Number 3 Year 1993

FSC **Newsletter**

The use of personal computer systems : A guide to secure system implementation

Organisations are investing in PCs because they substantially improve productivity at relatively low cost. More and more, PCs are used to provide the information storage and processing support needed for critical business applications.

In distributing processing facilities, organisations also distribute the responsibility for protecting one of their most valued assets - information. PCs increase the exposure to which these holdings of information are subjected.

- They are user-friendly, allowing users with very little computer knowledge to work with the organisation's information;
- They have fast processors that can process highly critical and sensitive information;
- They have a large information-holding capacity, both on-line and removable, which concentrates the organisation's information on physically small devices;
- They have communication links to other computers and their information;
- They distribute the organisation's automated information system processes;
- Decrease the organisation's centralised control over those processes.

PCs and other small systems have unique security requirements which must be understood if effective security measures are to be implemented. Although they perform essentially the same functions as large systems, they have some characteristics which present special security problems.

Organisations which rely on PCs need to become fully aware of the security issues such machines raise. They need to understand the special exposures to which the organisation's information assets are subject. They also need to understand the security methodologies and the specific safeguards which help prevent loss, and to learn how to implement the chosen safeguards.

To achieve this, organisations can develop and maintain a PC security programme. There are many similarities, equivalents and ties between personal computer and other security programmes.

A completely secure PC environment is virtually impossible to obtain. However, particular risks can be identified and analysed. Reasonable and realistic safeguards can be provided to reduce these risks to an acceptable level.

- **Organisation Vulnerabilities**

This area includes the organisational and managerial structure within which personnel work. It also includes the policies, standards and guidelines that they use to direct their efforts.

Several factors in the organisational area gives rise to vulnerabilities unique to PCs. PCs are distributed throughout the organisation. As a result there are few central systems management groups which oversee computer operations in their entirety. Typically, the computer support structure is informal and the few support specialists are based outside the organisation that uses the equipment.

These factors can create several PC security problems. First, because responsibility for overseeing PC implementation is distributed to the users few security policies, standards or procedures are developed. This often results in low levels of security and, potentially high levels of loss. Secondly, because computer support structures are not formalised, personnel may be insufficiently trained in the use of their computers. This often results in data entry errors and omissions, the primary cause of losses in an organisation. Thirdly, owing to the lack of PC specialists, users often configure and maintain their own hardware and software. System configuration mistakes usually go undetected. As a consequence, the integrity of the information being processed and stored may be reduced.

- **Administrative Vulnerabilities**

This area includes the day-to-day management activities and the record-keeping necessary to ensure the smooth running of an organisation.

There are four factors in the administrative area that may lead to specific security problems. First, users work in relative isolation from each other. Secondly, micro-computing processes receive less overall supervision than those in other computing environments. Thirdly, there is little independent verification of the information manipulation processes. Finally, the record keeping activities for assets are not always carried out.

Users working in isolation often become "key staff" because they are the only ones with the necessary knowledge of a critical business system, its applications and the related information. When these employees leave at short notice, their knowledge of the particular system is lost. The costs of training a replacement can be very high.

PC applications are unusually developed without the cross-checks used in other environments. This often results in computing processes that create undetected errors under certain circumstances. Combined with the lack of independent verification, the impact on the organisation can be significant.

Unless the organisation has well-established central facilities for keeping asset records, there are few staff to verify the inventory of assets, the distribution of access control devices and the classification of information assets. This results in low overall integrity of the PC management systems. This problem eventually leads to the misuse and abuse of computing resources.

- **Physical / Environmental Vulnerabilities**

The physical/environmental area prefers to the tangible surroundings within which PCs are located.

Office buildings are rarely constructed to take account of the specific environment required for using PCs. The architectural design, the building materials chosen, the positioning of electrical and mechanical devices and the implementation of a fire detector, sprinkler, heating and ventilation systems can lead to problems with PC processing.

In open office areas PCs are vulnerable to accidental and deliberate tampering, unauthorised access or damage. All the security aspects (integrity, confidentiality and availability) of the information are affected.

Often, the computers and their peripherals are in close proximity to workplace hazards, such as would not be allowed to threaten mainframe computing resources. Hazards that can contribute to various kinds of information and equipment loss include:

- fire hazards, such as flammable liquids and large stocks of paper;
- water hazards, such as sprinklers, overhead water pipes, leaking roofs and basements print to flooding, coffee and other beverages;
- high humidity, dust particles and smoke.

- **Operational Vulnerabilities**

The operational area includes the specific procedures used to operate and maintain the PCs.

Generally, the users of PCs follow fewer operating procedures and instructions than users of mini-computers and mainframes. This is often related to the lack of policy and standards described in the section above dealing with organisational vulnerabilities.

Confidentiality and availability of information can be affected by the lack of clearly defined protection standards. PCs without appropriate levels of safeguards could be used to process critical and sensitive information. The lack of adequate back-up and off-site storage for information can result in irrecoverable losses.

Where procedures have been centrally developed, the users' applications and system configurations are not always given proper consideration. Procedures developed without the participation of the users can be too difficult to perform. Special care must be taken in the area of logical access controls: should they be too difficult to perform the user may attempt to bypass them, creating a serious exposure and potential loss of information.

- **Contingency Vulnerabilities**

Contingency measures are those which are used to prepare for the orderly continuation of normal business operations when information losses occur or when machines become inoperable.

In the mainframe and mini-computer environments a centralised approach is used to develop business recovery plans and to recover from minor and major disaster. Each member of the recovery team understands his responsibility for maintaining the plan and his specialist role during the recovery.

In the PC environment, individual users have to fulfil all the specialised roles and have to perform all the procedures carried out by the traditional contingency team. They usually have little training in this area and do not use formalised approaches to contingency planning. For example, a user with a good contingency plan who notices a computer virus can take steps to save vital information before the virus can cause irreparable damage. A poor or non-existent contingency plan may result in losses for the organisation.

The large number of processors within any organisation results in a high probability that serious losses will occur. The lack of appropriate policies and procedures that could facilitate recovery often increases the degree of loss suffered by the organisation.

Developing A Personal Computer Security Programme

The problems described in the previous section are specific to the PC security environment. In addition to these, PC installations are also subject to the problems associated with mini-computers and mainframes. The total range of security issues can best be analysed and resolved on the basis of a PC security programme designed to meet the organisation's needs.

PC security is not an isolated process or problem. It forms part of an organisation's overall information security strategy, integrating both technical and non-technical protection measures.

A security programme focuses on the security of the information being processed rather than on the PC environment itself. Most important, it must also maintain a balance between too many security and computer user restrictions and not enough protection for the organisation's information and other computer-related assets.

The main elements of a programme are:

- building the programme foundations:-
  identify employees' responsibilities;
  develop strategies;
  develop policies;
  develop standards, guidelines and procedures;
  develop security awareness, and
  plan security programme implementation.
- developing a baseline protection standard;
- using risk management; and
- choosing safeguards.

• Building programme foundation

A PC security programme must evolve from a solid foundation. This foundation provides the reasons and the rationale for implementing various types of security safeguard. With this security programme the efforts requested from employees are easier to justify.

Employees' responsibilities

Responsibility for ensuring that an organisation's information and other assets remain confidential, integral and available rests with all the staff in an organisation. This is especially true for the security of assets within the PC environment.

The first phase in the development of a security programme foundation is to identify and assign security duties to individuals and groups of individuals.

Various groups share responsibility for developing and implementing various aspects of security. They are:

Senior managers' responsibilities

- management responsibilities for PC security are clearly defined and communication to the user managers;
- adequate and effective organisational and administrative arrangements are in place, enabling PC security requirements to be addressed in full;

- the requisite resources for effective PC security are provided;
- a general culture of "security awareness" is established and maintained;
- guidelines are developed which outline the use of different technology environments for different applications;
- PC security strategies, policies, standards, guidelines and procedures are developed.

User managers' responsibilities

- the PCs are used in accordance with the organisation's policies, standards, guidelines and procedures;
- risk assessments are performed for systems under their control;
- the information processed and stored in their user's PCs is adequately protected on the basis of safeguard baseline standards and risk assessments;
- their staff understand the organisation's PC policies, standards, guidelines and procedures,
- users understand the duties assigned to them.

Other managerial responsibilities

There are a number of other important responsibilities that need to be assigned to managers. The particular managers to whom these responsibilities are assigned will depend on the individual organisation's structure. The following are the responsibilities:

- Training/educating/advising
- supporting and training users in the proper use of PCs and related technology;
- providing advice on PC security standards, guidelines, and procedures;
- developing and maintaining a security manual;
- advising on secure applications and secure systems design;
- administering the security awareness programme.

Implementing

- Providing suitable security-related hardware and software tools;
- administering the implementation and maintenance of the critical security safeguards and control techniques, as determined by policy baseline standards and risk assessments;
- assigning each information type and asset to a classification category and determining where, how and by whom the asset may be used;
- maintaining an inventory of all software, hardware and information;
- developing contingency and disaster plans for critical functions, information and systems.

Reviewing/auditing/verifying

- Monitoring the distribution and use of PCs;
- reviewing changes in existing laws as they relate to security privacy, health and safety;
- monitoring techniques and procedures used to detect, report and investigate security breaches;
- performing periodic compliance tests to ensure adherence to policy;
- monitoring changes in information and other assets to detect classification change requirements;
- reviewing business controls described in functional specifications for each information processing system.

User Responsibilities

- Everyday security duties are the responsibility of the PC users.
- It is the responsibility of the user to ensure that:

- he or she understands the organisation's PC policies, standards, guidelines and procedures;
- the security tools and techniques as prescribed in the PC security guidelines and procedures are used diligently in the performance of the organisation's business to protect information and other assets;
- security problems, breaches, occurrences, and new vulnerabilities and exposures observed by the user are brought to the attention of user and security management.

Security Strategies

The second phase in the development of the security programme foundation is to create the PC security strategies. These describe the security goals and, in broad terms, the means by which these goals are to be accomplished. The focus of the strategies is the protection of information. They are developed in the light of the users' business objectives and their need for PCs, LANs and wide area networks (WANs) to support those objectives.

The security strategies are linked directly to the overall business strategies and office automation, telecommunications and electronic data interchange objectives of the organisation.

Security Policies

The third phase of foundation building concerns the development of the security policies once the strategies have been approved by senior management.

PC policies are basic in design, easy to implement and directly related to the problems encountered in the PC environment. They do not create a new supporting organisational structure.

The minimum policy aspects to be covered are:

- PC purchasing;
- PC hardware/software configuration management;
- taking hardware and software home;
- software copyright protection;
- malicious code (viruses, etc.) protection;
- software storage and backup;
- information storage and backup;
- access control for stand-alone computers and LANs;
- electro-magnetic emission (TEMPEST) protection;
- dial in and dial out access;
- encryption of information;
- message authentication;
- eating and drinking near PCs;
- network security administration, and
- PC Security breaches.

An organisation will also need to update the following general security policies to reflect the requirements of the PC environment:

- classification of information;
- handling of classified information;
- contingency planning;
- performing threat and risk assessments;
- contract administration - security aspects;
- personal accountability for information and other assets;

- security auditing;
- division of critical duties;
- compliance with relevant legislation, including data protection laws.

Security standards, guidelines and procedures

The fourth phase in building the security programme foundations consists in establishing the PC security standards, guidelines and procedures. The extent to which policy statements will be translated into standards, guidelines or procedures will depend on the particular circumstances prevailing in each organisation.

Security awareness

The success of a PC security programme depends on two factors: management taking overall responsibility for developing the strategies, policies and safeguards, and users taking responsibility for following them. An effective bridge to join the two is a well-designed security awareness programme. This is the fifth phase of foundation building.

There are many benefits to be gained from an awareness programme. An awareness programme can make security constraints more acceptable by educating users about the reasons for security. In addition, users can learn how to avoid common errors and omissions. This will reduce the overall exposure of the organisation to theft, lawsuits but rather a continuing activity.

Security planning

The sixth phase of programme foundation building involves the planning of the implementation of the security programme.

Security planning transposes the PC security strategies and policies into action. Typically, this function is not performed in isolation but is part of the overall co-ordinated efforts devoted by the organisation to physical security or information security planning.

- Security planning:
- identifies the personnel and other resource requirements;
- details the structured security processes, such as business contingency planning and disaster recovery planning;
- identifies the costing, priorities and schedules for implementing the safeguards;
- takes into account the need for security at all stages of systems development, including design.

- **Developing a baseline protection standard**

Once the programme foundations have been established, the development of the baseline protection standard can be initiated.

Understanding safeguards

Safeguards are the programmes, methods or devices which protect information and other assets from being adversely affected by threats.

They may be technical or non-technical in nature. For example, security training and security awareness are non-technical measures of protection. Locks, smart cards and disk write-protect tabs are examples of technical safeguards.

In order to be of value, safeguards must have one or more "safeguard objectives":

- prevention (including avoidance),
- deterrence,

- monitoring,
- detection, and
- recovery (including correction and restoration).

The safeguard must also fulfil one or more of the asset's requirements for:

- confidentiality,
- integrity, and
- availability.

Baseline protection standard

Every computer environment has a set of commonly used safeguards that meet commonly desired safeguard objectives. The justification for their existence is nothing more than "good business practice". Together, these safeguards form the organisation's baseline protection standard.

A baseline standard imposes the minimum amounts and types of protection required to bring the information and other assets up to the "baseline level". For example, computers need a clean, reliable source of power. A baseline safeguard, for most PCs is a computer "power bar" which has spike, voltage ripple and surge protection.

It is important to keep in mind that a baseline standard is not static. It requires frequent updating as technology changes and as the threats to the environment change. In addition, these standards are only standards in the particular environment for which they were created.

They will vary between environments and between organisations. To create a new baseline standard, an organisation can consult its experienced in-house staff, external security professionals, Government security organisations and other organisations which have similar PC environments.

- **Using risk management**

The third element of a PC security programme is the formation of a customised risk management process.

Risk management is a formalised, comprehensive process which identifies, analyses and reduces the threats to an organisation's assets and business functions. It is a security tool which assists management in minimising unacceptable loss and in maximising the return on investment of security resources. It can identify those safeguards outside the scope of the organisation's baseline standard.

There are many methodologies of risk assessment, risk analysis and risk reduction. The approach chosen will depend on many factors, including the staff's risk management experience, management's requirements for quantitative or qualitative results and the security of the PC environment. Once selected, it will need to be customised.

The following is a general introduction to the risk management process.

Phase 1 Risk assessment and risk analysis

- Identify the information being processed, the hardware and software and the business functions which could be at risk;
- identify the threats that could potentially cause loss of the assets;
- identify the vulnerabilities inherent in the PC environment which could allow a threat to result in a loss;
- identify the safeguards currently in place which are protecting the information and other assets;

- estimate the likelihood that the threat will occur;
- estimate the impact should the threat occur.

Phase 2 Risk reduction analysis

- Identify the potential safeguards which will reduce the previously identified areas of high risk;
- determine the economic, technical and operational feasibility of the potential safeguards;
- draw up in order of priority, a list of safeguards for each high-risk area with summaries of cost benefit and risk impact relationships.

Phase 3 Management review and decisions

- Select the option that best fits the organisation's climate, including avoiding risk, transferring risk, limiting risk and accepting risk;
- acknowledge the residual risk, i.e the risk which still exists after the safeguards have been implemented.

Phase 4 New or modified safeguard implementation

- Identify the safeguards to be implemented;
- identify the resources needed to implement the safeguards;
- identify the timetables, milestones and deadlines;
- identify how the safeguards are to be implemented;
- identify the maintenance requirements for the newly implemented safeguards.

Phase 5 Periodic review and audit

- Reassess the functioning and effectiveness of the safeguards on a periodic basis;
- repeat the process from Phase 1 whenever the environment undergoes major organisational, administrative or technological changes.

• Choosing safeguards

The fourth element of a PC security programme is the selection of appropriate safeguards.

Safeguards are determined in two ways: by using the organisation's baseline protection standards. These safeguards which offer this protection are then selected on the basis of the baseline protection standards. These minimum safeguards protect the organisation's assets against common vulnerabilities.

Secondly, a risk assessment of critical information, systems and other assets is carried out to identify assets that may still be exposed. If the risk of loss is deemed unacceptable, additional safeguards will be required. These safeguards are considered to be "above baseline", because they exceed the basic minimum protection requirements.

SOURCE: THIS NEWSLETTER IS DRAWN FROM A PAPER "MONOGRAPH ON PERSONNEL COMPUTER SECURITY" ISSUED BY THE WORKING PARTY ON SECURITY ISSUES OF THE GROUP OF COMPUTER EXPERTS OF THE CENTRAL BANKS OF THE GROUP OF TEN COUNTRIES, EXTRACTS OF WHICH HAVE BEEN REPRODUCED WITH THEIR KIND PERMISSION.

Financial Services Commission
Suite 943
Europort

April 1993