability of services and put prosecution as a secondary objective.

Network forensics is an extension of the cyber security model which traditionally emphasizes prevention and detection of network attacks. Current network forensics approaches are costly and time-consuming. However, unlike other areas of digital forensics, network forensics deals with volatile and dynamic data. It helps organizations to investigate attacks that originated from outside and inside of the company. It's also important for law enforcement agencies when solving crimes.

A network forensic expert must deal with a lot of problems when collecting data from a network;

- organizational,
- technical and
- Legal issues.
- Organizational issues arise as the network forensics investigator is called to examine a digital crime scene, without impairing the function of the company, which is the victim of the crime.

- Technical issues arise due to difficulties in collecting and producing digital evidence that is beyond any reasonable doubt.
- Legal issues that arise concern protection of privacy and jurisdiction problems.

CONCLUSION

Information security, put in short as InfoSec, involves the alleviation of information risks in order to safeguard hardware, software, and data which can otherwise be gained via unauthorized access or use. It typically consists of prevention of disruption or destruction of information or networks by hackers. The primary goal is to reduce inappropriate disclosure, inspection, deletion, modification of information as well as to decrease adverse aftermath of incidents.

At an individual level, a cyber-security attack results in everything from theft of identity, to attempts of breach, to the loss of important data like family photos, which can be used for nasty purposes. To keep our society functioning, it becomes important to safeguard critical infrastructure of hospitals and financial service companies.

REFERENCES

1. Childs J. Rives, *General Solution of the ADFGVX Cipher System,* Aegean Park Press, Laguna Hills, California, 2001
2. The Wikipedia has many informative articles on Cryptology.

——==00==——