UNIT 1
INFORMATION SECURITY (INTRODUCTION)

1. *Read the following terms and word combinations and learn them:*

Information security - информационная безопасность
Confidentiality - конфиденциальность
Integrity - целостность
Availability - доступность
Hardware - аппаратные средства
Software - программное обеспечение
Unauthorized access - несанкционированный доступ
Unauthorized use - несанкционированное использование
Unauthorized disclosure - несанкционированное раскрытие
Unauthorized disruption - несанкционированное разрушение
Unauthorized modification - несанкционированное изменение
Unauthorized perusal - несанкционированное прочтение
Unauthorized inspection - несанкционированный просмотр
Unauthorized recording - несанкционированная запись
Unauthorized destruction - несанкционированное уничтожение
Data - данные
Database - база данных
Application - приложение
To collect information - собирать информацию
To process information - обрабатывать информацию
To store information - хранить информацию
To transmit information - передавать информацию
Computer/server malfunction - неисправность компьютера/сервера
Computer security - компьютерная безопасность
Information assurance - гарантия информации

2. *Read and translate the following text:*

Information security (InfoSec for short) means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are often interrelated and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them.

These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration.

Information security is concerned with confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print or other forms.

Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer.

It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory (even a calculator). IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal systems.

Information assurance is the act of ensuring that data is not lost when critical issues arise. These issues include but are not limited to: natural disasters, computer/server malfunction, physical theft, or any other instance where data has the potential of being lost. Since most information is stored on computers in our modern era, information assurance is typically dealt with by IT security specialists. One of the most common methods of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arise.

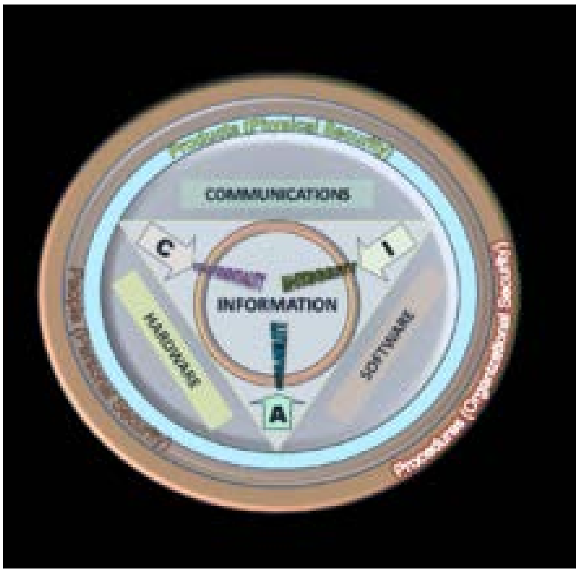
Governments, military, corporations, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers.

Should confidential information about a business' customers or finances or new product line fall into the hands of a competitor or a black hat hacker, a business and its customers could suffer widespread, irreparable financial loss, not to mention damage to the company's reputation. Protecting confidential information is a business requirement and in many cases also an ethical and legal requirement.

For the individual, information security has a significant effect on privacy, which is viewed very differently in different cultures.

The field of information security has grown and evolved significantly in recent years. There are many ways of gaining entry into the field as a career. It offers many areas for specialization including securing network(s) and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning and digital forensics, etc.

Information Security Attributes: or qualities, i.e., Confidentiality, Integrity and Availability (CIA). Information Systems are composed in three main portions, hardware, software and communications with the purpose to help identify and apply information security industry standards, as mechanisms of protection and prevention, at three levels or layers: physical, personal and organizational. Essentially, procedures or policies are implemented to tell people (administrators, users and operators) how to use products to ensure information security within the organizations.


Products (Physical Security)
COMMUNICATIONS
C
I
INFORMATION
HARDWARE
SOFTWARE
A
People (Personal Security)
Procedures (Organizational Security)

Definitions:

The definitions of InfoSec suggested in different sources are summarised below:

1. "Preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved." (ISO/IEC 27000:2009)

2. "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." (CNSS, 2010)

3. "Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)." (ISACA, 2008)

4. "Information Security is the process of protecting the intellectual property of an organization." (Pipkin, 2000)

5. "...information security is a risk management discipline, whose job is to manage the cost of information risk to the business." (McDermott and Geer, 2001)

6. "A well-informed sense of assurance that information risks and controls are in balance." (Anderson, J., 2003)

7. "Information security is the protection of information and minimises the risk of exposing information to unauthorised parties." (Venter and Eloff, 2003)

8. "Information Security is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organizational, human-oriented and legal) in order to keep information in all its locations (within and outside the organization’s perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats. Threats to information and information systems may be categorised and a corresponding security goal may be defined for each category of threats. A set of security goals, identified as a result of a threat analysis, should be revised periodically to ensure its adequacy and conformance with the evolving environment. The currently relevant set of security goals may include: confidentiality, integrity, availability, privacy, authenticity & trustworthiness, non-repudiation, accountability and auditability." (Cherdantseva and Hilton, 2013)

Profession

Information security is a stable and growing profession – Information security professionals are very stable in their employment; more than 80 percent had no change in employer or employment in the past year, and the number of professionals is projected to continuously grow more than 11 percent annually over the next five years.

3. *Answer the following questions:*

1) What does information security mean?
2) What are information security components (attributes)?
3) What does computer security focus on?
4) What are the most common methods of providing information assurance?
5) Why is protecting of confidential information very important?
6) How is most of information collected, stored and transmitted nowadays?
7) What consequences can be in the case of a breach of security?
8) Do you think a career in this field can be very perspective?
9) What are your professional plans for future?
10) What do you know about the history of origin and development of information security?

4. *Read the following statements. Are they true or false?*

1) Information security, computer security and information assurance are the same things.
2) A computer is any device with a processor and some memory (even a calculator).
3) IT security specialists are very seldom found in major enterprises.
4) The field of information security has grown and evolved significantly in recent

years.
5) It is a problem to gain entry into this field as a career.

5. *Summarize the text.*

UNIT 2
HISTORY

1. *Read the following terms and word combinations and learn them:*

To detect tampering - обнаружить подделку
Cipher - шифр
Procedural handling control - контроль за процедурой обращения (с информацией)
To intercept (information) - перехватывать (информацию)
To decipher - расшифровывать
To reseal (a letter) - запечатывать снова (письмо)
To codify - приводить в систему
Multi-tier classification system - многоступенчатая система классификации
To scramble information - зашифровывать информацию
To unscramble information - расшифровывать информацию
Hardware - аппаратные средства
Software - программное обеспечение
Data encryption - шифрование данных
To store information - хранить информацию
To process information - обрабатывать информацию
To transmit information - передавать информацию
To share the common goals - разделять общие цели
Security and reliability of information systems - безопасность и надежность информационных систем

2. *Read and translate the following text:*

Since the early days of communication, diplomats and military commanders understood that it was necessary to provide some mechanism to protect the confidentiality of correspondence and to have some means of detecting tampering. Julius Caesar is credited with the invention of the Caesar cipher c. 50 B.C., which was created in order to prevent his secret messages from being read should a message fall into the wrong hands, but for the most part protection was achieved through the application of procedural handling controls. Sensitive information was marked up to indicate that it should be protected and transported by trusted persons, guarded and stored in a secure environment or strong box. As postal services expanded, governments created official organizations to intercept, decipher, read and reseal letters (e.g. the UK Secret Office and Deciphering Branch in 1653).

In the mid-19th century more complex classification systems were developed to allow governments to manage their information according to the degree of sensitivity. The British Government codified this, to some extent, with the publication of the Official Secrets Act in 1889. By the time of the First World War, multi-tier classification systems were used to communicate information to and from various fronts, which encouraged greater use of code making and breaking sections in diplomatic and military headquarters. In the United Kingdom this led to the creation of the Government Code and Cipher School in 1919. Encoding became more sophisticated between the wars as machines were employed to scramble and unscramble information. The volume of information shared by the Allied countries during the Second World War necessitated formal alignment of classification systems and procedural controls. An arcane range of markings evolved to indicate who could handle documents (usually officers rather than men) and where they should be stored as increasingly complex safes and storage facilities were developed. Procedures evolved to ensure documents were destroyed properly and it was the failure to follow these procedures which led to some of the greatest intelligence coups of the war (e.g. U-570).

The end of the 20th century and early years of the 21st century saw rapid advancements in telecommunications, computing hardware and software, and data encryption. The availability of smaller, more powerful and less expensive computing equipment made electronic data processing within the reach of small business and the home user. These computers quickly became interconnected through the Internet.

The rapid growth and widespread use of electronic data processing and electronic business conducted through the Internet, along with numerous occurrences of international terrorism, fueled the need for better methods of protecting the computers and the information they store, process and transmit. The academic disciplines of computer security and information assurance emerged along with numerous professional organizations – all sharing the common goals of ensuring the security and reliability of information systems.

3. *Answer the following questions:*

1) What did politicians, diplomats and military commanders understand since the early days of writing?
2) Who is credited with the invention of the Caesar cipher?
3) When and why was the Caesar cipher invented?
4) How was sensitive information marked and handled?
5) What official organizations did governments create as postal services expanded?
6) When did encoding become more sophisticated?
7) What advancements did the end of the 20th century and early years of the 21st century see?

8) How did computers become interconnected?
9) What fueled the need for better methods of protecting the computers and the information they store, process and transmit?
10) What are the common goals of numerous professional organizations?

4. *Read the following statements. Are they true or false?*

1) Only some years ago people understood that it was necessary to provide some mechanism to protect the confidentiality of correspondence.
2) The Caesar cipher was created in order to prevent secret messages from being read should a message fall into the wrong hands; it happened 30 B.C.
3) Governments have never created official organizations to intercept, decipher, read and reseal letters.
4) The war and wider use of electronic communication systems encouraged greater use of code making and breaking sections in diplomatic and military headquarters.
5) Encoding didn’t become sophisticated when machines were employed to scramble and unscramble information.

5. *Summarize the text.*

UNIT 3
BASIC PRINCIPLES, KEY CONCEPTS

1. *Read the following terms and word combinations and learn them:*

Accountability - подотчетность
Non-repudiation - неотказуемость
Legality - законность
Awareness - осознание
Responsibility - ответственность
Response - ответ, отклик
Ethics - этика
Democracy - демократия
Risk assessment - оценка риска
Security design and implementation - проект и осуществление безопасности
Security management - управление безопасностью
Reassessment - переоценка
Possession - владение, обладание
Authenticity - подлинность, достоверность
Utility - полезность
Transaction - операция, сделка
To enforce (confidentiality) - усилить (конфиденциальность)
To encrypt - зашифровать

Log file - файл регистрации
Backup - резервная копия
Printed receipt - напечатанный чек
Breach of confidentiality - нарушение конфиденциальности
Consistency - согласованность
Power outage - отключение эл. питания
Upgrade - повышение технических возможностей (компьютера)
Denial-of-service - отказ в обслуживании
Genuine - подлинный
To validate - подтверждать
Digital signature - цифровая подпись
Public key encryption - шифрование с открытым ключом

2. *Read and translate the following text:*

Key concepts

The CIA triad (confidentiality, integrity and availability) is one of the core principles of information security. (The members of the classic InfoSec triad -confidentiality, integrity and availability - are interchangeably referred to in the literature as security attributes, properties, security goals, fundamental aspects, information criteria, critical information characteristics and basic building blocks.) There is continuous debate about extending this classic trio. Other principles such as Accountability have sometimes been proposed for addition – it has been pointed out[citation needed] that issues such as Non-Repudiation do not fit well within the three core concepts, and as regulation of computer systems has increased (particularly amongst the Western nations) Legality is becoming a key consideration for practical security installations.

In 1992 and revised in 2002 the OECD's Guidelines for the Security of Information Systems and Networks proposed the nine generally accepted principles: Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design and Implementation, Security Management, and Reassessment. Building upon those, in 2004 the NIST's Engineering Principles for Information Technology Security proposed 33 principles. From each of these derived guidelines and practices.

In 2002, Donn Parker proposed an alternative model for the classic CIA triad that he called the six atomic elements of information. The elements are confidentiality, possession, integrity, authenticity, availability, and utility. The merits of the Parkerian hexad are a subject of debate amongst security professionals.

In 2013, based on the extensive literature analysis, the Information Assurance & Security (IAS) Octave has been developed and proposed as an extension of the CIA-triad. The IAS Octave is one of four dimensions of a Reference Model of Information Assurance & Security (RMIAS). The IAS Octave includes confidentiality, integrity, availability, privacy, authenticity & trustworthiness, non-repudiation, accountability and auditability. The IAS Octave as a set of currently relevant security goals has been evaluated via a series of interviews with InfoSec and IA professionals and academics. In, definitions for every member of the IAS Octave are outlined along with the applicability of every security goal (key factor) to six components of an Information System.

Confidentiality

Confidentiality refers to preventing the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

Confidentiality is necessary for maintaining the privacy of the people whose personal information is held in the system.

Integrity

In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of consistency as understood in the classic ACID model of transaction processing. Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system essentially forcing it to shut down.

Authenticity

In computing, e-Business, and information security, it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be. Some information security systems incorporate authentication features such as "digital signatures", which give evidence that the message data is genuine and was sent by someone possessing the proper signing key.

Non-repudiation

In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

It is important to note that while technology such as cryptographic systems can assist in non-repudiation efforts, the concept is at its core a legal concept transcending the realm of technology. It is not, for instance, sufficient to show that the message matches a digital signature signed with the sender's private key, and thus only the sender could have sent the message and nobody else could have altered it in transit. The alleged sender could in return demonstrate that the digital signature algorithm is vulnerable or flawed, or allege or prove that his signing key has been compromised. The fault for these violations may or may not lie with the sender himself, and such assertions may or may not relieve the sender of liability, but the assertion would invalidate the claim that the signature necessarily proves authenticity and integrity and thus prevents repudiation.

Information security analysts

Information security analysts are information technology (IT) specialists who are accountable for safeguarding all data and communications that are stored and shared in network systems. In the financial industry, for example, information security analysts might continually upgrade firewalls that prohibit superfluous access to sensitive business data and might perform defencelessness tests to assess the effectiveness of security measures.

Electronic commerce uses technology such as digital signatures and public key encryption to establish authenticity and non-repudiation.

3. *Answer the following questions:*

1) What does the CIA triad mean?
2) Why is legality becoming a key consideration for practical security installations?
3) What principles did the OECD’s Guidelines for Security of Information Systems and Networks propose?
4) What is confidentiality? Are there ways to enforce it?
5) What does integrity mean in information security?
6) When must the information be available in any information system?
7) What do high availability systems aim to?
8) What is necessary and important for authenticity?
9) What does non-repudiation imply?
10) What technology does electronic commerce use?

4. *Read the following statements. Are they true or false?*

1) There is no debate about extending the CIA triad. Other principles have never been proposed for addition.

2) Donn Parker proposed an alternative model for the classic CIA triad in 2002. He called eight atomic elements of information.

3) Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. Breach of confidentiality takes only one form.

4) Information security systems typically provide message integrity in addition to data confidentiality.

5) Electronic commerce uses secret key encryption to establish authenticity and non-repudiation.

5. *Summarize the text.*

UNIT 4
RISK MANAGEMENT

1. *Read the following terms and word combinations and learn them:*

Risk management - управление рисками

Vulnerability - уязвимость

Threat - угроза

Countermeasure - контрмера

To reduce risk - уменьшить риск

Value of information resource - ценность информационного ресурса

Ongoing, iterative process - непрерывный, повторяющийся процесс

Business environment - бизнес среда

To emerge - появляться, возникать

Productivity - производительность

Cost effectiveness - экономическая эффективность

Information asset - информационный актив

Breakdown - отказ, поломка

Side-effect - побочный эффект

Loss of an asset - потеря актива

To inflict harm - нанести вред

Impact - воздействие

To identify risk - распознать риск

To eliminate risk - устранить риск

Residual risk - остаточный риск

Risk assessment - оценка риска

Qualitative analysis - качественный анализ

Quantitative analysis - количественный анализ

To evaluate - оценить

Risk evaluation - оценка риска

To accept the risk - принять риск

To mitigate the risk - уменьшить риск

To transfer the risk - передать риск

To deny the risk - отвергать риск

2. *Read and translate the following text:*

The Certified Information Systems Auditor (CISA) Review Manual 2006 provides the following definition of risk management: "Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization."

There are two things in this definition that may need some clarification. First, the process of risk management is an ongoing, iterative process. It must be repeated indefinitely. The business environment is constantly changing and new threats and vulnerabilities emerge every day. Second, the choice of countermeasures (controls) used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected.

Risk analysis and risk evaluation processes have their limitations since, when security incidents occur, they emerge in a context, and their rarity and even their uniqueness give rise to unpredictable threats. The analysis of these phenomena which are characterized by breakdowns, surprises and side-effects, requires a theoretical approach which is able to examine and interpret subjectively the detail of each incident.

Risk is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset). A vulnerability is a weakness that could be used to endanger or cause harm to an informational asset. A threat is anything (manmade or act of nature) that has the potential to cause harm.

The likelihood that a threat will use a vulnerability to cause harm creates a risk. When a threat does use a vulnerability to inflict harm, it has an impact. In the context of information security, the impact is a loss of availability, integrity, and confidentiality, and possibly other losses (lost income, loss of life, loss of real property). It should be pointed out that it is not possible to identify all risks, nor is it possible to eliminate all risk. The remaining risk is called "residual risk".

A risk assessment is carried out by a team of people who have knowledge of specific areas of the business. Membership of the team may vary over time as different parts of the business are assessed. The assessment may use a subjective qualitative analysis based on informed opinion, or where reliable dollar figures and historical information is available, the analysis may use quantitative analysis.

The research has shown that the most vulnerable point in most information systems is the human user, operator, designer, or other human. The ISO/IEC 27002:2005 Code of practice for information security management recommends the following be examined during a risk assessment:

security policy,
organization of information security,
asset management,
human resources security,
physical and environmental security,
communications and operations management,
access control,
information systems acquisition, development and maintenance,
information security incident management,
business continuity management, and
regulatory compliance.

In broad terms, the risk management process consists of:

1. Identification of assets and estimating their value. Include: people, buildings, hardware, software, data (electronic, print, other), supplies.

2. Conduct a threat assessment. Include: Acts of nature, acts of war, accidents, malicious acts originating from inside or outside the organization.

3. Conduct a vulnerability assessment, and for each vulnerability, calculate the probability that it will be exploited. Evaluate policies, procedures, standards, training, physical security, quality control, technical security.

4. Calculate the impact that each threat would have on each asset. Use qualitative analysis or quantitative analysis.

5. Identify, select and implement appropriate controls. Provide a proportional response. Consider productivity, cost effectiveness, and value of the asset.

6. Evaluate the effectiveness of the control measures. Ensure the controls provide the required cost effective protection without discernible loss of productivity.

For any given risk, management can choose to accept the risk based upon the relative low value of the asset, the relative low frequency of occurrence, and the relative low impact on the business. Or, leadership may choose to mitigate the risk by selecting and implementing appropriate control measures to reduce the risk. In some cases, the risk can be transferred to another business by buying insurance or outsourcing to another business. The reality of some risks may be disputed. In such cases leadership may choose to deny the risk.

3. *Answer the following questions:*

1) What is the definition of risk management?
2) What sort of a process is the process of risk management? Why?

3) How does the business environment change?
4) What requirements must countermeasures meet?
5) What is risk? What is a vulnerability? What is a threat?
6) Is it possible to identify and eliminate all risks?
7) Who is a risk assessment carried out by?
8) What sort of analysis may be used for a risk assessment?
9) What is the most vulnerable point in most information systems?
10) What does the risk management process consist of?
11) What can Executive Management choose for any given risk?

4. *Read the following statements. Are they true or false?*

1) The process of risk management must be repeated indefinitely.
2) The likelihood that a threat will use a vulnerability to cause harm doesn’t create a risk.
3) It is possible to identify all risks, but it is impossible to eliminate all of them.
4) The most vulnerable point in any information system is its software.
5) For any given risk, Executive Management can choose different policy (to accept the risk, to mitigate the risk, to transfer the risk, to deny the risk).

5. *Summarize the text.*

UNIT 5
CONTROLS

1. *Read the following terms and word combinations and learn them:*

To implement control - осуществлять контроль
Administrative control - административный контроль
Logical control - логический контроль
Intrusion detection system - система определения вторжения
Access control - контроль доступа
Data encryption - шифрование данных
To overlook - упустить из виду
Principle of least privilege - принцип наименьших привилегий
To log - регистрировать(ся)
Physical control - физический контроль
Computing facilities - вычислительные средства
Separation of duties - разделение обязанностей
To authorize - разрешать
Acceptable level - приемлемый уровень
Risk assessment - оценка рисков
Violation - нарушение

2. *Read and translate the following text:*

Selecting proper controls and implementing those will initially help an organization to bring down risk to acceptable levels. Control selection should follow and should be based on the risk assessment. Controls can vary in nature but fundamentally they are ways of protecting the confidentiality, integrity or availability of information. ISO/IEC 27001:2005 has defined 133 controls in different areas, but this is not exhaustive. You can implement additional controls according to requirement of the organization. ISO 27001:2013(Still it's in drafted version) has cut down the number of controls to 113.

Administrative:

Administrative controls (also called procedural controls) consist of approved written policies, procedures, standards and guidelines. Administrative controls form the framework for running the business and managing people. They inform people on how the business is to be run and how day to day operations are to be conducted. Laws and regulations created by government bodies are also a type of administrative control because they inform the business. Some industry sectors have policies, procedures, standards and guidelines that must be followed – the Payment Card Industry (PCI) Data Security Standard required by Visa and MasterCard is such an example. Other examples of administrative controls include the corporate security policy, password policy, hiring policies, and disciplinary policies.

Administrative controls form the basis for the selection and implementation of logical and physical controls. Logical and physical controls are manifestations of administrative controls. Administrative controls are of paramount importance.

Logical:

Logical controls (also called technical controls) use software and data to monitor and control access to information and computing systems. For example: passwords, network and host-based firewalls, network intrusion detection systems, access control lists, and data encryption are logical controls.

An important logical control that is frequently overlooked is the principle of least privilege. The principle of least privilege requires that an individual, program or system process is not granted any more access privileges than are necessary to perform the task. A blatant example of the failure to adhere to the principle of least privilege is logging into Windows as user Administrator to read Email and surf the Web. Violations of this principle can also occur when an individual collects additional access privileges over time. This happens when employees' job duties change, or they are promoted to a new position, or they transfer to another department. The access privileges required by their new duties are frequently added onto their already existing access privileges which may no longer be necessary or appropriate.

Physical:

Physical controls monitor and control the environment of the work place and computing facilities. They also monitor and control access to and from such facilities. For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc. Separating the network and workplace into functional areas are also physical controls.

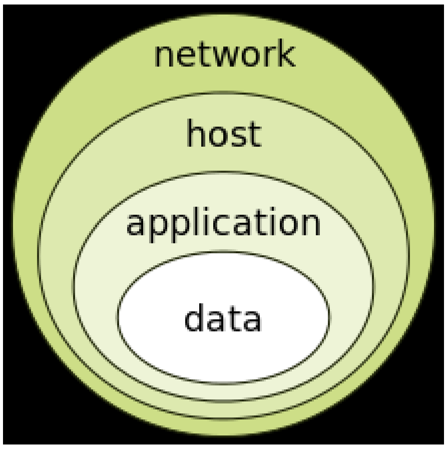
An important physical control that is frequently overlooked is the separation of duties. Separation of duties ensures that an individual can not complete a critical task by himself. For example: an employee who submits a request for reimbursement should not also be able to authorize payment or print the check. An applications programmer should not also be the server administrator or the database administrator – these roles and responsibilities must be separated from one another.

Defense in depth

Information security must protect information throughout the life span of the information, from the initial creation of the information on through to the final disposal of the information. The information must be protected while in motion and while at rest. During its lifetime, information may pass through many different information processing systems and through many different parts of information processing systems. There are many different ways the information and information systems can be threatened. To fully protect the information during its lifetime, each component of the information processing system must have its own protection mechanisms. The building up, layering on and overlapping of security measures is called defense in depth. The strength of any system is no greater than its weakest link. Using a defense in depth strategy, should one defensive measure fail there are other defensive measures in place that continue to provide protection.

Recall the earlier discussion about administrative controls, logical controls, and physical controls. The three types of controls can be used to form the basis upon which to build a defense-in-depth strategy. With this approach, defense-in-depth can be conceptualized as three distinct layers or planes laid one on top of the other. Additional insight into defense-in- depth can be gained by thinking of it as forming the layers of an onion, with data at the core of the onion, people the next outer layer of the onion, and network security, host-based security and application security forming the outermost layers of the onion. Both perspectives are equally valid and each provides valuable insight into the implementation of a good defense-in-depth strategy.

The onion model of defense in depth:



3. *Answer the following questions:*

1) What does the Management do when they choose to mitigate a risk?
2) What do administrative controls consist of?
3) What do administrative controls form?
4) What do logical controls use software and data for?
5) Which principle is frequently overlooked?
6) How does the principle of least privilege work?
7) When and why do violations of the principle of least privilege occur?
8) What do physical controls monitor and control?
9) Why is separation of duties very important?
10) Can administrative, logical and physical controls be used separately?

4. *Read the following statements. Are they true or false?*

1) Administrative controls inform people on how the business is to be run and day to day operations are to be conducted.
2) Laws and regulations created by government bodies are not a type of administrative control.
3) Logical and physical controls are not manifestations of administrative control.
4) Logical controls use software and data to monitor and control access to information and computing systems.
5) Separation of duties is an important part of physical control.

5. *Summarize the text.*

UNIT 6
SECURITY CLASSIFICATION FOR INFORMATION

1. *Read the following terms and word combinations and learn them:*

Value of information - ценность информации
Protection requirements - требования защиты
To assign a security classification - присвоить классификацию безопасности
Classification policy - политика классификации
Classification label- классификационная метка, знак
Public (information) - для всеобщего пользования, общедоступная (информация)
Sensitive (information) - деликатная, конфиденциальная (информация)
Private (information) - частная, личная (информация)
Restricted (information) - для ограниченного пользования (информация)
Information asset - информационный актив

2. *Read and translate the following text:*

An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information. Not all information is equal and so not all information requires the same degree of protection. This requires information to be assigned a security classification.

The first step in information classification is to identify a member of senior management as the owner of the particular information to be classified. Next, develop a classification policy. The policy should describe the different classification labels, define the criteria for information to be assigned a particular label, and list the required security controls for each classification.

Some factors that influence which classification information should be assigned include how much value that information has to the organization, how old the information is and whether or not the information has become obsolete. Laws and other regulatory requirements are also important considerations when classifying information.

The Business Model for Information Security enables security professionals to examine security from systems perspective, creating an environment where security can be managed holistically, allowing actual risks to be addressed.

The type of information security classification labels selected and used will depend on the nature of the organization, with examples being:

In the business sector, labels such as: Public, Sensitive, Private, Confidential.

In the government sector, labels such as: Unclassified, Sensitive But Unclassified, Restricted, Confidential, Secret, Top Secret and their non-English equivalents.

In cross-sectoral formations, the Traffic Light Protocol, which consists of: White, Green, Amber, and Red.

All employees in the organization, as well as business partners, must be trained on the classification schema and understand the required security controls and handling procedures for each classification. The classification of a particular information asset that has been assigned should be reviewed periodically to ensure the classification is still appropriate for the information and to ensure the security controls required by the classification are in place.

3. *Answer the following questions:*

1) What is an important aspect of information security and risk management?
2) Does all information require the same degree of protection?
3) What is the first step in information classification?
4) What should the classification policy describe and define?
5) What factors influence which classification information should be assigned?
6) Why should the classification of a particular information asset be reviewed periodically?

4. *Read the following statements. Are they true or false?*

1) All information which must be protected is equal.
2) There are some steps in information classification.
3) Laws and other regulatory requirements are not important considerations when classifying information.
4) All security classification labels are of the same type.

5. *Summarize the text.*

UNIT 7
ACCESS CONTROL

1. *Read the following terms and word combinations and learn them:*

Access control - контроль доступа
Identification - идентификация
To grant access - разрешить доступ
To verify - верифицировать (проверить, подтвердить)
Authentication - аутентификация (подтверждение подлинности)
Authorization- авторизация (разрешение)
To be authorized - иметь право доступа (к информации)
Discretionary approach-дискреционный подход (предоставляемый по усмотрению лица, имеющего соответствующие полномочия)
Non-discretionary approach - недискреционный подход
Need-to-know principle - принцип необходимости знания информации (получения доступа к информации)
Clearance - допуск к секретной информации

2. *Read and translate the following text:*

Access to protected information must be restricted to people who are authorized to access the information. The computer programs, and in many cases the computers that process the information, must also be authorized. This requires that mechanisms be in place to control the access to protected information. The sophistication of the access control mechanisms should be in parity with the value of the information being protected – the more sensitive or valuable the information the stronger the control mechanisms need to be. The foundation on which access control mechanisms are built starts with identification and authentication.

Access control is generally considered in three steps: Identification, Authentication, and Authorization.

Identification

Identification is an assertion of who someone is or what something is. If a person makes the statement "Hello, my name is John Doe" they are making a claim of who they are. However, their claim may or may not be true. Before John Doe can be granted access to protected information it will be necessary to verify that the person claiming to be John Doe really is John Doe. Typically the claim is in the form of a username. By entering that username you are claiming "I am the person the username belongs to".

Authentication

Authentication is the act of verifying a claim of identity. When John Doe goes into a bank to make a withdrawal, he tells the bank teller he is John Doe—a claim of identity. The bank teller asks to see a photo ID, so he hands the teller his driver's license. The bank teller checks the license to make sure it has John Doe printed on it and compares the photograph on the license against the person claiming to be John Doe. If the photo and name match the person, then the teller has authenticated that John Doe is who he claimed to be. Similarly by entering the correct password, the user is providing evidence that they are the person they username belongs to.

There are three different types of information that can be used for authentication:

Something you know: things such as a PIN, a password, or your mother's maiden name.

Something you have: a driver's license or a magnetic swipe card.

Something you are: biometrics, including palm prints, fingerprints, voice prints and retina (eye) scans.

Strong authentication requires providing more than one type of authentication information (two-factor authentication). The username is the most common form of identification on computer systems today and the password is the most common form of authentication. Usernames and passwords have served their purpose but in our modern world they are no longer adequate.[citation needed] Usernames and passwords are slowly being replaced with more sophisticated authentication mechanisms.

Authorization

After a person, program or computer has successfully been identified and authenticated then it must be determined what informational resources they are permitted to access and what actions they will be allowed to perform (run, view, create, delete, or change). This is called authorization. Authorization to access information and other computing services begins with administrative policies and procedures. The policies prescribe what information and computing services can be accessed, by whom, and under what conditions. The access control mechanisms are then configured to enforce these policies. Different computing systems are equipped with different kinds of access control mechanisms—some may even offer a choice of different access control mechanisms. The access control mechanism a system offers will be based upon one of three approaches to access control or it may be derived from a combination of the three approaches.

The non-discretionary approach consolidates all access control under a centralized administration. The access to information and other resources is usually based on the individuals function (role) in the organization or the tasks the individual must perform. The discretionary approach gives the creator or owner of the information resource the ability to control access to those resources. In the Mandatory access control approach, access is granted or denied basing upon the security classification assigned to the information resource.

Examples of common access control mechanisms in use today include role-based access control available in many advanced database management systems—simple file permissions provided in the UNIX and Windows operating systems, Group Policy Objects provided in Windows network systems, Kerberos, RADIUS, TACACS, and the simple access lists used in many firewalls and routers.

To be effective, policies and other security controls must be enforceable and upheld. Effective policies ensure that people are held accountable for their actions. All failed and successful authentication attempts must be logged, and all access to information must leave some type of audit trail. Also, need-to-know principle needs to be in affect when talking about access control. Need-to-know principle gives access rights to a person to perform their job functions. This principle is used in the government, when dealing with difference clearances. Even though two employees in different departments have a top-secret clearance, they must have a need-to-know in order for information to be exchanged. Within the need-to-know principle, network administrators grant the employee least amount privileges to prevent employees access and doing more than what they are supposed to. Need-to-know helps to enforce the confidentiality-integrity-availability (C ‑ I ‑ A) triad. Need-to-know directly impacts the confidential area of the triad.

3. *Answer the following questions:*

1) Who and what must access to protected information be restricted to?
2) What should access control mechanisms be in parity with?

3) What foundations are access control mechanisms built on?
4) What is identification?
5) What is authentication?
6) How many types of information can be used for authentication? What are they?
7) Why are usernames and passwords (as the most common forms of identification and authentication) slowly being replaced with more sophisticated mechanisms?
8) What is authorization?
9) What is need-to-know principle?
10) What does need-to-know principle help to enforce?

4. *Read the following statements. Are they true or false?*

1) Access to protected information must be restricted.
2) Only identification is the foundation for access control mechanisms.
3) One type of information can be used for strong authentication.
4) Usernames and passwords as the most common forms of identification and authentication are still adequate in our modern world.
5) Different computing systems are equipped with different kinds of access control mechanisms.

5. *Summarize the text.*

UNIT 8
CRYPTOGRAPHY

1. *Read the following terms and word combinations and learn them:*

Cryptography - криптография, шифрование
Encryption - шифрование
Decryption - дешифрование
Message digest - краткая, сжатая форма сообщения
Digital signature - цифровая подпись
Non-repudiation - неотказуемость
Public key - открытый ключ

2. *Read and translate the following text:*

Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. Information that has been encrypted (rendered unusable) can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption. Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit (either electronically or physically) and while information is in storage.

Cryptography provides information security with other useful applications as well including improved authentication methods, message digests, digital signatures, non-repudiation, and encrypted network communications. Older less secure applications such as telnet and ftp are slowly being replaced with more secure applications such as ssh that use encrypted network communications. Wireless communications can be encrypted using protocols such as WPA/WPA2 or the older (and less secure) WEP. Wired communications (such as ITU‑T G.hn) are secured using AES for encryption and X.1035 for authentication and key exchange. Software applications such as GnuPG or PGP can be used to encrypt data files and Email.

Cryptography can introduce security problems when it is not implemented correctly. Cryptographic solutions need to be implemented using industry accepted solutions that have undergone rigorous peer review by independent experts in cryptography. The length and strength of the encryption key is also an important consideration. A key that is weak or too short will produce weak encryption. The keys used for encryption and decryption must be protected with the same degree of rigor as any other confidential information. They must be protected from unauthorized disclosure and destruction and they must be available when needed. Public key infrastructure (PKI) solutions address many of the problems that surround key management.

3. *Answer the following questions*:

1) What does information security use cryptography for?
2) How is this process called?
3) Who can transform the encrypted information into its original usable form?
4) How is this process called?
5) What does cryptography protect information from?
6) What else does cryptography provide information security with?
7) When can cryptography introduce security problems?
8) In what case will an encryption key produce weak encryption?
9) How must the keys used for encryption and decryption be protected?
10) What must they be protected from?

4. *Read the following statements. Are they true or false?*

1) Information that has been encrypted can be transformed back into its original usable form by any person.
2) Cryptography is used in information security to protect information from unauthorized or accidental disclosure only while the information is in transit.
3) Cryptography provides information security with other useful applications.

4) Cryptography can’t introduce security problems.
5) The length and strength of the encryption key is a very important factor.

5. *Summarize the text.*

INFORMATION SECURITY CULTURE

Employee’s behavior has a big impact to information security in organizations. Cultural concept can help different segments of the organization to concern about the information security within the organization.″Exploring the Relationship between Organizational Culture and Information Security Culture″ provides the following definition of information security culture: ″ISC is the totality of patterns of behavior in an organization that contribute to the protection of information of all kinds.″

Information security culture needs to be improved continuously. In ″Information Security Culture from Analysis to Change″, authors commented, ″It′s a never ending process, a cycle of evaluation and change or maintenance.″ To manage the information security culture, five steps should be taken: Pre-evaluation, strategic planning, operative planning, implementation, and post-evaluation.

Pre-Evaluation : to identify the awareness of information security within employees and to analysis current security policy.

Strategic Planning: to come up a better awareness-program, we need to set clear targets. Clustering people is helpful to achieve it.

Operative Planning: we can set a good security culture based on internal communication, management-buy-in, and security awareness and training program.

Implementation: four stages should be used to implement the information security culture. They are commitment of the management, communication with organizational members, courses for all organizational members, and commitment of the employees.

CONCLUSION

Information security is the ongoing process of exercising due care and due diligence to protect information, and information systems, from unauthorized access, use, disclosure, destruction, modification, or disruption or distribution. The never ending process of information security involves ongoing training, assessment, protection, monitoring & detection, incident response & repair, documentation, and review. This makes information security an indispensable part of all the business operations across different domains.