Security Processes In Practice For Businesses

Objectives

After completing this unit, you should be able to:

- Understand the Need for Business Security
- Know the types of Cyber Attacks and leveraging industry good practices
- Link between Corporate & Security Governance
- Understand IT Strategy, Project & Change management
- Know how Supplier (third party) management can be handled
- Understand Info-sec management
- Learn how to implement a secure BCP (Business Continuity Plan)

FTVETI

ICT @ FTVETI

Need For Business Security

Security & Business Relation

Why Business Security?

Business should invest in cyber security, as it helps the organisation in:

1. Securing Valuable Data
2. Establish Framework and Guidelines using ISMS(Information Security Management System) Framework
3. Increasing Customer Confidence
4. Keeping strong Company Reputation
5. Ongoing Support and Peace of Mind

FTVETI

Cyber Attacks - Your Business Needs To Avoid

FTVETI

ICT @ FTVETI

What Do You Mean By Cyber Attack?

A **Cyber-Attack** is any type of offensive operation that targets computer information systems, infrastructures, computer networks, or personal computer devices

Different Types Of Cyber Attacks – In Business

Malware

Phishing

Password Attacks

Denial-of-Service (DoS) Attacks

"Man in the Middle" (MITM)

Drive-By Downloads

Malvertising

Rogue Software

Cyber Attack - Leveraging Industry Good Practices

FTVETI

ICT @ FTVETI

Malware

Definition

Malware is a term which can be used for a variety of cyber threats including **Trojans**, **viruses**, **worms**, and so on. It is a code with malicious intent that is used to steal or destroy confidential data from the system

Working

Most often, Malware is injected into the system through emails/ email attachments, software downloads or operating system vulnerabilities

Prevention

Best way to prevent malware attack is to avoid clicking on links or downloading attachments from unknown senders. This can be done by deploying robust and updated firewalls, which prevent the transfer of large data files over the network, to weep out the attachments that may contain malware

Phishing

Definition

Phishing attacks are sent via email and this email asks the users to click on a given link and enter their personal data

Working

Phishing emails contains a link that directs the user to a dummy site that steals a user's information, if a user clicks on the link

Prevention

Verify the requests that arrive via email or over the phone

Password Attacks

Definition

In **Password Attack** a third party tries to gain access to the system by cracking a user's password

Working

This type of attack does not usually require any type of malicious code or software to run on the system. There are software that the attackers use to try and crack the password. Programs use many methods to access accounts, including **Brute force** attacks made to guess passwords, as well as comparing various words from a dictionary

Prevention

Strong passwords are only way to safeguard against password attacks, such as using a combination of upper and lower case letters, symbols, and numbers and having at least eight characters or more. An attacker using a **brute force** password cracking program, can typically unlock a password with all lower case letters in a matter of minutes. It's also recommended not to use words found in the dictionary

Denial-of-Service (DoS) Attacks

Definition

DoS attack focuses on disrupting the service to a network. Attackers send high volumes of data or traffic through the network by making lots of connection requests, until the network becomes overloaded by traffic and can no longer function

Working

The attackers use multiple computers to send the traffic or data that overloads the system. In many instances, a person may not even realize that his or her computer has been hijacked and is contributing to the DoS attack

Prevention

The best way to prevent such type of attack is by keeping the system as secure as possible with regular software updates, monitoring online security and monitoring the data flow to identify any unusual or threatening rise in traffic

“Man In The Middle” (MITM)

Definition

The **MITM** can obtain information from the end users and the entity that a person is communicating with, by imitating the endpoints in an online information exchange such as the connection from the smartphone to website

Working

MITM gains access through a non-encrypted wireless access point, one that doesn’t use WAP, WPA, WPA2 or other security measures. They would then have access to all of the information being transferred between both parties

Prevention

Using encrypted wireless access points that use WPA security, are best way to prevent such attacks

Drive-By Downloads

Definition

In **Drive-By Download** attack, a program is downloaded in the user's system just by visiting the website. It doesn't require any type of user action to download the file

Working

A code is downloaded to the user's system and that code then reaches out to another computer. It often exploits vulnerabilities in the user's operating system

Prevention

Making sure that the operating system and software programs are up to date, doing this lowers the risk of vulnerability. Also, minimize the number of browser add-ons, as these can be easily compromised

Malvertising

Definition

In **Malvertising Attack**, the computer is affected with malicious code that is downloaded to the system when one click on an affected ad

Working

Cyber attackers upload infected display ads to different websites using an ad network. These ads are then distributed to sites that match certain keywords and search criteria. If a user clicks on one of these ads, some malware will be downloaded on their system

Prevention

The best way to prevent malvertising is to use common sense and prevent clicking on ads that look fake. Also, up-to-date software and operating systems are best way of defence

Rogue Software

Definition

Malware that act as legal and necessary security software to keep your system safe

Working

These are pop-up windows and alerts that look legal to us. These alerts advise the user to download security software, agree to terms or update their current system to stay protected. By clicking “yes”, the rogue software is downloaded to the user’s computer

Prevention

The best practice is to have an updated firewall and anti-virus program

Corporate & Security Governance

What Is Corporate Governance?

- Corporate governance is the system consisting of rules, practices and processes by which a firm is directed and controlled
- Corporate governance provides the framework for attaining a company's objectives, it encloses every sphere of management, from action plans and internal controls to performance measurement and corporate disclosure

What Is Security Governance?

Security governance is the means by which you control & direct an organisation's approach to security

Effective Security governance will successfully coordinate the security activities within an organisation

It enables the flow of security information and decisions around your organisation

Security decision making can happen at all levels

An organisation's senior leadership should use security governance to set out the kinds of security risks they are prepared for staff to take Vs. those they are not

We can now easily create a link between Corporate Governance and security governance.....

- Corporate Governance is used to control or manage the working of an organisation whereas,
- Security Governance is used to control & direct an organisation's approach to security
- An organisation should incorporate both, in order to be secure and function properly

Organisations Related To Corporate Governance

There are four organisations that have been working on issues related to corporate governance, regarding Cyber-Security:

Information Systems Audit and Control Association (ISACA)
Associated with the development, adoption and use of globally accepted, industry-leading knowledge and practices for information technology systems

Institute of Internal Auditors (IIA)
An international professional association recognized as the professional organisation for internal Auditors

National Association of Corporate Directors (NACD)
Recognized authority on advancing exemplary board leadership and establishing boardroom practices

Internet Security Alliance (ISA)
Association providing thought leadership and advocacy centered at enhancing cybersecurity

Source: https://threatbrief.com/cyber-security-corporate-governance-five-principles-every-corporate-director-embody/

Key Principles For Corporate Governance

NACD and ISA published a report titled as **"Cyber-Risk Oversight"** where they propose five key principles which every corporate director should incorporate in approaching cyber-risk:

01 Cyber-risk is more than just an IT issue: it is a key component of enterprise risk management, requiring board-level oversight

02 Cyber risks have important legal ramifications, which directors need to understand

03 Cyber-risk should be a topic of regular board discussion, and boards need access to the expertise to engage with cyber-risk issues

04 Directors should ensure management implements an effective cyber-risk framework for the company

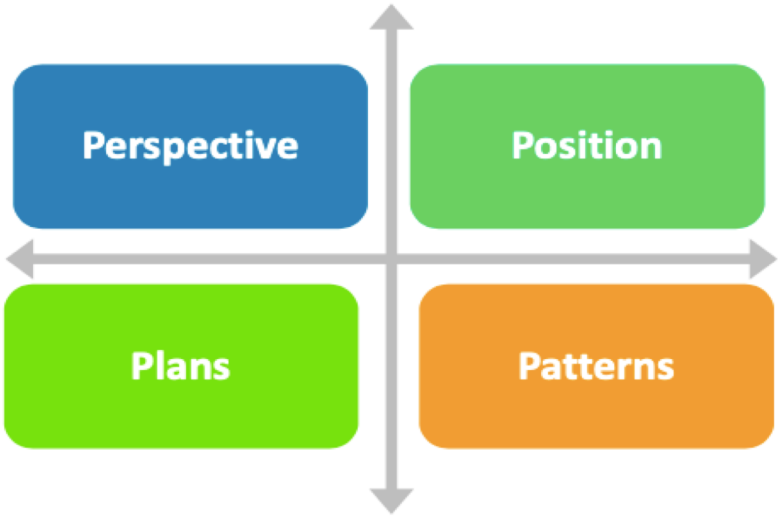
05 The board and management should assess cyber-risk just like other enterprise-level risks: ensuring a specific determination is made of which aspects of cyber-risk to accept, avoid, mitigate or insure against

Source: https://threatbrief.com/cyber-security-corporate-governance-five-principles-every-corporate-director-embody/

IT Strategy Management

What Is IT Strategy Management?

- IT Strategy management is a process of defining and maintaining the **Perspective**, **Position**, **Plans**, and **Patterns** of an organisation with regards to its services and management of those services
- The purpose of strategy management for IT services is to make sure that a strategy is defined, maintained and managed properly to achieve its purpose



Key Process Of Strategy Management For IT Services

Challenges Of Strategy Management For IT Services

- Usually conducted at an inappropriate level: It should start from the top senior executives and other unit should follow them
- Lack of information about the external environment
- Absence of support from the stakeholders
- Lack of understanding regarding the usage of tools and techniques required in the organisation
- Failure to match operational targets with strategic objectives: this results in struggling to achieve targets which are not aligned with the strategy

Risks Of Strategy Management For IT Services

- A governance model having flaws can allow the managers to decide whether to implement all the aspects of a strategy or to deviate from the strategy for short-term goals
- Short-term priorities can sometimes override the directives of the strategy
- Absence of key information while making strategic decisions
- Choosing an incorrect strategy which does not match the goals of the organisation
- Strategies often happens once a year and has no effect on what happens for the rest of the year

Whether moving infrastructure to the cloud or building a new CRM system, having an effective Project Management is very essential. But without cyber security knowledge, any project could lead an organisation to exploitation

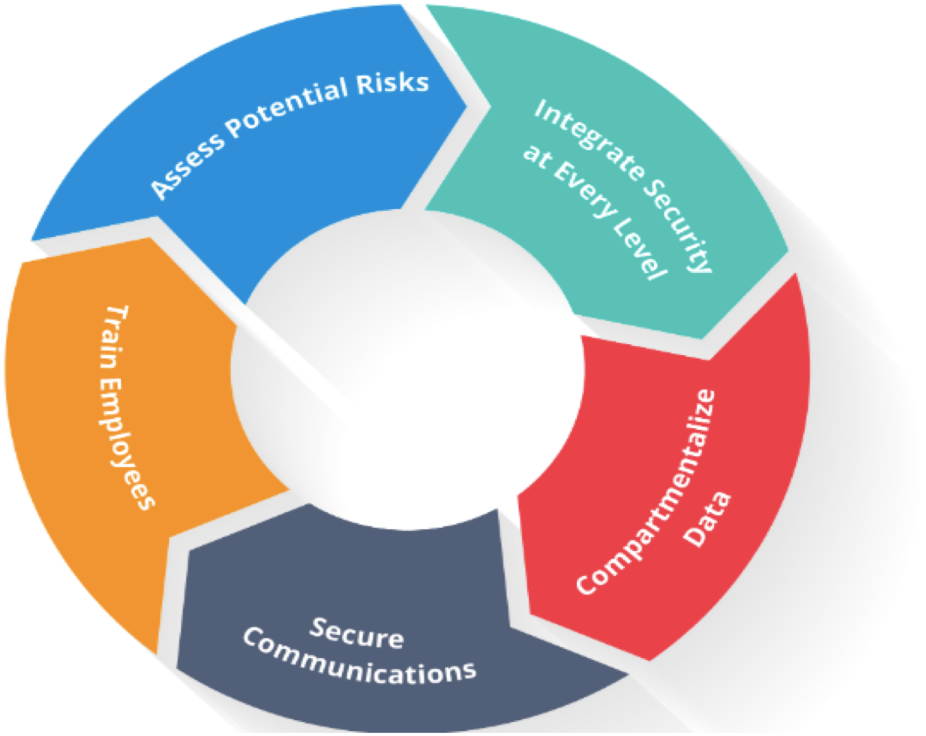
Project Management

What Do You Mean By Project Management?

Project management is the practice of initiating, planning, executing, controlling, and closing the work of a team to achieve specific goals and meet specific success criteria at the specified time

Project Management & Cyber Security

In order to have a perfect and secure Project Management plan, the project managers should have the knowledge of cyber security. Few things every project manager should know about cyber security are:



In order to stay competitive, relevant change in an organisations is important.

Change Management encompasses cultural, business and technology change initiative

FTVETI

ICT @ FTVETI

Change Management

What Is Change Management?

Change management is a collective term for all approaches to prepare and support individuals, teams, and organisations in making organisational change

Need For Change Management

- Change Management is part of Risk Management program
- Change Management helps to controls any additions, deletions, or modifications in an organisation such as configuration of desktops, servers and network hardware and software
- It brings new capabilities, better efficiencies, and creative ways of doing things in an organisation
- It helps to identify and change the poor processes, eliminates toxic leadership, and increases the standard of the products
- We should always conduct a vulnerability scans each and every time a change is introduced into system configurations, software, web pages, and data exchanges. This helps to reduce security risks

Change Management For Cyber Security Threats

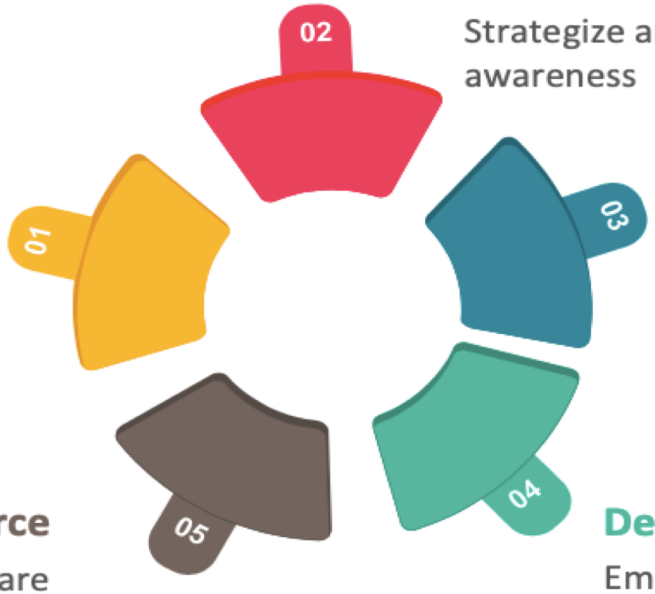
Five organisational change management principles that can be applied in an organisation, when security threat arises:

Plan

Strategize and expand the approach towards awareness

Assess

Evaluate the risk by communicating with teams, and understand the level of potential threat



Act

Be proactive and train the employees to help reinforce the communications and process changes

Reinforce

As cyber threats are more frequent, prepare your organisation in advance, so they can respond quickly and effectively

Deploy

Employees should be fully briefed before deploying the change

Supplier(Third Party) Management

What Is Supplier Management?

Supply Management describes the methods and processes of modern corporate. This may be for the purchasing of supplies for internal use, purchasing raw materials for the consumption during the manufacturing process, or for the purchasing of goods for inventory to be resold as products in the distribution and retail process

Cyber Supply Chain Security Principles

According to **NIST**(National Institute of Standards and Technology), below are the cyber supply chain security principles:

01 Develop your defences based on the principle that your systems will be breached

02 Cybersecurity is never just a technology problem, it's a people, processes and knowledge problem

03 Security is Security, there should not be any gap between physical security and cybersecurity

Cyber Supply Chain Risks

Cyber supply chain include risks from:

- Third party service providers or vendors
- Poor information security practices by lower-tier suppliers
- Compromised software or hardware purchased from suppliers
- Software security vulnerabilities in supply chain management or supplier systems
- Counterfeit hardware or hardware with embedded malware
- Third party data storage or data aggregators

Source: https://csrc.nist.gov/

Information is one of the most valuable assets in business.

The use of proper preventive measures and safeguards can reduce the risk of potentially devastating security attacks. Let us know about information security management

Info-Sec Management

FTVETI

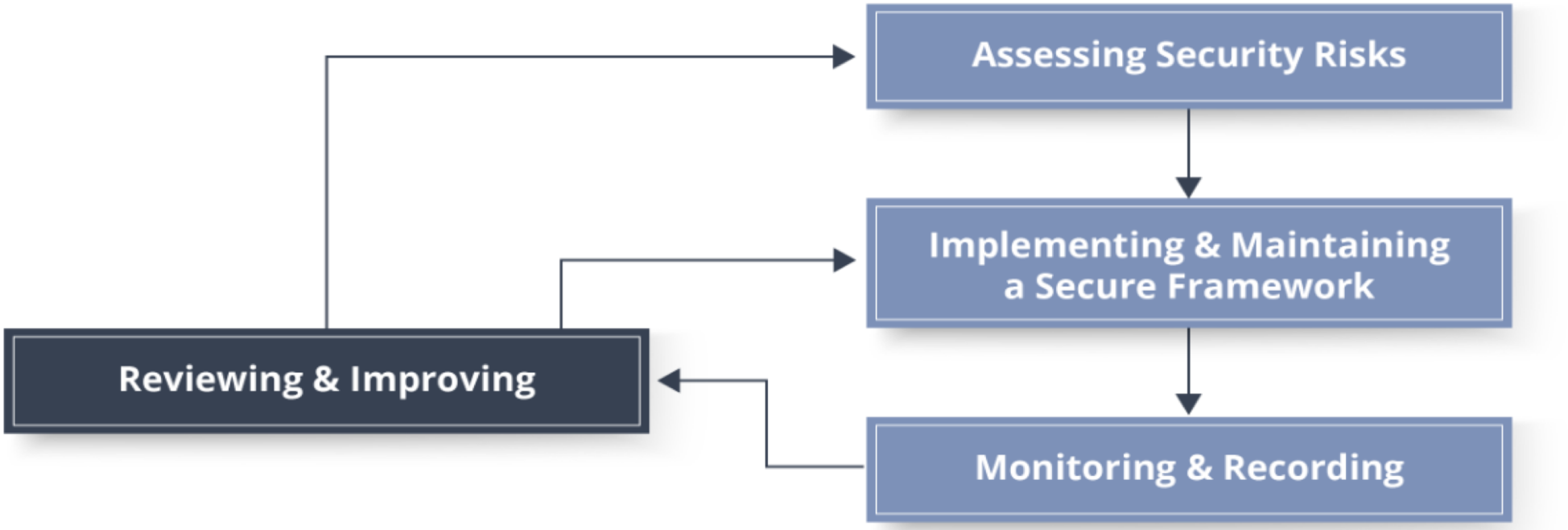
ICT @ FTVETI

What Is Info-Sec Management?

Information security (info-sec) is a set of strategies for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information

Information Security Management Cycle

Information security management is a combination of prevention, detection and reaction processes. It is a cycle of repetitive activities and processes that require ongoing and control monitoring



BCP

What Is BCP?

A **Business Continuity Plan** (BCP) is a plan to help ensure that business processes can continue during a time of emergency or disaster

Business Continuity Plan & Security

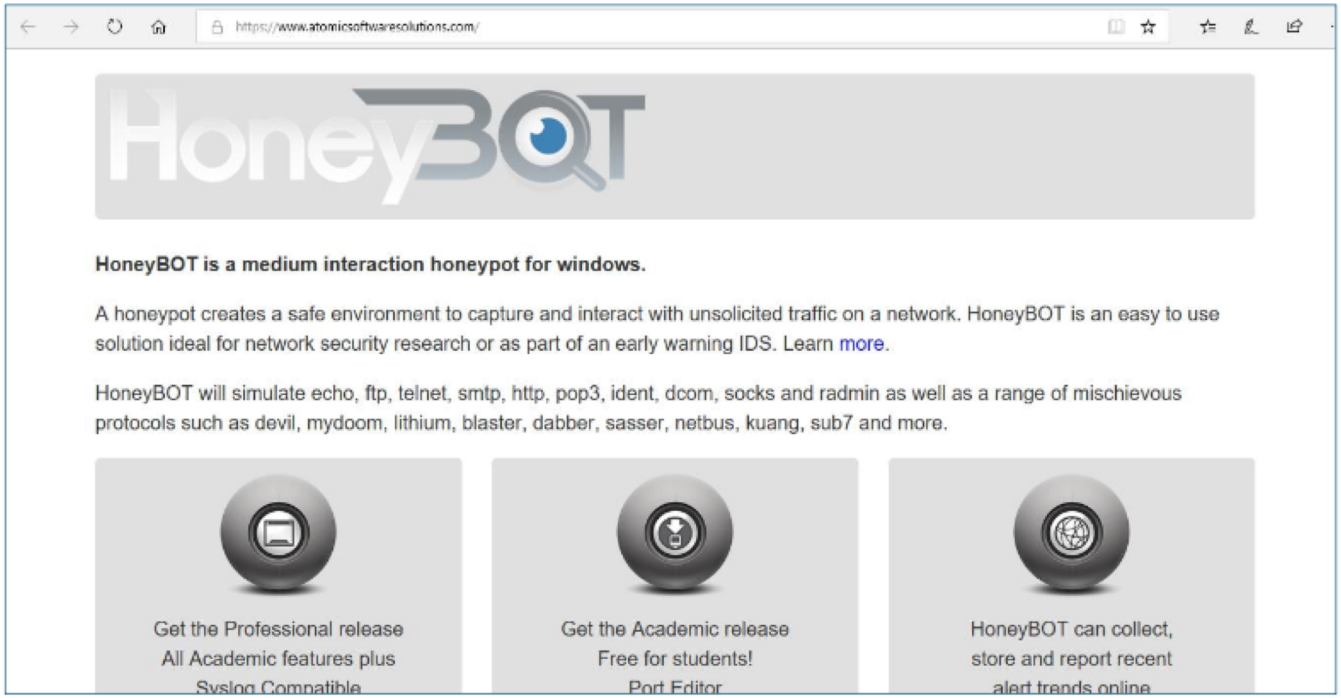
A business continuity plan involves the following:

- Analyze organisational threats
- A list processes and tasks required to keep the organisation operations flowing
- Easily located management contact information
- Explanation of where personnel should go if there is a disastrous event
- Data backups and organisation site backup
- Collaboration among all facets of the organisation
- Buy-in from everyone in the organisation

BCP Lifecycle

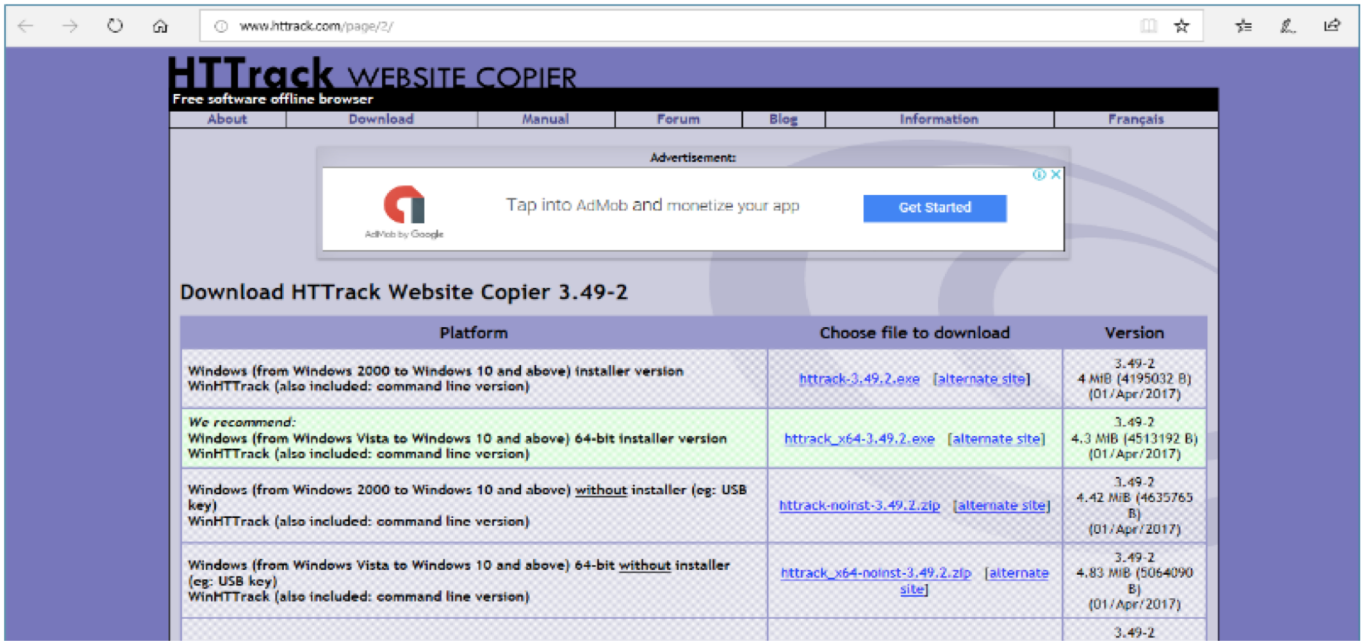
Demo 1: Honeypot

- Secure your network by setting up a **Honeypot**
- Capture and analyze unsolicited traffic on the network
- Setup honeypot using HoneyBot tool
- Download and install HoneyBot tool from the link: https://www.atomicsoftwaresolutions.com/



Demo 2: Website Mirroring

- Download a World Wide Web site from the Internet to a local directory
- Create a mirrored website on the browser for offline viewing
- Download and install HTTrack Website Copier for website mirroring from the link: http://www.httrack.com/page/2/



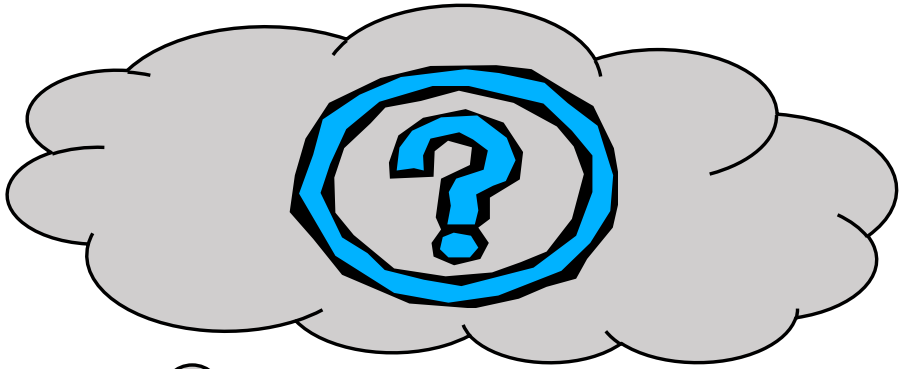
Summary

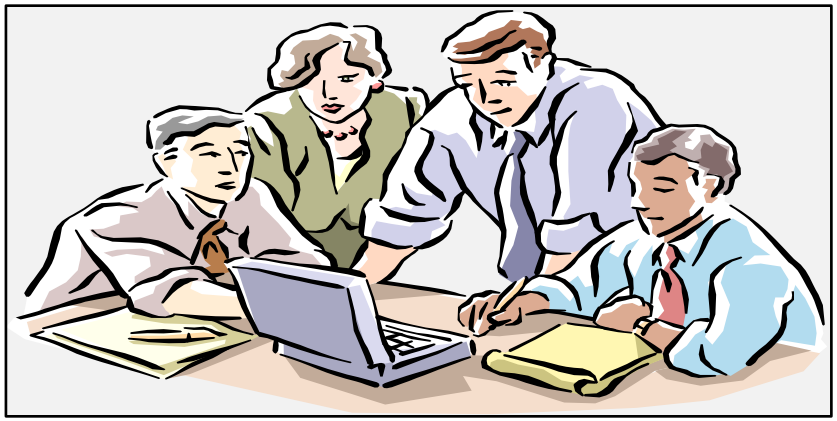
In this unit, you should have learnt:

- Need for Business Security
- Types of Cyber Attacks and Leveraging industry good practices
- Corporate & Security Governance
- IT Strategy management
- Project management
- Change management
- Supplier (third party) management
- Info-sec management
- BCP (Business Continuity Plan)

FTVETI

QUESTIONS PLEASE ☺





FTVETI

ICT @ FTVETI