



Good Practice Note No. 18

Management of Information Security

Part of a series of notes to help Centers review their own internal management processes from the point of view of managing risks and promoting value for money, and to identify where improvement efforts could be focused. The good practices described in this series of notes should not be interpreted as minimum standards as not all may be applicable to every Center.

SUMMARY

Information security relates to the protection of valuable assets against loss, misuse, disclosure or damage.

This Good Practice Note (GPN), which focuses on the specific risk of information security, was developed to complement the earlier released overview GPN on Management of ICT risks. The note identifies four high-level security good practices that should be implemented by CGIAR Centers:

- Treat security management as a business issue
- Ensure management support for information security decisions
- Define roles and responsibilities for information security
- Implement an information security program

This note also sets out the main elements of an Information Security Program, based on the COBIT framework.

Finally, this note provides a summary of the main technical information security risks facing Centers at this time, broadly categorized as

- Computer misuse
- Violations of rules and regulations
- Accidents



Good Practice Note No. 3

Management of Information Security

INTRODUCTION

The growing dependence on information systems is widely accepted among the CGIAR Centers. Information systems can generate many direct and indirect benefits, and as many direct and indirect risks. These are increasingly being shared across the Centers and the current CGIAR-wide initiative on enterprise wide security – under the ICT-KM Enterprise Security and Business Continuity Project - seeks to identify and address in a coordinated and comprehensive fashion, the internal and external security exposures to the Center’s information systems and IT Infrastructure, both of individual Centers and of the System as a whole (i.e., including shared systems hosted at CGNET).

This Good Practice Note (GPN) complements the earlier released GPN on Management of ICT risks. This focuses on the specific risk of ICT security and provides:

- An introduction to information security – what does it mean and what does it cover
- The COBIT-based security baseline, providing key controls
- A summary of technical risks

This GPN is closely based on the COBIT Security Baseline and the Information Security Governance: Guidance for Boards of Directors and Executive Management, issued by the IT Governance Institute.

DEFINING INFORMATION SECURITY

Information security relates to the protection of valuable assets against loss, misuse, disclosure or damage. In this context, “valuable assets” are the information recorded on, processed by, stored in, shared by, transmitted or retrieved from an electronic medium. The information must be protected against harm from threats leading to different types of vulnerabilities such as loss, inaccessibility, alteration or wrongful disclosure. Threats include errors and omissions, fraud, accidents and intentional damage.

The objective of information security is “protecting the interests of those relying on information, and the systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality and integrity.” The security objective is met when:



- Information is available and usable when required, and the systems that provide it can appropriately resist attacks and recover from failures (availability)
- Information is observed by or disclosed to only those who have a right to know (confidentiality)
- Information is protected against unauthorized modification (integrity)
- Business transactions as well as information exchanges between enterprise locations or with partners can be trusted (authenticity and non-repudiation)

The relative priority and significance of availability, confidentiality, integrity and trust vary according to the value and type of information and the context in which the information is used.

The amount of protection required depends on how likely a security risk might occur, and how big an impact it would have if it did occur. Protection is achieved by a combination of technical and non-technical safeguards.

In the ever-changing technological environment, security that is state-of-the-art today is obsolete tomorrow. Security must keep pace with these changes and must be dealt with in a proactive and timely manner to be effective.

HIGH LEVEL INFORMATION SECURITY GOOD PRACTICE

Good practice

Treat security management as a business issue.

Too often information security has been dealt with as a technology issue only, with little consideration given to enterprise priorities and requirements. Effective security should not be viewed as a technology problem, but rather as a business concern. Instead of leaving security matters in the hands of technologists, Centers should:

- Achieve a better alignment of technological and business requirements by incorporating security into ICT investment plans
- Track the cost of security breaches
- Evaluate return on security investment



Good practice

Ensure management support for information security decisions

Center management should participate in the security decisions. Management has several very fundamental responsibilities to ensure that information security governance is in force. They should:

- Become informed about information security.
- Set direction, i.e., drive policy and strategy and define a risk framework within which information security risks can be assessed. This should be done in the context of Center-wide risk management policies and frameworks.
- Provide resources to information security efforts based on clearly articulated cost-benefit submissions.
- Assign responsibilities for information security.
- Set priorities for information security.
- Support change that is required to enhance information security to desired levels.
- Set security risk consciousness.
- Obtain assurance from internal or external auditors.
- Insist that security investments and security improvements are measurable, and that they receive and monitor reports on information security program effectiveness.

They should understand that:

- Information security risks and threats are real and could have significant impact on the organization.
- Effective information security requires coordinated and integrated action from the top down, taking into consideration cultural and organizational factors.
- IT investments can be very substantial and easily misdirected.
- Rules and priorities need to be established and enforced.
- Trust in reliability of system security needs to be demonstrated to all stakeholders.
- Security incidents are likely to be exposed to the public and reputational or other damage could be considerable. For example in some jurisdictions in which Centers operate, privacy laws exact significant penalties for non-compliance with the protection of certain data. Loss of confidentiality of research data developed or proprietary information provided under agreements with third parties may attract contract disputes and loss of strategic partnerships.
- Center Boards of Trustees should be briefed on these issues, as part of the Center's risk management reporting process.



Good practice

Define roles and responsibilities for information security

Responsibility for governing and managing the improvement of security has traditionally been limited to operational and technical managers.

For information security to be properly addressed, greater involvement of executive management and business process owners is required. All interested parties should be involved in the process. It should be ensured that individual roles, responsibilities and authority are clearly communicated and understood by all.

Good practice

Implement an information security program

Introducing an information security program is the cornerstone for an effort to transform information security into a proactive activity driven by the business leadership, instead of reactive one driven by technologists within an organization.

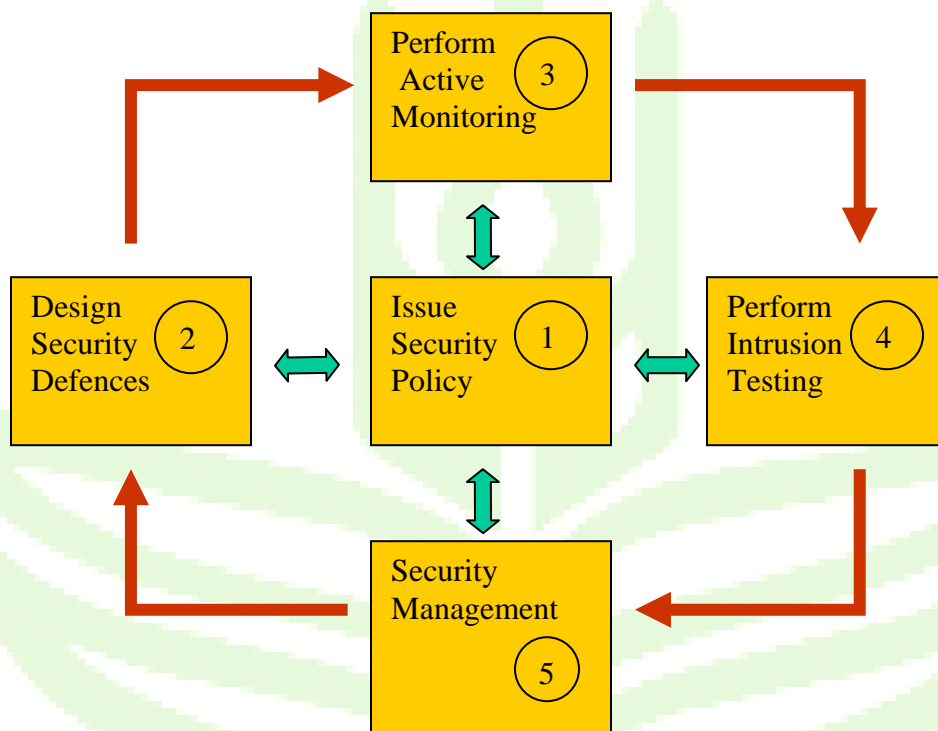
An information security program is a risk mitigation method like other control and governance actions and should therefore clearly fit into, and become an important part of, overall IT governance. Information security governance should become a very focused activity, with specific value drivers: integrity of information, continuity of services and protection of information assets.

According to the International Guidelines for Managing Risk of Information and Communications Statement #1: Managing Security of Information, issued by the International Federation of Accountants, the six major activities involved in information security is:

- Policy Development—Using the security objective and core principles as a framework around which to develop the security policy
- Roles and Responsibilities—Ensuring that individual roles, responsibilities and authority are clearly communicated and understood by all
- Design—Developing a security and control framework that consists of standards, measures, practices and procedures
- Implementation—Implementing the solution on a timely basis, then maintaining it



- Monitoring—Establishing monitoring measures to detect and ensure correction of security breaches, such that all actual and suspected breaches are promptly identified, investigated and acted upon, and to ensure ongoing compliance with policy, standards and minimum acceptable security practices
- Awareness, Training and Education—Creating awareness of the need to protect information, providing training in the skills needed to operate information systems securely, and offering education in security measures and practices.



ELEMENTS OF AN INFORMATION SECURITY PROGRAM

In order assist the Centers to develop an information security program, below are key control objectives and 39 steps toward better information security. This covers the most important security-related objectives, and has been extracted from the COBIT framework. The COBIT framework process model is consist of generic IT processes grouped into four domains – Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate.



PLAN AND ORGANISE

Control Objective

Define a strategic IT plan – define the information architecture

Identify information and services critical to the enterprise and consider their security requirements.

1. Based on business impact for critical business processes, identify:

- Data that must not be misused or lost. Services that need to be available
- Transactions that must be trusted (to be authentic and have integrity)

Consider the security requirements:

- Who may access and modify data?
- What data retention and backup are needed? .What availability is required?
- What authorizations and verification are needed for electronic transactions?

Define the IT Organization and relationship

Define and communicate IT security responsibilities.

2. Define specific responsibilities for the management of security and:

- Ensure that they are assigned, communicated and properly understood
- Be aware of the dangers of concentrating too many security roles and responsibilities in one person
- Provide the resources required to exercise responsibilities effectively

Communicate Management aims direction

Appropriately define and circulate management aims and directions with respect to IT security.

3. Consistently communicate and regularly discuss the basic rules for implementing security requirements and responding to security incidents. Establish minimum dos and do nots and regularly remind people of security risks and their personal



	responsibilities.
Manage Human Resource	
Ensure functions are staffed properly by the right people who possess the necessary skills to fulfill responsibilities, including security.	<p>4. When hiring, verify with reference checks.</p> <p>5. Obtain through hiring or training the skills needed to support the enterprise security requirements. Verify annually whether skills and qualifications are up to date, and act accordingly.</p> <p>6. Ensure that no key security task is critically dependent upon a single resource.</p>
Ensure compliance with external requirements	
Ensure that IT security functions comply with applicable laws, regulations and other external requirements.	7. Identify what, if anything needs to be done with respect to security obligations to comply with privacy, intellectual property rights, and other legal, regulatory, contractual and insurance requirements. Encourage staff to understand and be responsive to these security obligations.
Discover, prioritize, and either contain or accept relevant IT security risks.	<p>8. At appropriate times, discuss with key staff what can go wrong with IT security that could significantly impact the business objectives. Consider how best to secure services, data and transactions that are critical for the success of the business. Prepare a risk management action plan to address the most significant risks.</p> <p>9. Establish staff understanding of the need for responsiveness and consider cost-effective means to manage the identified security risks through security practices (e.g., effective backup, basic access control, virus protection, firewalls) and insurance coverage.</p>
ACQUIRE AND IMPLEMENT	
Identify automated solution	
Consider security when identifying automated solution.	10. Consider how automated solutions may introduce security risks to the business and supporting processes they plan to



	<p>change. Ensure that the solution is functional and that operational security requirements are specified and compatible with current system. Obtain comfort regarding the trustworthiness of the selected security technology/service through references, external advice, contractual arrangement, etc.</p>
Acquire and maintain technology infrastructure	
<p>Consider security when acquiring and maintaining the technology infrastructure.</p>	<p>11. Ensure that the technology infrastructure properly supports automated security practices.</p> <p>12. Consider what additional security requirements are needed to protect the technology infrastructure itself.</p> <p>13. Identify and monitor sources for keeping up to date with security patches and implement those appropriate for the enterprise infrastructure.</p>
Develop and maintain procedures	
<p>Consider security when developing and maintaining Procedures.</p>	<p>14. Ensure that staff knows how to integrate security in day-to-day procedures. Document procedures and train staff.</p>
Install and accredit systems	
<p>Ensure that all new systems and changes are accepted only after sufficient testing of security functions.</p>	<p>15. Test the system (or major change) against functional and operational security requirements in a representative environment so the results are reliable. Consider testing how the security functions integrate with existing systems. Do not test on the live production system.</p> <p>16. Perform final security acceptance by evaluating all test results against business goals and security requirements involving key staff who will use, run and maintain the system.</p>
Manage change	
<p>Ensure that all changes, including patches, support enterprise objectives, are carried out in a</p>	<p>17. Evaluate all changes, including patches, to establish the impact on the integrity, exposure or loss of sensitive data, availability of critical services, and validity of important</p>



secure manner. Ensure that day-to-day business processes are not impacted	transactions. Based on this impact, perform adequate testing prior to making the change. 18. Record and authorize all changes, including patches (emergency changes possibly after the fact).
DELIVER AND SUPPORT	
Define and manage service level	
Define and manage security aspects of service levels.	19. Ensure that management establishes security requirements and regularly reviews compliance of internal service level agreements and contracts with third-party service providers.
Manage third-party services	
Manage security aspect of services.	20. Assess the professional capability of third parties and ensure they provide adequate contact with the authority to act upon enterprise security requirements and concerns. 21. Consider the dependence on third-party suppliers for security requirements, and mitigate continuity, confidentiality and intellectual property risk by, for example, escrow, legal liabilities, penalties and rewards.
Ensure continuous service	
Ensure that the enterprise is capable of carrying on its day-to-day automated business activities with minimal interruption from a security incident.	22. Identify critical business functions and information, and those resources (e.g., applications, third-party services, supplies and data files) that are critical to support them. Provide for availability of these resources in the event of a security incident to maintain continuous service. Ensure that significant incidents are identified and resolved in a timely manner. 23. Establish basic principles for safeguarding and reconstructing IT services, including alternative processing procedures, how to obtain supplies and services in an emergency, how to return to normal processing after the security incident, and how to communicate with customers and suppliers.



	<p>24. Together with key employees, define what needs to be backed up and stored offsite to support recovery of the business, e.g., critical data files, documentation and other IT resources, and secure it appropriately. At regular intervals, ensure that the backup resources are usable and complete.</p>
Ensure systems security	
<p>Ensure that all aspects of the enterprise's automated processing are used only by authorized persons/systems for business purposes.</p>	<p>25. Implement rules to control access to services based on the individual's need to view, add, change or delete information and transactions. Especially consider access rights of service providers, suppliers and customers.</p> <p>26. Ensure that responsibility is allocated to manage all user accounts and security tokens (e.g., passwords, cards and devices) to control devices, tokens and media with financial value. Periodically review/confirm the actions and authority of those managing user accounts. Ensure that these responsibilities are not assigned to the same person.</p> <p>27. Detect and log important security violations (e.g., system and network access, virus, misuse, and illegal software). Ensure that they are reported immediately and acted upon in a timely manner.</p> <p>28. To ensure that counterparties can be trusted and transactions are authentic when using electronic transaction systems, ensure that the security instructions are adequate and compliant with contractual obligations.</p> <p>29. Enforce the use of virus protection software throughout the enterprise's infrastructure and maintain up-to-date virus definitions. Use only legal software.</p> <p>30. Define policy for what information can come into and go out of the organization, and configure the network security systems, e.g., firewall, accordingly. Consider how to protect physically transportable storage devices. Monitor exceptions and follow up on significant incidents.</p>



Manage the configuration	
Ensure that all assets are appropriately secured and security risks minimized by maintaining the enterprise's awareness of its IT-related assets and licenses.	<p>31. Ensure that there is a regularly updated and complete inventory of the IT hardware and software configuration.</p> <p>32. Regularly review whether all installed software is authorized and licensed properly.</p>
Manage data	
Ensure that all data remain complete, accurate and valid during input, processing, storage and distribution.	<p>33. Subject data to a variety of controls to check for integrity (accuracy, completeness and validity) during input, processing, storage and distribution. Control transactions to ensure their authenticity and that they cannot be repudiated.</p> <p>34. Distribute sensitive output only to authorized people.</p> <p>35. Define retention periods, archival requirements and storage terms for input and output documents, data and software. Ensure that they comply with user and legal requirements. While in storage, check continuing integrity and ensure that data cannot be retrieved.</p>
Manage facilities	
Protect all IT equipment from damage.	<p>36. Physically secure the IT facilities and assets, especially those most at risk to a security threat, and if applicable, obtain expert advice.</p> <p>37. Protect computer networking and storage equipment (particularly mobile equipment) from damage, theft, accidental loss and interception.</p>
MONITOR AND EVALUATE	
Monitor the processes-assess internal control adequacy	
Regularly monitor the performance of information security.	<p>38. Have key staff periodically:</p> <ul style="list-style-type: none">Assess adequacy of security controls compared to defined requirements and in light of current vulnerabilities



	<ul style="list-style-type: none">● Reassess what security exceptions need to be monitored on an ongoing basis● Evaluate how well the security mechanisms are operating and check for weaknesses, such as intrusion detection, penetration and stress testing, and testing of contingency plans.● Ensure that exceptions are acted upon. Monitor compliance to key controls.
Obtain independent assurance	
Gain confidence and trust in security through reliable and independent sources.	39. Obtain, where needed, competent external resources to review the information security control mechanisms; assess compliance with laws, regulations and contractual obligations relative to information security. Leverage their knowledge and experience for internal use.

SUMMARY OF TECHNICAL SECURITY RISKS

Computer Misuse Security Risks

Trojan Horse programs

Trojan Horse programs are a common way for intruders to trick the user (sometimes referred to as “social engineering”) into installing “back door” programs, which can allow intruders easy access to the user’s computer without his/her knowledge, change the system configurations or infect the computer with a computer virus.

Back door and remote administration programs

On computers using a Windows operating system, intruders commonly use three tools—Back Orifice, Netbus and SubSeven—to gain remote access to the computer. These back door or remote administration programs, once installed, allow other people to access and control the computer. The CERT vulnerability note about Back Orifice should be reviewed. Other computer platforms may be vulnerable and the user needs to monitor vulnerability reports and maintain the system.



Denial-of-service attacks

Another form of attack is called a denial-of-service attack. This type of attack causes the computer to crash or become so busy processing data that the user is unable to use it. In most cases, the latest patches will prevent the attack.

Being an intermediary for another attack

Intruders frequently use compromised computers as launching pads for attacking other systems. The use of distributed denial-of-service (DDoS) tools is an example of this. The intruders would install an “agent” (frequently through a Trojan Horse program) that runs on the compromised computer awaiting further instructions. Then, when many agents are running on different computers, a single “handler” can instruct all of them to launch a denial-of-service attack on another system. Thus, the end target of the attack is not the original user’s computer, but someone else’s—the original user’s computer is just a convenient tool in a larger attack.

Unprotected Windows networking shares

Intruders can exploit unprotected Windows networking shares in an automated way to place tools on large numbers of Windows-based computers attached to the Internet. Because site security on the Internet is interdependent, a compromised computer not only creates problems for the computer's owner, but it is also a threat to other sites on the Internet.

Mobile code (Java/JavaScript/ActiveX)

There have been reports of problems with “mobile code” (e.g., Java, JavaScript and ActiveX). These programming languages let web developers write code that is executed by the organization’s web browser. Although such code is generally useful to the organization, intruders also use it to gather information (such as which web sites the user visits) or run malicious code on the computer. It is possible to disable Java, JavaScript and ActiveX in the web browser, but the user should be aware that this may limit legitimate browser functionality. Also, the user should be aware of the risks involved in the use of mobile code within e-mail programs. Many e-mail programs use the same code as web browsers to display HTML. Thus, vulnerabilities that affect Java, JavaScript and ActiveX are often applicable to e-mail and web pages.

Cross-site scripting

A malicious web developer may attach a script to something sent to a web site, such as a URL, an element in a form or a database inquiry. Later, when the web site responds, the malicious script is transferred to the browser. This can potentially expose the web browser to malicious scripts by:
Following links in web pages, e-mail messages or newsgroup postings without knowing where they link
Using interactive forms on an untrustworthy site



Viewing online discussion groups, forums or other dynamically generated pages where users can post text containing HTML tags

E-mail spoofing

E-mail spoofing is when an e-mail message appears to have originated from one source when it actually was sent from another source. E-mail spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords). Spoofed e-mail can range from harmless pranks to social engineering ploys. Examples of the latter include:

E-mail claiming to be from a system administrator requesting users to change their passwords to a specified string and threatening to suspend their account if they do not comply

E-mail claiming to be from a person in authority requesting users to send a copy of a password file or other sensitive information

E-mail-borne viruses

Viruses and other types of malicious code are often spread as attachments to e-mail messages. Before opening any attachments, the user should be aware of the source of the attachment. It is not enough that the e-mail originated from a recognized address. For example, the Melissa virus spread precisely because it originated from a familiar address. Also, malicious code might be distributed in amusing or enticing programs. Many recent viruses use these social engineering techniques to spread. Examples include W32/Sircam and W32/Goner.

Hidden file extensions

Windows operating systems contain an option to hide file extensions for known file types. The option is enabled by default, but a user may choose to disable this option to have file extensions displayed by Windows. Multiple e-mail-borne viruses are known to exploit hidden file extensions. The first major attack that took advantage of a hidden file extension was the VBS/LoveLetter worm that contained an e-mail attachment named LOVE-LETTER-FOR-YOU.TXT.vbs. Other examples include Downloader (MySis.avi.exe or QuickFlick.mpg.exe), VBS/CoolNote (COOL_NOTEPAD_DEMO.TXT.vbs), and VBS/OnTheFly (AnnaKournikova.jpg.vbs). The files attached to the e-mail messages sent by these viruses may appear to be harmless text (.txt), MPEG (.mpg), AVI (.avi) or other file types, when in fact the file is a malicious script or executable (.vbs or .exe).

Chat clients

Internet chat applications, such as instant messaging applications and Internet relay chat (IRC) networks, provide a mechanism for information to be transmitted bi-directionally between computers on the Internet. Chat clients provide groups of individuals with the means to exchange dialogue, web URLs and, in many cases, files of any type. Because many chat clients allow for the exchange of executable



code, they present risks similar to those of e-mail clients. As with e-mail clients, the chat clients' ability to execute downloaded files should be limited. As always, the user should be wary of exchanging files with unknown parties.

Packet sniffing

A packet sniffer is a program that captures data from information packets as they travel over the network. These data may include user names, passwords and proprietary information that travels over the network in cleartext. With perhaps hundreds or thousands of passwords captured by the packet sniffer, intruders can launch widespread attacks on systems. Installing a packet sniffer does not necessarily require administrator-level access. Relative to DSL and traditional dial-up users, cable modem users have a higher risk of exposure to packet sniffers, since entire neighborhoods of cable modem users are effectively part of the same LAN. A packet sniffer installed on any cable modem user's computer in a neighborhood may be able to capture data transmitted by any other cable modem in the same neighborhood.

Identity theft

Information stored on a home computer may provide a hacker with enough personal data to apply for a credit card or identification in the user's name.

Tunneling

When employees work at home and transfer files to a computer at the office, there is potential that someone could remotely gain access to the home PC and place a secret file in a document that ends up on the company system.

Zombies

Automatic programs search for systems that are connected to the Internet, but are unprotected; take them over without the owner's knowledge; and use them for malicious purposes.

Spyware

Innocent looking software (e.g., P2p-agent software used in popular peer-to-peer communications software) can include or hide software that collects information about the system and the user, and can send this information to third parties without the legitimate user knowing.



Violations of Rules and Regulations

Intellectual property

Compliance with all software license agreements should be ensured. In addition, intellectual property law will protect other forms of media and care should be taken to respect these rights.

Decent use of the Internet

The Internet allows access to unlimited information, including sources that are considered indecent or sometimes outright illegal. Such use of the Internet is discouraged in both a working environment and the private home.

Industrial espionage

Data and information that are not well protected may allow competitors to spy upon the user's information.

Rules and regulations

The use of information systems is, depending on the country, state or industry, subject to a number of rules and regulations. These need to be known and obeyed. Domains covered by such rules include privacy, retention of information, minimal system protection requirements and attestation requirements.

Accidents

Disk failure

Availability is one of the three key elements of information security. Although all stored data can become unavailable—if the media they are stored on are physically damaged, destroyed or lost—data stored on hard disks are at higher risk due to the mechanical nature of the device. Hard disk crashes are a common cause of data loss on personal computers.

Power failure and surges

Power problems (e.g., surges, blackouts and brownouts) can cause physical damage to a computer, inducing a hard disk crash or otherwise harming the electronic components of the computer. Common mitigation methods include using surge suppressors and uninterruptible power supplies (UPS).



Physical theft

Physical theft of a computer, of course, results in loss of confidentiality and availability, and (assuming the computer is ever recovered) makes the integrity of the data stored on the disk suspect. Regular system backups (with the backups stored somewhere away from the computer) allow for recovery of the data, but backups alone cannot address confidentiality. Cryptographic tools are available that can encrypt data stored on a computer's hard disk.

Software Problem

One of the most common problems when using computers is software, i.e., software not performing in a stable or predictable manner or not performing up to expectations or specifications. End users carry little responsibility here, but manufacturers and developers do.

Exposure Draft: October 2005 (Adopted without Change)
Author: Vima Salazar