UNIT-1 The Need for and Importance of Security

Learning Outcomes

By the end of this unit the learner will be able to:

- ✓ Understand the importance of security
- ✓ Discuss the various stages of the risk assessment process
- ✓ Identify the differences between the various types of assets

Unit 1

The need for Importance of Security

In today's fast paced modern world, the importance of security is greater than ever before. This is also the reason why security is one of the fastest growing sectors, creating millions of new job opportunities that didn't exist just a few years ago.

What makes the difference in today's security landscape is the way in which threats are no longer confined to traditional physical security issues. The internet has paved the way for an entirely new category of criminal activities, posing a direct threat to practically every business in operation worldwide.

For today's business, an effective security management system must take into account and sufficiently safeguard three entirely different classifications of assets:

1. **Physical assets**
2. **HR assets**
3. **IT assets**

Each of which brings its own unique challenges into the mix, which must be considered independently within the individual asset classification *and* as part of a broader security program.

What is Security?

The term 'security' derives from the Latin word for 'care' or 'concern'. It is used in relation to any policy, procedure, action or activity undertaken to protect an entity from an undesirable outcome.

For today's business, security is the sum total of all resources and measures invested in the prevention of unlawful or potentially harmful interventions. Hence, for a security policy or framework to be considered viable and effective, it must take into account *every* identifiable risk at *every* level across the organization as a whole.

Importantly, security should never be misinterpreted as a finite task or a one-time-only responsibility. Quite the opposite - security is an ongoing and endless activity, which in order to be successful must be continuously revisited, refined and improved along the way.

As there's no such thing as a 'flawless' security framework, there is always room for improvement.

The Five Graded Levels of Security

Every organization has its unique security requirements, which for some will be more sophisticated and advanced than others. Across the board, however, security can be graded within five levels, in accordance

with the threat respectively:

- **Minimum Level** – The most basic provisions to prevent unauthorized entry and activities on the part of external parties
- **Low Level** – Relatively remedial security policies and processes to detect, prevent and address unauthorized internal and external activity
- **Medium Level** – Extends security policies to include the forecasting of potential threats and more comprehensive preparation to successfully detect and impede internal and external threats
- **High Level** – Aims for more comprehensive protection for the organization, incorporating contingency management and disaster planning
- **Maximum Level** – Advance integrated security systems to provide protection on a national security level.

Changing Trends in Security

In years gone by, the only threats posed to organizations in general were physical in nature. The idea of launching a remote or 'virtual' threat against an organization would have seemed nonsensical.
Likewise, organizations once existed in an era where national and international terrorism wasn't considered a particularly credible threat. Today, many countries worldwide live with a continuously elevated terrorism 'threat level' and must therefore consider the potential consequences of such an event.
To a degree, this doesn't mean that the likelihood of any given business falling victim to a dangerous incident is higher today than it was before. It's more a case of the types of threats the business must contend with having become more diverse and difficult to protect themselves against.
Particularly when it comes to virtual threats, it's a continuous 'cat and mouse' game to try to stay one step ahead of sophisticated criminal entities.

The Principles of Security

While every organizational security policy is unique, all efforts and activities are guided by a series of universal security principles. The most important of which are as follows:

- Business activities fuel the economies of every nation. In which case, business security plays a direct role in national economic stability.
- Even the smallest additional efforts made to protect a business or a sector from threats can make a big difference.
- Security is a shared responsibility throughout the organization, which should involve top management and leadership figures.
- Security should never a mistakenly be viewed as a non-productive investment.
- An effective security policy is one that makes allowances for acceptable levels of residual risks.
- The only viable approach to security is to view it as a continuous activity where there is always room for improvement.

- Even when returns on security investments cannot be quantified monetarily, this doesn't mean they aren't financially beneficial.

Individual Safety and Security

The importance of individual safety and security lies not only in the physical safety and wellbeing of the individual, but also their psychological wellbeing. Individual safety and security doesn't just reduce/eliminate the threats of physical harm - it also removes the *fear* of harm from the equation.

Threats to individual safety and security vary in terms of source, severity and likelihood of occurrence. All types of accidental injuries fall within this bracket, as do episodes of deliberate violence or threatening behaviour. Even when the physical harm suffered by an individual is relatively minor, the psychological impact such an event can have may be life affecting long-term.

Physical Security Controls

Physical security controls are the equipment, materials and procedures put in place to protect an organization and its assets. Physical security is based around similarly physical (or tangible) countermeasures, including things like CCTV camera, security lighting, reinforced doors, fences, gates and so on.

These types of controls are implemented to deter would-be intruders on two equally important levels:

Physical Deterrence

This refers to the process of deterring criminals by placing physical barriers between them and the organization (or its assets). From locked doors to bolted shutters to window bars and so, anything that makes it physically difficult to get into the building in the first place is an example of a physical deterrent.

Psychological Deterrence

Equally important and effective, psychological deterrence works on the basis of the would-be intruder's perceived consequences of their intended actions. For example, a CCTV system or intruder alarm won't physically stop them from entering the building, but will make it far more likely that they'll be identified and prosecuted.

As a result, an effective security system must always place equally heavy emphasis on physical and psychological deterrence. Neither is necessarily 'better' than the other - both are required for a security framework to achieve its objectives.

Vulnerability Assessment

The first step in the process when devising a security policy is to conduct a detailed vulnerability assessment. A vulnerability assessment provides the organization with the detail information and insights they need to identify security weaknesses and make the necessary improvements. Vulnerability assessments must be carried out in a structured and formal way, as a collaborative effort between senior management (or business owners) and experienced security personnel.

At its core, at vulnerability assessment seeks to identify witch of the organization's assets are at risk and therefore need protecting. Where there's a vulnerability, the business and its assets are at risk. All existing security measures are then identified and assessed, in order to determine what is working and what needs to be expanded or improved. To an extent, a vulnerability assessment must be conducted from the perspective of a would-be attacker, for whom spotting security flaws and weaknesses is no less than a career.

For a vulnerability assessment to be performed successfully, the organisation and its key personnel must focus heavily on the following:

Asset Identification

This refers to the process of identifying the various assets the business either owns or is responsible for, which may fall within a series of categories including:

- **Property** - Business premises, office equipment and physical assets
- **Human Resources** - The workforce, customers, visitors etc.
- **Information** - Financial data, customers' private information, important documents

Where an asset is of potential value at any level - tangible or intangible - it needs to be incorporated in a vulnerability assessment.

After successfully identifying and recording the organization's assets, the next step in the process is to assess the potential threats posed to these assets accordingly.

Threat Perception

Today's organization must contend with a longer and more diverse list of potential threats they're never before. Threats to any given asset can be numerous, such as in the examples below:

- **Infrastructure**. Natural disasters, accidental damage, deliberate sabotage.
- **Physical Assets**. Theft, purposeful damage, accidental damage.
- **Human Resources**. Violence, threatening behaviour, accidents/ injuries.
- **Information.** Data theft, server failure, hacking

Considering these different types of threats is essential to ensure that the business is ready for any potential security issues it may encounter. It's also important to carefully consider the likelihood of any given security issue occurring, along with the potential consequences in the event that it does.
This is necessary to subsequently prioritise the vulnerabilities, in order that they can be addressed in order of severity and significance.

Standards in Security

To establish standards is to create an agreed, effective and repeatable way of getting something done. In security, it means publishing a document (or series thereof) that outlines the policies and practices everyone must adhere to. The importance of standards lies in the fact that they bring consistency, simplicity and reliability into security practices.

To a degree, to attempt to get by without establishing standards is to make things up as you go along. For this reason, this is neither an efficient nor a viable solution for today's organization.

The Benefits of Standards

In the field of security, standards (in terms of practices, policies and procedures) often differ wildly between different security and police organizations. This can sometimes lead to difficulties with collaborative ventures and general communications.

Therefore, it is generally believed that to introduce much broader standardisation would bring a variety of benefits such as:

- Improved efficiency and consistency
- Lower operational costs
- Easier training for new security personnel
- Enhanced accountability
- Simplified communication between parties
- The opportunity to collaborate more efficiently
- Elimination of ambiguity and misunderstandings

Challenges to Standardisation

While most agree that widespread standardisation would be beneficial, there's no denying the enormous challenges such an initiative would face. Particularly due to the near-total privatisation of the security sector, wherein different organizations and entities approach things in very different ways.

Lack of Coordination among Different Security Providers

Decentralised security enables those within the sector and those hiring security services to essentially write their own rulebooks. This in turn means that the operational models and policies of two separate security services or entities will almost always be completely different. There's little to no widespread coordination (or even communication) between these separate entities, making it difficult (if not impossible) for standardisation efforts to be stepped up.

The Risks of Poor Data Security Management

Without broad and effective data security policies in place, an organization leaves itself wide open to attack. Both on external and internal levels, threats that are not planned for are exponentially more likely to materialise.

Typical internal threats the business must contend with include information theft, deliberate or accidental damage of IT equipment, corruption of data, legal liability and so on. External threats extend to hacks conducted by external parties, damage to off-site servers, viruses, trojans and more.

Getting to grips with data security management means focusing the necessary time, effort and resources on the following:

- ***Integrity***: This means making sure that the data you collect, hold and use isn't modified or compromised without authorization. There should be systems in place to both detect and prevent data from being modified, thus preserving its integrity. In a typical example, a hacker may target a server and alter the account number of a weekly payment recipient, so that they receive the payment illegally.
- ***Availability***: Only those who absolutely *need* to be able to access any given piece of data should be permitted to access it. The more heavily you restrict access to important information and sensitive data, the less likely it is to fall into the wrong hands. When any data is no longer required, it should be removed completely so that it is no longer available for *anyone* to access.

Risk Assessment

A risk assessment is a little like a vulnerability assessment, though takes a look at potential risks and threats on a much more in-depth level. Organisations of all shapes and sizes are advised to conduct risk assessments on a regular basis, in order to establish how well-protected (or otherwise) they are from the various threats they face.

Risk assessments are usually conducted by senior management, in conjunction with security personnel where present. For a risk assessment to achieve its objectives, it must be overseen by those who understand the business inside and out. Each and every member of the workforce should be invited to

offer their suggestions and contribute to the process, but the criticality of top-level management involvement cannot be overstated.

Far too many business owners and senior managers see risk assessments and security in general as a non-priority, without realizing just how important they are.

Risk Management

The term 'risk management' refers to a series of interconnected activities, initiatives and policies, which come together to protect the organization from all threats at all levels. As the threats faced by each and every business are fundamentally unique, so too should be every risk management framework.

A risk management take things a step further by identifying, classifying, categorising, prioritizing and ultimately putting measures in place to mitigate all types of risks. Effective risk management means first building an understanding of threats, vulnerabilities and controls, as defined briefly below:

- **Threat**—This refers to anything that 'threatens' the organization directly (manmade or otherwise) that could lead to negative consequences.
- **Vulnerability**—This refers to an error, issue, oversight or imperfection in existing security coverage that could be exploited to the organization's detriment.
- **Controls**—This refers to all actions, activities and policies put in place to prevent, address or deter the potential risks from occurring.

Mitigating Risk

Accurately and comprehensively identifying all risks at all levels is the most important step in the risk management process. After which, the time comes to decide exactly what you are going to do about the risks you have identified. The action required will be determined by the nature and severity of the risk in question, along with its likelihood of occurring.

However, there are four primary ways by which risk can be dealt with, which in many instances may be combined with one another:

- **Risk Reduction**—Implementation of measures to reduce the likelihood of the risk occurring, or the severity of the consequences if it does.
- **Risk Transference**—Covering the business against the consequences of the risk by transferring them elsewhere - such as insuring property against damage.
- **Risk Acceptance**—Where the risk is considered relatively minor and its potential consequences are therefore simply accepted by the business.
- **Risk Rejection**—Exclusion of the risk from consideration and ignoring it entirely, under the assumption it will not occur.

In terms of which approach to handling risk is most appropriate, it comes entirely down to the nature of the risk, its likelihood of occurring, the potential consequences if it does and whether it is realistically possible to control or prevent it.

The simple fact of the matter being that in many instances where important and potentially major risks are identified, there isn't a great deal the organisation can do about them. In order to go about its everyday operations, every business must take a wide variety of risks, all day and every day.
There is no such thing as a 100% secure organization, nor should any business strive to eliminate all risk from the equation.

Multi-Dimensional Security

The only viable approach to security for today's organization is a complex and multi-dimensional approach. Conducting detailed assessments is essential to build a comprehensive picture of the various risks and vulnerabilities the business needs to contend with. After which, it's a case of determining which kinds of policies and protocols need to be drafted and brought in accordingly.
Physical security (by way of physical deterrents) isn't a particularly complex subject. Essentially, any obstacles or barriers you can physically place between your organisation's assets and would-be criminals will help get the job done.

Data security, on the other hand, isn't quite so simple. There's no 'physical' way of preventing hackers from making their way into the your systems - everything takes place in a more 'virtual' capacity.
This is where data security safeguards such as the following are essential:

- Passwords
- Patch management
- Backup practices and storage requirements
- Security awareness training
- Antivirus
- System setup and configuration

Of course, internal risks (those posed by the workforce itself) can be even more difficult to prevent and plan for. There's almost no way of knowing who will pose a threat to your business and its assets at any given time, be it directly, indirectly, deliberately or accidentally.

Nevertheless, the findings of your risk assessment and vulnerability assessment will help you determine the extent to which your business needs to contend with internal threats.

Effective security always starts at the top of the business, going on to permeate each hierarchical level right down to the bottom. The decisions on what needs to be protected and how should be made by senior management, before being formally recorded in the form of policy documents.

Prior to being formalised, the content of the documents should be checked to ensure none of the policies break any applicable laws. It should also be made clear at to what extent all members of the workforce are expected and required to contribute to the organisation's security framework.

The Evolution of Security Standards

As touched upon earlier, the subject of 'standards' in security is still something of a grey area. But what also makes the standardisation of security practices are difficult is the way in which security standards (in the sense of expectations and quality) are continuously evolving

Today, the most broadly-acknowledged and followed security standards (or principles) are the various 'ISO' standards. The International Organization for Standardization publishes a series of good practice standards, which are internationally agreed by experts in their respective fields.
ISO standards in terms of security are therefore considered the best way of doing something, but do not necessarily represent 'rules' and are not a matter of law.

For example, ISO 45001 - OCCUPATIONAL HEALTH AND SAFETY - was introduced to help organizations improve working conditions and general workplace safety for the benefit of employees. Meanwhile, ISO/IEC 27001 - INFORMATION SECURITY MANAGEMENT - was more recently introduced, in an attempt to standardise data security practices for the modern business.

You'll find full information on ISO standards and their relevance on the official International Organization for Standardization website, which can be accessed via the following link:

https://www.iso.org/standards.html

Further Reading:

- ✓ ***The Importance of Information Security Awareness for the Success of Business Enterprises January 2016 by Ebru Yeniman Yildirim***
- ✓ ***Security Awareness February 4, 2020 'The Importance of Security Awareness Training' by Cindy Brodie***