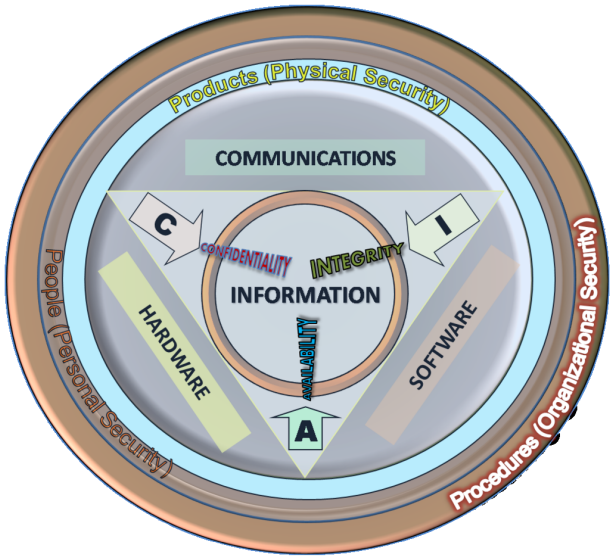
Information security

Information security, sometimes shortened to **InfoSec**, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc...)[1]



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.

Two major aspects of information security are:

- **IT security**: Sometimes referred to as computer security, Information Technology Security is information security applied to technology (most often some form of computer system). 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**: 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, such a breach of security could lead to exploited data and/or information, exploited staff/personnel, fraud, theft, and information leaks. Also, irreparable data loss and system instability can result from malicious access to confidential data and systems.[*clarify*] 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.

This article presents a general overview of information security and its core concepts.

History

Since the early days of writing, politicians, 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 ca. 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 organisations 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.During WWII, Alan Turing served in the cryptanalytic headquarters at the Government Code and Cypher School at Bletchley Park, Buckinghamshire, where he was largely responsible for breaking the German Enigma military codes. In the United Kingdom this led to the creation of the Government Codes and Cypher 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 a network generically called 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.

Basic principles

Key concepts

The CIA triad (confidentiality, integrity and availability) is one of the core principles of information security.[2]

There is continuous debate about extending this classic trio. [*citation needed*] Other principles such as Accountability[3] 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. [*citation needed*]

In 1992 and revised in 2002 the OECD's Guidelines for the Security of Information Systems and Networks[4] 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[5] 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. [*citation needed*]

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 a system holds.

Integrity

In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle.[6] 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.

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.

Risk management

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."[7]

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.[8]

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[9] 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.[10] The reality of some risks may be disputed. In such cases leadership may choose to **deny the risk**.

Controls

When management chooses to mitigate a risk, they will do so by implementing one or more of three different types of controls.

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.

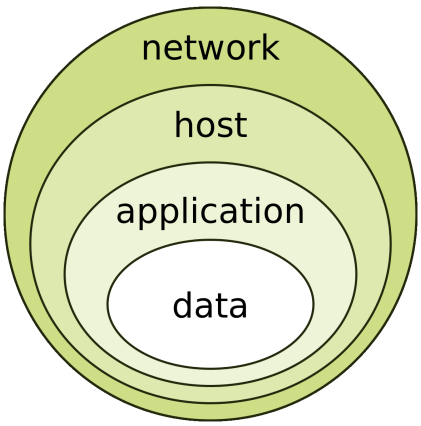
An important logical control that is frequently overlooked is the **principle of least privilege**. The principle of least privilege requires that an individual, program or system process is not granted any more access privileges than are necessary to perform the task. A blatant example of the failure 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.[11]

Defense in depth



The onion model of 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.

Security classification for information

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.

Access control

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 start with identification and authentication.

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.

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.

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.

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.[*citation needed*]

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 confidential-integrity-availability (C-I-A) triad. Need-to-know directly impacts the confidential area of the triad.

Cryptography

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.

Process

The terms **reasonable and prudent person**, **due care** and **due diligence** have been used in the fields of Finance, Securities, and Law for many years. In recent years these terms have found their way into the fields of computing and information security. U.S.A. Federal Sentencing Guidelines now make it possible to hold corporate officers liable for failing to exercise due care and due diligence in the management of their information systems.

In the business world, stockholders, customers, business partners and governments have the expectation that corporate officers will run the business in accordance with accepted business practices and in compliance with laws and other regulatory requirements. This is often described as the "reasonable and prudent person" rule. A prudent person takes due care to ensure that everything necessary is done to operate the business by sound business principles and in a legal ethical manner. A prudent person is also diligent (mindful, attentive, and ongoing) in their due care of the business.

In the field of Information Security, Harris[12] offers the following definitions of **due care** and **due diligence**:

> *"Due care are steps that are taken to show that a company has taken responsibility for the activities that take place within the corporation and has taken the necessary steps to help protect the company, its resources, and employees."* And, [Due diligence are the] *"continual activities that make sure the protection mechanisms are continually maintained and operational."*

Attention should be made to two important points in these definitions. First, in due care, steps are taken to ***show*** - this means that the steps can be verified, measured, or even produce tangible artifacts. Second, in due diligence, there are **continual activities** - this means that people are actually doing things to monitor and maintain the protection mechanisms, and these activities are ongoing.

Security governance

The Software Engineering Institute at Carnegie Mellon University, in a publication titled "Governing for Enterprise Security (GES)", defines characteristics of effective security governance. These include:

- An enterprise-wide issue
- Leaders are accountable
- Viewed as a business requirement
- Risk-based
- Roles, responsibilities, and segregation of duties defined
- Addressed and enforced in policy
- Adequate resources committed
- Staff aware and trained
- A development life cycle requirement
- Planned, managed, measurable, and measured
- Reviewed and audited

Incident response plans

1 to 3 paragraphs (non technical) that discuss:

- Selecting team members
- Define roles, responsibilities and lines of authority
- Define a security incident
- Define a reportable incident
- Training
- Detection
- Classification
- Escalation
- Containment
- Eradication
- Documentation

Change management

Change management is a formal process for directing and controlling alterations to the information processing environment. This includes alterations to desktop computers, the network, servers and software. The objectives of change management are to reduce the risks posed by changes to the information processing environment and improve the stability and reliability of the processing environment as changes are made. It is not the objective of change management to prevent or hinder necessary changes from being implemented.

Any change to the information processing environment introduces an element of risk. Even apparently simple changes can have unexpected effects. One of Management's many responsibilities is the management of risk. Change management is a tool for managing the risks introduced by changes to the information processing environment. Part of the change management process ensures that changes are not implemented at inopportune times when they may disrupt critical business processes or interfere with other changes being implemented.

Not every change needs to be managed. Some kinds of changes are a part of the everyday routine of information processing and adhere to a predefined procedure, which reduces the overall level of risk to the processing environment. Creating a new user account or deploying a new desktop computer are examples of changes that do not generally require change management. However, relocating user file shares, or upgrading the Email server pose a much higher level of risk to the processing environment and are not a normal everyday activity. The critical first steps in change management are (a) defining change (and communicating that definition) and (b) defining the scope of the change system.

Change management is usually overseen by a Change Review Board composed of representatives from key business areas, security, networking, systems administrators, Database administration, applications development, desktop support and the help desk. The tasks of the Change Review Board can be facilitated with the use of automated work flow application. The responsibility of the Change Review Board is to ensure the organizations documented change management procedures are followed. The change management process is as follows:

- **Requested:** Anyone can request a change. The person making the change request may or may not be the same person that performs the analysis or implements the change. When a request for change is received, it may undergo a preliminary review to determine if the requested change is compatible with the organizations business model and practices, and to determine the amount of resources needed to implement the change.
- **Approved:** Management runs the business and controls the allocation of resources therefore, Management must approve requests for changes and assign a priority for every change. Management might choose to reject a change request if the change is not compatible with the business model, industry standards or best practices. Management might also choose to reject a change request if the change requires more resources than can be allocated for the

change.

- **Planned:** Planning a change involves discovering the scope and impact of the proposed change; analyzing the complexity of the change; allocation of resources and, developing, testing and documenting both implementation and backout plans. Need to define the criteria on which a decision to back out will be made.
- **Tested:** Every change must be tested in a safe test environment, which closely reflects the actual production environment, before the change is applied to the production environment. The backout plan must also be tested.
- **Scheduled:** Part of the change review board's responsibility is to assist in the scheduling of changes by reviewing the proposed implementation date for potential conflicts with other scheduled changes or critical business activities.
- **Communicated:** Once a change has been scheduled it must be communicated. The communication is to give others the opportunity to remind the change review board about other changes or critical business activities that might have been overlooked when scheduling the change. The communication also serves to make the Help Desk and users aware that a change is about to occur. Another responsibility of the change review board is to ensure that scheduled changes have been properly communicated to those who will be affected by the change or otherwise have an interest in the change.
- **Implemented:** At the appointed date and time, the changes must be implemented. Part of the planning process was to develop an implementation plan, testing plan and, a back out plan. If the implementation of the change should fail or, the post implementation testing fails or, other "drop dead" criteria have been met, the back out plan should be implemented.
- **Documented:** All changes must be documented. The documentation includes the initial request for change, its approval, the priority assigned to it, the implementation, testing and back out plans, the results of the change review board critique, the date/time the change was implemented, who implemented it, and whether the change was implemented successfully, failed or postponed.
- **Post change review:** The change review board should hold a post implementation review of changes. It is particularly important to review failed and backed out changes. The review board should try to understand the problems that were encountered, and look for areas for improvement.

Change management procedures that are simple to follow and easy to use can greatly reduce the overall risks created when changes are made to the information processing environment. Good change management procedures improve the overall quality and success of changes as they are implemented. This is accomplished through planning, peer review, documentation and communication.

ISO/IEC 20000, The Visible OPS Handbook: Implementing ITIL in 4 Practical and Auditable Steps[13] (Full book summary),[14] and Information Technology Infrastructure Library all provide valuable guidance on implementing an efficient and effective change management program information security.

Business continuity

Business continuity is the mechanism by which an organization continues to operate its critical business units, during planned or unplanned disruptions that affect normal business operations, by invoking planned and managed procedures.

Unlike what most people think business continuity is not necessarily an IT system or process, simply because it is about the business. Today disasters or disruptions to business are a reality. Whether the disaster is natural or man-made, it affects normal life and so business. So why is planning so important? Let us face reality that "all businesses recover", whether they planned for recovery or not, simply because business is about earning money for survival.

The planning is merely getting better prepared to face it, knowing fully well that the best plans may fail. Planning helps to reduce cost of recovery, operational overheads and most importantly sail through some smaller ones

effortlessly.

For businesses to create effective plans they need to focus upon the following key questions. Most of these are common knowledge, and anyone can do a BCP.

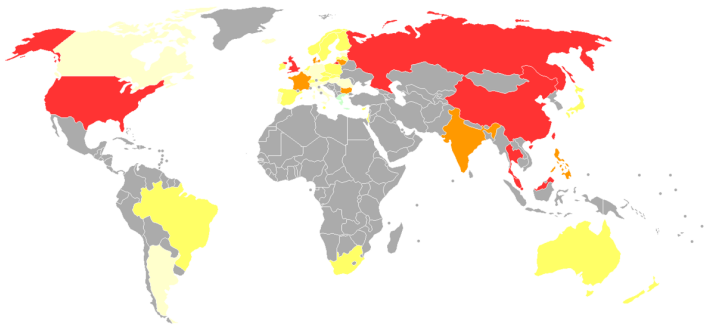
1. Should a disaster strike, what are the first few things that I should do? Should I call people to find if they are OK or call up the bank to figure out my money is safe? This is Emergency Response. Emergency Response services help take the first hit when the disaster strikes and if the disaster is serious enough the Emergency Response teams need to quickly get a Crisis Management team in place.
2. What parts of my business should I recover first? The one that brings me most money or the one where I spend the most, or the one that will ensure I shall be able to get sustained future growth? The identified sections are the critical business units. There is no magic bullet here, no one answer satisfies all. Businesses need to find answers that meet business requirements.
3. How soon should I target to recover my critical business units? In BCP technical jargon this is called Recovery Time Objective, or RTO. This objective will define what costs the business will need to spend to recover from a disruption. For example, it is cheaper to recover a business in 1 day than in 1 hour.
4. What all do I need to recover the business? IT, machinery, records...food, water, people...So many aspects to dwell upon. The cost factor becomes clearer now...Business leaders need to drive business continuity. Hold on. My IT manager spent $200000 last month and created a DRP (Disaster Recovery Plan), whatever happened to that? a DRP is about continuing an IT system, and is one of the sections of a comprehensive Business Continuity Plan. Look below for more on this.
5. And where do I recover my business from... Will the business center give me space to work, or would it be flooded by many people queuing up for the same reasons that I am.
6. But once I do recover from the disaster and work in reduced production capacity, since my main operational sites are unavailable, how long can this go on. How long can I do without my original sites, systems, people? this defines the amount of business resilience a business may have.
7. Now that I know how to recover my business. How do I make sure my plan works? Most BCP pundits would recommend testing the plan at least once a year, reviewing it for adequacy and rewriting or updating the plans either annually or when businesses change.

Disaster recovery planning

While a business continuity plan (BCP) takes a broad approach to dealing with organizational-wide effects of a disaster, a disaster recovery plan (DRP), which is a subset of the business continuity plan, is instead focused on taking the necessary steps to resume normal business operations as quickly as possible. A disaster recovery plan is executed immediately after the disaster occurs and details what steps are to be taken in order to recover critical information technology infrastructure.[15] Disaster recovery planning includes establishing a planning group, performing risk assessment, establishing priorities, developing recovery strategies, preparing inventories and documentation of the plan, developing verification criteria and procedure, and lastly implementing the plan.[16]

Laws and regulations

*Below is a **partial** listing of European, United Kingdom, Canadian and USA governmental laws and regulations that have, or will have, a significant effect on data processing and information security. Important industry sector regulations have also been included when they have a significant impact on information security.*



Privacy International 2007 privacy ranking
green: Protections and safeguards
red: Endemic surveillance societies

- UK Data Protection Act 1998 makes new provisions for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. The European Union Data Protection Directive (EUDPD) requires that all EU member must adopt national regulations to standardize the protection of data privacy for citizens throughout the EU.
- The Computer Misuse Act 1990 is an Act of the UK Parliament making computer crime (e.g. hacking) a criminal offence. The Act has become a model upon which several other countries including Canada and the Republic of Ireland have drawn inspiration when subsequently drafting their own information security laws.
- EU Data Retention laws requires Internet service providers and phone companies to keep data on every electronic message sent and phone call made for between six months and two years.
- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232 [17] g; 34 CFR Part 99) is a USA Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record.
- Federal Financial Institutions Examination Council's (FFIEC) security guidelines for auditors specifies requirements for online banking security.
- Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires the adoption of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. And, it requires health care providers, insurance providers and employers to safeguard the security and privacy of health data.
- Gramm-Leach-Bliley Act of 1999 (GLBA), also known as the Financial Services Modernization Act of 1999, protects the privacy and security of private financial information that financial institutions collect, hold, and process.
- Sarbanes–Oxley Act of 2002 (SOX). Section 404 of the act requires publicly traded companies to assess the effectiveness of their internal controls for financial reporting in annual reports they submit at the end of each fiscal year. Chief information officers are responsible for the security, accuracy and the reliability of the systems that manage and report the financial data. The act also requires publicly traded companies to engage independent auditors who must attest to, and report on, the validity of their assessments.
- Payment Card Industry Data Security Standard (PCI DSS) establishes comprehensive requirements for enhancing payment account data security. It was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

- State Security Breach Notification Laws (California and many others) require businesses, nonprofits, and state institutions to notify consumers when unencrypted "personal information" may have been compromised, lost, or stolen.
- Personal Information Protection and Electronics Document Act (PIPEDA) – An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act.

Sources of standards

International Organization for Standardization (ISO) is a consortium of national standards institutes from 157 countries, coordinated through a secretariat in Geneva, Switzerland. ISO is the world's largest developer of standards. ISO 15443: "Information technology - Security techniques - A framework for IT security assurance", ISO/IEC 27002: "Information technology - Security techniques - Code of practice for information security management", ISO-20000: "Information technology - Service management", and ISO/IEC27001: "Information technology - Security techniques - Information security management systems - Requirements" are of particular interest to information security professionals.

The USA National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Department of Commerce. The NIST Computer Security Division develops standards, metrics, tests and validation programs as well as publishes standards and guidelines to increase secure IT planning, implementation, management and operation. NIST is also the custodian of the USA Federal Information Processing Standard publications (FIPS).

The Internet Society is a professional membership society with more than 100 organization and over 20,000 individual members in over 180 countries. It provides leadership in addressing issues that confront the future of the Internet, and is the organization home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). The ISOC hosts the Requests for Comments (RFCs) which includes the Official Internet Protocol Standards and the RFC-2196 Site Security Handbook.

The Information Security Forum is a global nonprofit organization of several hundred leading organizations in financial services, manufacturing, telecommunications, consumer goods, government, and other areas. It undertakes research into information security practices and offers advice in its biannual Standard of Good Practice and more detailed advisories for members.

The IT Baseline Protection Catalogs, or IT-Grundschutz Catalogs, ("IT Baseline Protection Manual" before 2005) are a collection of documents from the German Federal Office for Security in Information Technology (FSI), useful for detecting and combating security-relevant weak points in the IT environment (IT cluster). The collection encompasses over 3000 pages with the introduction and catalogs.

At the European Telecommunications Standards Institute a catalog of Information security indicators have been standardized by the Industrial Specification Group (ISG) ISI.

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.

Scholars working in the field

- Ross J. Anderson
- Adam Back
- Stefan Brands
- Lance Cottrell
- Ian Goldberg
- Peter Gutmann
- Bruce Schneier
- Gene Spafford
- L Jean Camp
- Brian LaMacchia
- Nadia Heninger
- Anna Lysyanskaya
- Dawn Song
- Cynthia Dwork
- Annie Anton
- Lorrie Cranor
- Joan Feigenbaum
- Monica S. Lam
- Deborah Estrin

Further reading

- Anderson, K., "IT Security Professionals Must Evolve for Changing Market [18]", SC Magazine, October 12, 2006.
- Aceituno, V., "On Information Security Paradigms", ISSA Journal, September, 2005.
- Dhillon, G., "Principles of Information Systems Security: text and cases", John Wiley & Sons, 2007.
- Easttom, C., "Computer Security Fundamentals (2nd Edition)" Pearson Press, 2011.
- Lambo, T., "ISO/IEC 27001: The future of infosec certification", ISSA Journal, November, 2006.

Notes and references

[1] (b)(1)

[4] oecd.org (http://www.oecd.org/dataoecd/16/22/15582260.pdf)

[10] NIST SP 800-30 Risk Management Guide for Information Technology Systems (http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf)

[13] itpi.org (http://www.itpi.org/home/visibleops2.php)

[14] wikisummaries.org (http://wikisummaries.org/Visible_Ops)

[17] http://www.law.cornell.edu/uscode/20/1232.html

[18] http://www.scmagazineus.com/IT-security-professionals-must-evolve-for-changing-market/article/33990/

External links

- DoD IA Policy Chart (http://iac.dtic.mil/iatac/ia_policychart.html) on the DoD Information Assurance Technology Analysis Center web site.
- patterns & practices Security Engineering Explained (http://msdn2.microsoft.com/en-us/library/ms998382.aspx)
- Open Security Architecture- Controls and patterns to secure IT systems (http://www.opensecurityarchitecture.org/)
- An Introduction to Information Security (http://security.practitioner.com/introduction/)
- IWS - Information Security Chapter (http://www.iwar.org.uk/comsec/)
- Ross Anderson's book "Security Engineering" (http://www.cl.cam.ac.uk/~rja14/book.html)

Bibliography

- Allen, Julia H. (2001). *The CERT Guide to System and Network Security Practices*. Boston, MA: Addison-Wesley. ISBN 0-201-73723-X.
- Krutz, Ronald L.; Russell Dean Vines (2003). *The CISSP Prep Guide* (Gold Edition ed.). Indianapolis, IN: Wiley. ISBN 0-471-26802-X.
- Layton, Timothy P. (2007). *Information Security: Design, Implementation, Measurement, and Compliance*. Boca Raton, FL: Auerbach publications. ISBN 978-0-8493-7087-8.
- McNab, Chris (2004). *Network Security Assessment*. Sebastopol, CA: O'Reilly. ISBN 0-596-00611-X.
- Peltier, Thomas R. (2001). *Information Security Risk Analysis*. Boca Raton, FL: Auerbach publications. ISBN 0-8493-0880-1.
- Peltier, Thomas R. (2002). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. Boca Raton, FL: Auerbach publications. ISBN 0-8493-1137-3.
- White, Gregory (2003). *All-in-one Security+ Certification Exam Guide*. Emeryville, CA: McGraw-Hill/Osborne. ISBN 0-07-222633-1.
- Dhillon, Gurpreet (2007). *Principles of Information Systems Security: text and cases*. NY: John Wiley & Sons. ISBN 978-0-471-45056-6.

Article Sources and Contributors

Information security *Source*: https://en.wikipedia.org/w/index.php?oldid=565168408 *Contributors*: 111Alleskönner, 193.203.83.xxx, 2601:1:B480:B3:105C:A42C:AE39:9729, 2edsphere, Aapo Laitinen, Abductive, Abyss of enchantment, Aclyon, Addshore, Adhemar, Aitias, Ajuk, Aka042, Akjar13, AlMac, Alanpc1, Ale jrb, AlephGamma, Alexandru47, Alexconlin, Alexttcn, Ali, Alucard (Dr.), Amatriain, Amorymeltzer, Andrewman327, Andycjp, Aneah, Angela, Anotherderelict, Ant, Apau98, Aperks1811, Aron.j.j, Awillcox, BD2412, BKD-Banker$, Bburton, Bill.martin, Bobo192, Bobrayner, BooleanMaybe, Borgx, BrWriter2006, Breadtk, Brian the Editor, Brwriter2, Btyner, Bzwas, Calm reason, Canoruo, Cartermichael, Cascadeuse, Cdschuett, CelebritySecurity, Centrx, Cflm001, Chealer, Choibg, Chris Brown, Chris Ulbrich, Chris the speller, ChrisGualtieri, Chrisbrown, CliffC, Closedmouth, Colemannick, Colonies Chris, CommodiCast, CommonsDelinker, Conversion script, Corp Vision, Cpaidhrin, Cralar, Csrcyborg, Cupids wings, DARTH SIDIOUS 2, DRAGON BOOSTER, DVdm, Danakil, Dancter, DanielPharos, Davebailey, Dawnseeker2000, Dcressb, DeadEyeArrow, Dekimasu, Delmundo.averganzado, Derekcslater, Dkosutic, Docpd, Donalcampbell, DouglasCalvert, Dtruonggwhs, Edcolins, Eddy Scott, Edward, El C, Elieb001, Emergentchaos, Enviroboy, Epbr123, Esmond.pitt, Eumolpo, Evb-wiki, FTsafe, Falcon8765, Fancy steve, Favertama, Fcoulter, Feldermouse, Fellwalker57, Fredrik, Fryed-peach, Gaius Cornelius, Ged fi, Gfragkos, Giraffedata, Glavin, Gomm, Gpdhillon2, GraemeL, Graham87, Grantgw, GrayFullbuster, GroupOne, Grutness, HaeB, Haeinous, HansWDaniel, Happyrose, Hephaestos, Himugk, Hnguyen322, Hoo man, Hu12, Hutcher, INFOSECFORCE, Imjustmatthew, Infinitesteps, Inkling, Inthenet, Ionutzmovie, Iridescent, Irishguy, Ishikawa Minoru, Itai, Itsecpardis, Itusg15q4user, IvanLanin, JCLately, JaGa, Jarble, JaredPoeppelman, Jdlambert, Jim.henderson, Jmilgram, Jobin RV, John Vandenberg, John Yesberg, John of Reading, JohnManuel, JohnOwens, JonHarder, Joy, Jpluser, Jramio, Kbolino, Kernel.package, Khendon, Kieraf, Kilopi, Kimvais, KizzoGirl, Kl4m, Klemen Kocjancic, Kozmando, Kungming2, Kuru, LMB, Leszek Jańczuk, LiDaobing, Liko81, LilHelpa, Little saturn, Lmatt, Lotje, MBisanz, MER-C, MK8, Madvenu, Malmoe7, Manasprakash79, Mandarax, Martarius, Matt Crypto, Mattatpredictive, Mattg82, Mauls, Mcicogni, MeS2135, MerileeNC, Michael Hardy, Mike Rosoft, Mike0131, MikeLynch, Mild Bill Hiccup, Mindmatrix, Mistress Selina Kyle, Mitte, Ml-crest, Mldisch, Mlichter, Morpheus063, MosaicSecurity, MrOllie, Mss. Selina Kyle, Nageh, Nainawalli, Nikai, Nitinbhogan, Noah Salzman, NoticeBored, Nuno Tavares, Nuwewsco, Nyttend, OKAMi-InfoSec, Obiwankenobi, ObscurO, Ohka-, Ohnoitsjamie, Open4Ever, Param21, Pastore Italy, Patrick.bausemer, PatrickFlaherty, Piano non troppo, Pkleinr, Plastikspork, Pnevares, PolarYukon, Portal60, Postonm, Pramukh Arkalgud Ganeshamurthy, Pratyya Ghosh, Prokopenya Viktor, Prowriter16, Prunesqualer, Pspagnoletti, Ptomes, Public Menace, Puntarenus, Quantumseven, Raed abu farha, RainbowOfLight, Rakomwolvesbane, Ramfoss, Ranman45, RealityApologist, Rearden9, Reenaiit, Revmachine21, RexNL, Rgalexander, Rhobite, Rich Farmbrough, Richard Bartholomew, Richu jose, Riker2000, Rjwilmsi, Rlendog, Robwhitcher, Ronz, Rossj81, Rsrikanth05, Rursus, SDC, Sa ashok, Sam Hocevar, Saqib, SasiSasi, Satellizer, Saurav kashyap, Sbilly, Scaar123, Scapler, Scgilardi, Scottdimmick, Seaphoto, SebastianHelm, Sephiroth storm, Sfoak, Sfoskett, Shadowjams, Shawnse, Shebang42, Shonharris, Soliloquial, Sonakshi87, Spearhead, Sperling, Srandaman, Stationcall, SteinbDJ, Stephenb, Stevedaily, Stuartfost, Sun Creator, Suruena, Sutch, Sweerek, Tabletop, TarseeRota, Tenbergen, Tentinator, The Anome, The Thing That Should Not Be, The wub, Think outside the box, Thireus, Tqbf, Truestate, Tsarihan, Tuxisuau, TyA, Umbrussels, Uncle Dick, UncleBubba, UriBraun, V1ntage318, Vaceituno, Vdmerwe.johann, VernoWhitney, Vinodvmenon, Violetriga, WalterGR, Wbm1058, Whouk, WideClyde, Widr, Wiki-Ed, Wikibob, Wikipediatrix, Wilcho, William Avery, Wingfamily, Wmasterj, Woohookitty, Wrp103, Xinconnu, Xsmith, Yakheart, ZeWrestler, كامبدرج, 608 anonymous edits

Image Sources, Licenses and Contributors

File:CIAJMK1209.png *Source*: https://en.wikipedia.org/w/index.php?title=File:CIAJMK1209.png *License*: Creative Commons Attribution-Sharealike 3.0 *Contributors*: John M. Kennedy T.

File:Defense In Depth - Onion Model.svg *Source*: https://en.wikipedia.org/w/index.php?title=File:Defense_In_Depth_-_Onion_Model.svg *License*: Creative Commons Attribution-Sharealike 3.0 *Contributors*: User:Kbolino

File:Privacy International 2007 privacy ranking map.png *Source*: https://en.wikipedia.org/w/index.php?title=File:Privacy_International_2007_privacy_ranking_map.png *License*: Creative Commons Attribution-Sharealike 3.0,2.5,2.0,1.0 *Contributors*: Wüstling

License