UNIT-1

Understanding IT Security

Learning Outcomes
By the end of this unit the learner will be able to:
✓ Define cyber security and its primary objectives ✓ Understand the various causes of cybercrime and those responsible for threats to cyber security ✓ Discuss the classifications of cyber crime and Microsoft's 10 laws of computer security

Unit 1

Understanding IT Security

What is Cyber Security?

The term 'cyber security' refers to all safeguards and measures implemented to reduce the likelihood of a digital security breach. Cyber security affects all computers and mobile devices across the board – all of which may be targeted by cyber criminals. Cyber security focuses heavily on privacy and confidentiality, along with data integrity and identity protection. Security breaches in general are nothing new, but have become more commonplace and problematic in today's digital era. The greater the extent to which the world becomes reliant on connected technology, the greater the threat posed by cybercriminals worldwide.

From reputation damage to system downtime to financial loss, cyber security issues can be incredibly costly. According to a recent study, almost half of all businesses operating in 2017 experienced at least one cyber attack or attempted security breach. Precisely the reason why businesses worldwide have begun prioritizing cyber security, implementing robust protective measures and hiring cyber security experts to oversee their operations.

The Importance of Security

The Internet has transformed the face of everyday life for billions of people worldwide. Already enormous, daily web traffic volumes are growing at an exponential rate. To such an extent that the vast majority of communications and business activities worldwide are fundamentally reliant on the Internet. From simple retail purchases to the most sensitive and high-profile business activities, everything takes place online. All of which adds up to a near-irresistible opportunity for the 21st century cyber criminal.

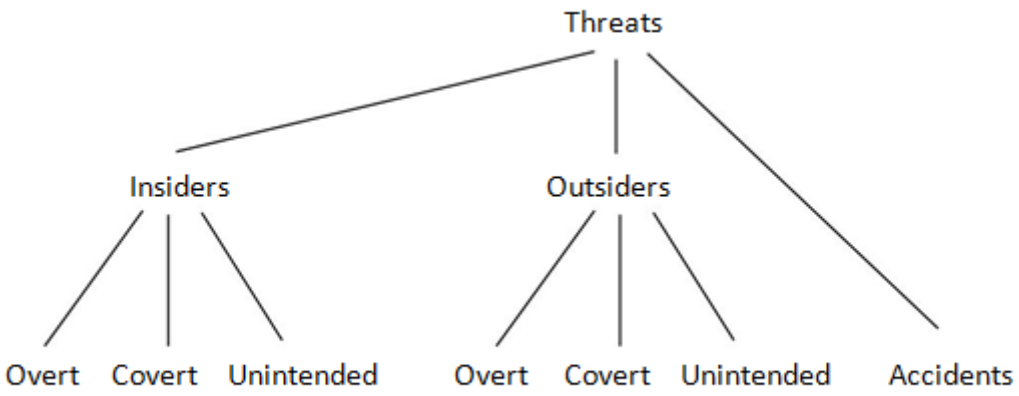
Turning a blind eye to cyber security is no longer an option. Businesses that fail to adequately protect themselves face the prospect of catastrophic consequences. Irrespective of the size, nature or purpose of the business, the effects of a cyber attack can be devastating. What's more, some of the highest-profile attacks over recent years have demonstrated how even the biggest companies in the world aren't always as well protected as they think they are. Even when their systems are brought back online and business continues as normal, the reputational damage incurred can be much more difficult to overcome.

Of course, it's not simply a case of proactively protecting your business and its general interests from cyber attacks. You also need to think carefully about the extent to which your *customers* are protected. Oftentimes, a security breach that has negative consequences for one or more customers

can be far more detrimental than an attack on the company itself. Businesses aren't simply expected to protect their customers online – they have a legal *obligation* to do so. All of which amounts to yet another responsibility, which calls for the input and expertise of talented of cyber security specialists.

Insiders and Outsiders

As far as general data security is concerned, there are two classifications of people – insiders and outsiders (aka employees and non-employees). Figure Intro.1 shows the three classes of computer security and crime caused by each of the two types, plus a special class of threats that are not directly caused by humans, namely accidents.



The seven individual classes are as follows:

1. Insiders overt. Overt actions on the part of insiders are usually the work of dissatisfied employees, often resulting in data being compromised and equipment being destroyed.
2. Insiders covert. Employees within a company can inflict more serious damage than outsiders, due to their access privileges and extensive knowledge of the organization in general.
3. Insiders unintended. Many security issues or threats that occur internally are the result of nothing more than genuine human error. This being one of the most common threat classes.
4. Outsiders overt. Direct attacks on network systems and computer facilities by outsiders, which also incorporates DoS attacks.
5. Outsiders covert. This refers to the type of attack that involves transmitting rogue software to one or more computers or systems from outside the business.
6. Outsiders unintended. It is fairly rare that an outsider will harm a computer or access sensitive data unintentionally.
7. Accidents. Issues regarding data integrity or security can arise due to unpredictable accidents that cannot be prevented, such as natural disasters, workplace fires and so on.

There are various different classifications of computer security issues and threats, though the vast majority can be grouped under three headers as follows:

- Physical Security. Examples of physical security issues include computer equipment being stolen, computer systems being accessed physically without authorization and general physical damage being caused to hardware.
- Rogue Software. This is the bracket that includes all examples of computer viruses and malware. More broadly, any software introduced to a system (accidentally or otherwise) that poses or creates a security threat.
- Network Security. The vast majority of computers these days are connected to one or more networks, which may be breached by insiders or outsiders. When a network is accessed or in any way compromised without authorisation, this is considered a network security issue.

It's hard to believe that such a complex and important field as computer security was largely non-existent three decades ago. The evolution of the field of cyber security in general over recent years has been no less than phenomenal.

While it's true to say that almost any security vulnerability or threat can be managed and brought under control, there is no such thing as 100% flawless protection from attacks. This is because cybercriminals are constantly refining and adapting their techniques, creating something of a continuous cat-and-mouse 'game' with cyber security experts. Both parties doing everything they can to stay one step ahead of the other.

Microsoft's 10 Laws of Cyber Security

Leading software companies like Microsoft employ enormous teams of cyber security experts to safeguard their systems and software. Over the years, Microsoft has published an extensive archive of invaluable cyber security guidelines for businesses of all shapes and sizes. They've also produced and published their own "10 laws of cyber security", which can and should be implemented at all levels throughout the business.

The 10 rules outlined by Microsoft are as follows:

1. If someone can persuade you to run their program on your computer, it's not your computer anymore.
2. If someone can alter the operating system on your computer, it's not your computer anymore.
3. If someone has unrestricted physical access to your computer, it's not your computer anymore.

4. If you allow someone to upload anything it's a to your website, it's not your website anymore.
5. Weak passwords defeat strong security.
6. A computer is only as secure as its owner/user is trustworthy.
7. Encrypted data is only as secure as the decryption key.
8. An out-of-date virus scanner is only marginally better than none at all.
9. Absolute anonymity isn't practical, in real life or on the Web.
10. Technology is not a panacea.

Physical Security

The vast majority of cyber security threat and attacks are 'virtual' in nature. Or in other words, those responsible don't gain physical access to the networks and computer systems they target. But alongside viruses, identity theft, general data security breaches and so on, there lies another aspect cyber security that's just important as virtual security. That being, the physical protection of computer equipment again every possible eventuality. Examples of which include fires, floods, theft and accidental damage.

Physical Threats

One of the most common physical threats to cyber security is also one of the most overlooked and underestimated. Electrical power surges – which can occur at any time without warning – can effectively destroy electronic devices like computers in a split second. This is why the use of power surge protectors and uninterruptible power supplies is considered mandatory by cyber security experts. The more important the computer or IT system, the greater the measures that should be taken to protect them.

The physical security of computers and network systems often begins and ends with the security of the facility itself. If the office or business location is not sufficiently protected from unauthorized entry, the risk of theft or damage to its property is elevated. The more difficult you make it for would-be criminals to gain access to your computers and related technology, the lower the likelihood of falling victim to attack. The physical security of the facility itself can also play a role in minimizing the threat posed by fire, flood and similar unpredictable eventualities.

It's therefore worth taking a step back from time to time to consider the extent to which your computer systems and related technology are protected. Is your building secured with impenetrable locks? Do you have a high-quality alarm and/or surveillance system in place? Have you set up a system to receive automatic alerts in the case of unauthorized entry? Exactly how much damage could a disgruntled employee cause, if they successfully gained unauthorized entry to your building?

All such questions form part of the essential cyber security risk assessment, which should be performed on a regular basis.

User tracking

Accountability lies at the heart of every successful cyber security framework. Or to put it another way, you need to maintain an accurate record of who is accessing your systems, when they are accessing them, where from and what kinds of activities they are performing. The greater the extent to which you track the activities of every user, the easier it becomes to pinpoint the responsible parties in the event of a cyber security issue.

A good working example is that of a team of administrators working in a doctor's surgery. Each of these workers will have their own unique login credentials, along with a card that must be used to activate the computer system. After which, a detailed log of their activities is kept until the moment they log off. Every page they visit within the intranet, every appointment they book, every note they take and every record they access. All such information is stored securely for future access and cannot be edited or deleted by anyone in the facility.

This way, any errors or oversights identified at a later date can be traced back to their origins. Most of which will, of course, turn out to be human error, but the importance of accountability cannot be overstated. These kinds of user tracking systems also serve as helpful deterrents, dissuading would-be attackers from engaging in malicious activities while logged-on. That is, unless they are able to log on using someone else's credentials – hence, the importance of strong and regularly updated passwords.

Physical Protection of Data

One of the biggest problems with physical data storage devices is the fact that most of them can be easily damaged or destroyed. Hard drives, DVDs, USB sticks and so on – all relatively simple to compromise. Both accidentally and maliciously, these and other physical storage devices/mediums come to harm on a daily basis.

This is why it is of the utmost importance to ensure *all* important data is backed up on a regular basis. Data storage devices in general should be viewed as fragile and imperfect. It should be assumed that at any time and without warning, any given device could be laid to waste. In which case, you'll be glad you made a backup you can now use in its place. Ideally, the data you back up should be kept in a separate location, away from the original storage device. The reason being that in the case of fire, flood, theft or accidental damage, you won't run the risk of *both* copies being damaged or destroyed at the same time.

Backing up data using online storage facilities is an option, but again cannot be counted on as flawless. It's important to remember that anything that exists in the virtual space of the web has the potential to be compromised at any time. Even if the likelihood is minimal, it still exists. Where data is important and you simply cannot risk losing it entirely, physical backups should be made on a regular basis and stored in a safe location.

Recovery Planning

Armed with these regularly updated backups, the proactive business is able to formulate an effective disaster-recovery plan. Your recovery plan should include a complete and detailed summary of what to do, in the event that your facility (as a whole or in part) is destroyed, or rendered inoperable. Typical information contained within a recovery plan may include the location of the data backups, instructions for the the procurement of new computer systems, the individual responsibilities of each member of the workforce, where new physical premises should be set up and so on.

Along with regularly updated backups, it can also be useful to keep hard copies of important documents. This is precisely why some of the most important documents in business and in everyday life have not yet been digitized. Contracts, invoices, purchase receipts and so on – all considered too important *not* to keep a hard copy of. This way, even if your primary systems and backups are destroyed, you'll still have a hard copy to work with. If you do keep hard copies, however, you'll need to ensure they are adequately protected and destroyed when no longer needed.

What is Cyber Crime?

The term 'cyber crime' refers to any unlawful activity involving a computer or a connected device of any kind. Incidents resulting from human error or accidents are not considered cyber crimes, but may nonetheless constitute a severe cyber security risk. For a cyber crime to be committed, the individual needs to have the express desire to carry out one or more unauthorized actions, which may have catastrophic consequences for the victim. Cyber criminals typically carry out their attacks for purposes of greed, revenge or simple enjoyment.

Cyber Crimes by Insiders and Outsiders

Cyber criminals may be known to the organization or entity they attack, or may be a stranger they've never had any contact with. As a result, there are two distinct categories of cyber attacks carried out by criminal entities worldwide:

- **Insider Attack**: An internal attack occurs when an individual engages in some kind of malicious activity, by way of their authorized access to the system. In the vast majority of instances, internal attacks are carried out by disgruntled employees, dissatisfied contractors, former

employees who still have access to the organization's systems and so on. Insider attacks can be particularly devastating, as the user may have high-level access privileges. However, insider attacks are also comparatively easy to trace back to their origins, ensuring the responsible parties are identified and held accountable.

- **External Attack**: By contrast, external attacks occur when anyone who does not have authorized access to the company's systems launches an attack. Any business that operates computers and IT systems that are connected to the Internet is technically a viable target for external attackers worldwide. Most external attacks are thwarted by firewalls and similar safeguards, though cannot be ruled out of the equation entirely. External attacks are motivated predominantly by greed, or on the basis of a dispute/disagreement with the organization in question.

Structured and Unstructured Attacks

Cyber attacks can also be divided into a further two categories – structured attacks and unstructured attacks. This is essentially a reference to the maturity and sophistication of the attacker at the time of the incident.

- **Unstructured Attack**: An unstructured attack will typically be carried out by an individual with little knowledge and experience. They may also have no specific motive for the attack, or a sense of the severity of the crime they are committing. Unstructured attacks are often performed on a random basis and can therefore be highly unpredictable.
- **Structured Attack**: The difference being that with a structured attack, the perpetrator knows exactly what they are doing and has a full understanding of the consequences of their actions. They are familiar with sophisticated hacking tools and technologies, they have a specific target in mind and most likely an objective. Essentially, structured attacks are performed by professional criminals, who know exactly what they want and have no interest in the potential consequences.

The appeal of cyber crime among criminal entities worldwide is growing. This is because cyber crime has the potential to generate enormous returns, by way of a low-risk, low-investment 'business' venture.

Not just this, but when cyber crimes are carried out by perpetrators from a far-off nation, it is almost impossible to bring them to justice. Even if they are identified, the likelihood of them being held accountable for their actions is low. The growing appeal of cyber crime representing one of many challenges facing cyber security experts and the businesses they work for worldwide.

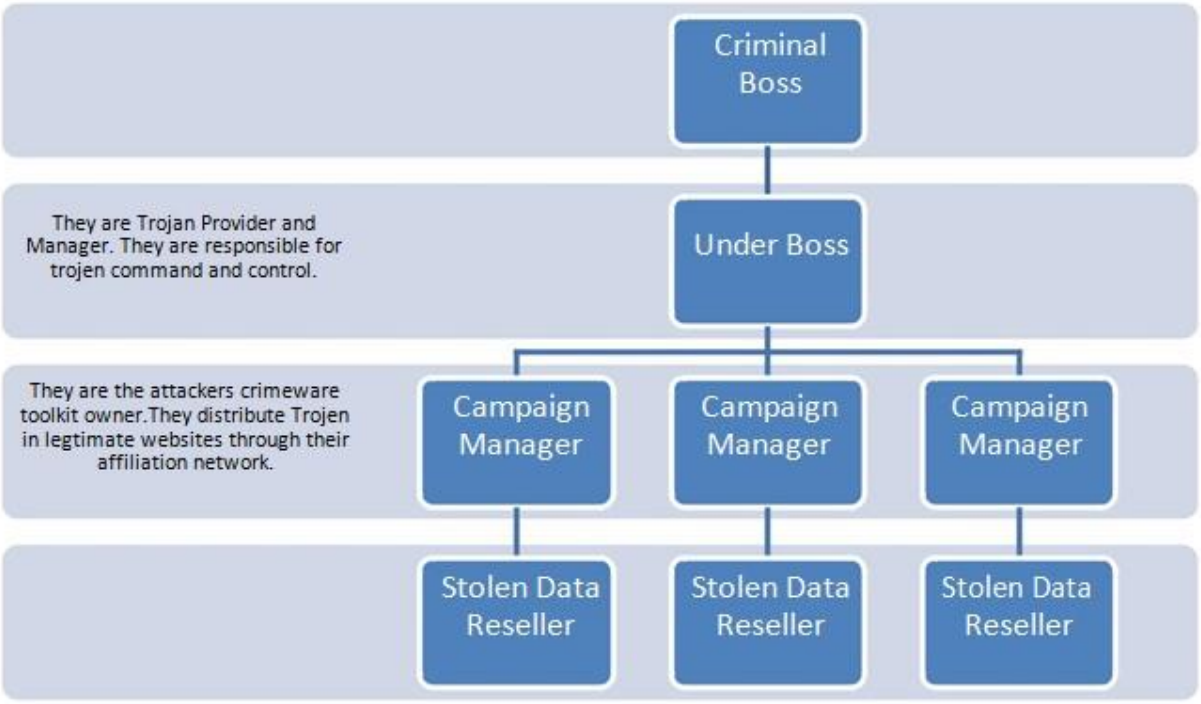


Figure 1.1 : Hierarchical Organisational Structure

The above represents the typical hierarchical organizational structure of a cyber crime enterprise. However, the hierarchy remains in a constant state of change and is based purely on opportunity. For example, if a hacker has the knowledge and expertise to sell sensitive data directly to a buyer at a lucrative price, he or she is unlikely to involve middlemen. By contrast, if the hacker doesn't have the contacts he or she needs to make a sale, they may only be able to operate as part of a criminal gang.

Motivations for Cyber Crime

Both the prevalence and the extent of the threat posed by cyber crime has grown exponentially over recent years. In terms of motivations, some of the most common reasons for engaging in these kinds of criminal activities include the following:

a. Money: The vast majority of people who commit cyber crimes are motivated by the prospect of making a lot of money in a short space of time.

b. Revenge: It's also common for people to commit cyber crimes as a form of revenge. One example of which being a disgruntled former employee launching an attack on their former employer.
c. Terrorism: Attacks motivated by religion or personal beliefs are becoming increasingly common, which can lead to enormous physical or economic loss for the victims.
d. Fun: There's often no specific motivation for a cyber attack, other than the entertainment of those responsible. They simply want to see what they're capable of.
e. Recognition: Hacking a supposedly impenetrable network can be an enormous source of pride and kudos for those operating in known cyber crime networks worldwide.
f. Anonymity: Individuals who would normally shy away from crime may take part in cyber crime activities, having been won over by the prospect of near-total anonymity.
g. Espionage: Computer systems worldwide are regularly hacked and/or monitored by international agencies and governments – a form of cyber espionage.

As it is often difficult to identify the parties responsible for a cyber crime, it is not always possible to pinpoint any specific motivation for the act.

The Different Kinds of Cyber Crime

As cyber criminals continue to evolve and enhance the sophistication of their attacks, new types of cyber crime are being identified all the time. As it stands, some of the most common types of cyber crime committed on a global basis are as follows:

Cyber Stalking

The term 'cyber stalking' refers to any kind of harassment or threatening behaviour perpetrated online. Social media in particular has provided an open platform for cyber criminals to stalk victims online, with little risk of being identified or held accountable. The effects of cyber stalking on those targeted can be devastating.

Child Pornography

Any kind of possession, distribution or accessing of sexual images or videos of minors (under the age of 18) is a serious criminal offense.

Forgery and Counterfeiting

The growing sophistication of computer technology is making it easier than ever before to counterfeit documents and create forgeries. To such an extent that it can be almost impossible to differentiate a counterfeit document from an original, without the use of extensive forensics.

Software Piracy and Crime related to IPRs

The unauthorized reproduction and/or distribution of software is referred to as software piracy. The world's biggest software companies invest heavily in the development of robust piracy prevention measures, but sophisticated cyber criminals are only ever a couple of steps behind.

Cyber Terrorism

Defined as the use of computer resources to intimidate or coerce government, the civilian population or any segment thereof in furtherance of political or social objectives.

Phishing

The term 'phishing' is used in reference to any attempt to acquire the personal information of one or more parties, by sending emails that look to have been sent from a trustworthy source. Common examples of which including emails that look almost identical to those sent by eBay, Amazon and Netflix, though are actually sent from rogue entities for the purpose of stealing the recipient's private information. Another form of phishing is Smishing, in which SMS text messages are used to lure customers.

Computer Vandalism

Any attempt to damage or destroy a computer or IT system using either malicious software or physical force is considered computer vandalism.

Computer Hacking

Computer hacking occurs when an individual or group thereof gains unauthorized access to any computer, device or IT system of any kind. Computer hacking can occur locally or remotely, motivated by the desire to steal sensitive data, destroy the information stored on the system or simply make a political point. Hackers also routinely lock individuals and businesses out of their systems entirely, demanding ransom payments to 'unlock' their computers.

There are four primary classifications of hackers, as outlined below:

- **White Hat**: These are the professional 'ethical' hackers, who are hired by businesses to find issues are vulnerabilities in their defences. Rather than actually engaging in malicious activities of any kind, they simply pinpoint the kinds of problems that could open the door to cyber criminals. Some are employed by businesses on a fulltime basis, others offer their services as self-employed freelancers.

- **Black Hat**: By contrast, the black hat hacker *only* has criminal intentions in mind. They may be motivated by any of the factors listed above and have no regard for the consequences of those they target. Most established black hat hackers have access to sophisticated hardware and software, along with the physical and virtual resources needed to orchestrate ambitious attacks.
- **Grey Hat**: The grey hat hacker identifies security vulnerabilities and provides the services required to address them, usually for a predetermined fee.
- **Blue Hat**: Prior to the launch of a new system or a system upgrade, an organization may hire a blue hat hacker to identify any potential issues *ahead* of time. Prevention at the earliest possible stage being preferable to addressing issues only when identified at a later date.

Creating and distributing viruses over internet

The vast majority of computer viruses serve no purpose other than to cause problems for those affected. Some hackers invest relentlessly in the development of cutting-edge viruses, with the potential to take down (or cause damage to) millions of computer systems worldwide. As a result, viruses are rarely created or distributed for the purpose of making money.

Spamming

Slowly but surely, spamming is being acknowledged as a form of cyber crime in its own right. In order for a message to be considered spam, it typically needs to form part of a mass mailing exercise, be sent from an entity with an unknown identity and have been sent without the express permission of the recipient. Spam emails aren't usually 'dangerous' as such, but can be inconvenient and irritating at the best of times.

Online Auction Fraud

The popularity of online auction sites like eBay has triggered a new wave of fraudulent activities by cybercriminals. Quite simply, items are listed for sale that either don't exist or will never reach the winning bidder. Instead, the 'seller' simply makes off with the money and disappears entirely.

Cyber Squatting

Defined as an act of reserving the domain names of someone else's trademark, with the intent to sell it afterwards to the organization who is the owner of the trademark at an elevated price.

Logic Bombs

A logic bomb is formally defined as a piece of code that is intentionally inserted into a software system, which will be automatically activated when certain conditions are met. In a working example,

an employer may insert a piece of code into a system that will begin wiping information and generally causing havoc, should their contract be terminated.

Web Jacking

This is a form of digital hijacking, wherein the hacker gains access to a website without authorization and summarily prevents its rightful owner from accessing it. They may do so to demand a ransom payment to unlock the site, or for political or social purposes.

Internet Time Thefts

Hacking the username and password of ISP of an individual and conducting online activities at their expense is referred to as Internet Time Theft.

Denial of Service Attack

A DoS attack occurs when a cybercriminal (or group thereof) attempts to flood a website with an influx of spam traffic, creating the kind of congestion that prevents it from operating properly. This is why it's often necessary to tick an 'I Am Not a Robot' box, before being granted access to a website.

Email Spoofing

This is where the header information of an email is changed to hide the identity of the actual source, making it look as if the email was sent from a source that was not in fact the actual sender.

Further Reading: