Ethical Hacking and Countermeasures

Version 6

Module XXI

Physical Security

Real World Scenario

Michael, a practicing computer security consultant, was asked to do a physical security test by the Chief of a well-known database firm. Their database was considered to have a major competitive edge. They believed their systems were secure, but wanted to be sure of it.

Michael went to the firm on the pretext of meeting its Chief. Before entering the lobby, Michael had driven around the building and checked for loopholes in the physical security, where he could easily slip into the building.

Real World Scenario

He walked to the loading bays, up the stairs, and proceeded through the warehouse, to what was an obvious entrance into the office building. Michael also knew of the location of the computer room. He took the elevator down, and entered the room, which was secured with cipher locks and access cards. He went straight to the tape racks. There, he studied the racks, as if looking for specific information. He grabbed a tape with an identifier that looked something like ACCT95QTR1.

The entire process lasted no more than 15 minutes. During that time, Michael breached their physical security by entering the building and taking a tape.

Security firms back CCTV use in business premises

Written by Steve Mbogo

Wangui Muchiri and Ken Wood (left) address the Press on security issues within the central business district.

Photo by: Frederick Onyango

January 25, 2008: The Kenya business community is likely to have a major shift in its security model following increased looting and vandalism of property during the post-poll violence.

Security companies and the business community told Business Daily the new models will include taking measures ranging from going for stronger equipment to secure business premises and use of latest technology that will ensure around the clock monitoring.

Ken Wood, the managing director of G4S, a private security company, said premises access control systems in Kenya are generally "weak", adding that more often than not, unwanted people are able to get into premises.

Mr Wood said companies should invest in high quality coloured close circuit cameras (CCTVs) which are more effective.

Most businesses have made losses from post-election violence and have to pay for the liabilities caused as some insurers remain unclear on how claims should be treated .

Insurance firms like Association of Kenya Insurers and the Association of Kenya Reinsurers said the loss or damage arising from political risks will not be covered, adding that they are willing to discuss the claims arising from the disturbances "positively."

Others like the Co-operative Company (CIC) say they will be paying the claims arising from the political violence through its microinsurance department.

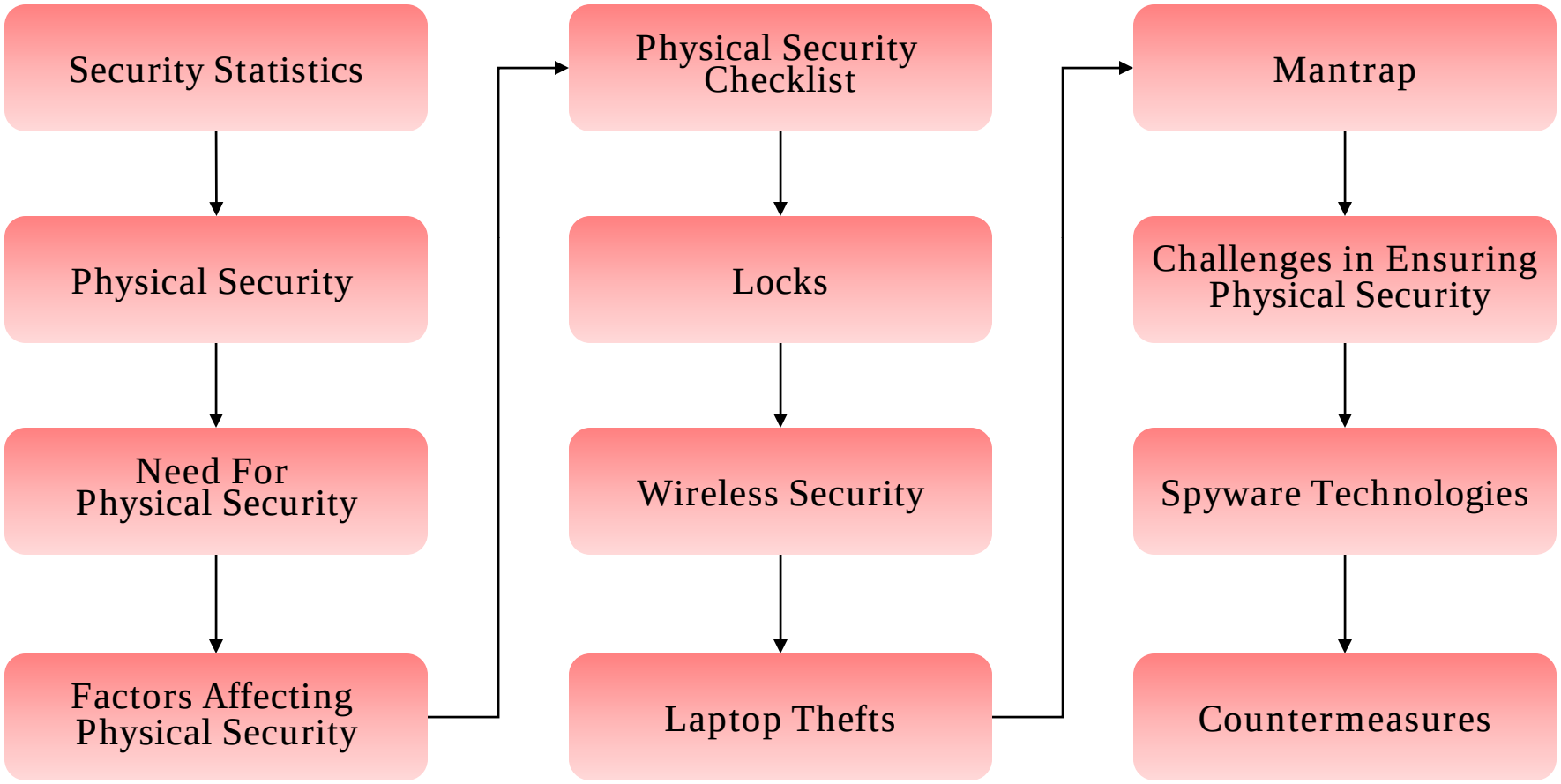
Source: *http://www.bdafrica.com/*

Module Objective

This module will familiarize you with:

- Security Statistics
- Physical security
- Need for physical security
- Factors that affect physical security
- Physical Security checklist
- Locks
- Wireless Security
- Laptop Thefts
- Mantrap
- Challenges in Ensuring Physical Security
- Spyware Technologies
- Countermeasures

Module Flow



Security Facts

- Receive alarm communications - 28%
- Access control technology with identification cards - 90%
- Companies require visitors to wear a badge or pass that identifies them as a visitor - 93%
- Explosion detection devices – 9%
- Emergency telephones in parking areas – 9%
- Police officers for security - 56%
- Companies use metal detectors for screen employees and visitors – 7%

Source: *http://www.aga.org/*

Another security breach: IRS sent taxpayer data on unencrypted tapes

By Beth Pariseau, Senior News Writer
14 Jan 2008 | SearchStorage.com

Despite all the high-profile incidents in the past two years of lost backup tapes and other security breaches, the Internal Revenue Service (IRS) was exposing personal information on unencrypted tapes until last fall.

The IRS confirmed to SearchStorage.com that copies of its tax database were distributed to state agencies on unencrypted tapes before Sept. 30, 2007. A source at one state agency said the tapes were also sent using common carriers, such as FedEx.

More on tape encryption and security

Iron Mountain loses backup tapes containing student data

Users: Storage security becoming a priority

How to destroy data on backup tapes

The source, whose agency received the database information on a regular basis, said the IRS had formal guidelines for agencies to place the tapes behind three layers of physical security -- inside a locked box, for example -- and restrict access to "need-to-know" personnel. He added a fourth layer of physical security, but that still didn't make him feel comfortable. "These were standard IBM mainframe tapes," he said. "It didn't take anything special to read them."

Source: *http://searchstorage.techtarget.com*

Understanding Physical Security

Since man always had something important to protect, he found various methods of protecting it

Egyptians were the first to develop a working lock

Physical security describes the measures that prevent or deter attackers from accessing a facility, resource, or information stored on the physical media

Physical security is an important factor of computer security

Major security actions that are involved with physical security are intended to protect the computer from climate conditions, even though most of them are targeted at protecting the computer from intruders who use, or attempt to use physical access to the computer to break into it

Physical Security

Physical security describes measures taken to protect personnel, critical assets, and systems against deliberate and accidental threats

Physical security measures can be:

Physical

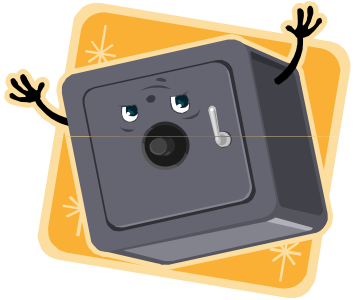
- Physical measures are taken to secure assets e.g. deploying security personnel

Technical

- Technical measures are taken to secure services and elements that support Information Technologies e.g. security for server rooms

Operational

- Common security measures are taken before performing an operation such as analyzing threats of an activity and taking appropriate countermeasures



What Is the Need for Physical Security

- To prevent any unauthorized access to computer systems
- To prevent tampering/stealing of data from computer systems
- To protect the integrity of the data stored in the computer
- To prevent the loss of data/damage to systems against any natural calamities

Who Is Accountable for Physical Security

In most organizations, there is not a single person who is accountable for physical security

People who should be made accountable for the security of a firm including both physical and information security are:

- The plant's security officer
- Safety officer
- Information systems analyst
- Chief information officer

Factors Affecting Physical Security

Factors that affect the physical security of a particular firm:

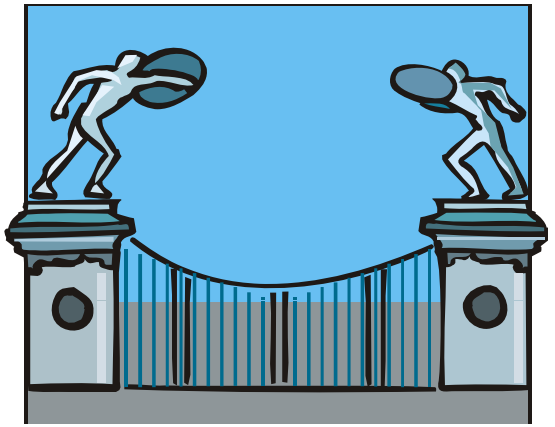
- Vandalism
- Theft
- Natural calamities:
  - Earthquake
  - Fire
  - Flood
  - Lightning and thunder
- Dust
- Water
- Explosion
- Terrorist attacks

Physical Security Checklist

- Company surroundings
- Premises
- Reception
- Server
- Workstation area
- Wireless access points
- Other equipment, such as fax, and removable media
- Access control
- Computer equipment maintenance
- Wiretapping
- Remote access

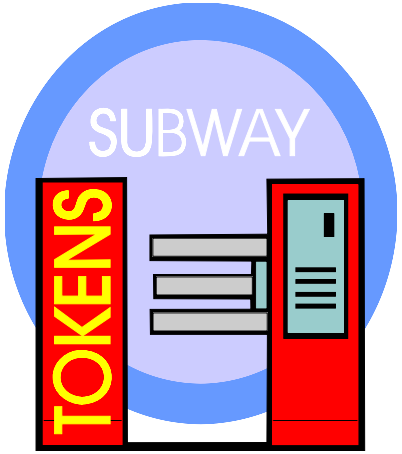
Physical Security Checklist: Company Surroundings

The entrance to the company premises should be restricted to only authorized access



Checklist for securing the company surroundings:

- Fences
- Gates
- Walls
- Guards
- Alarms



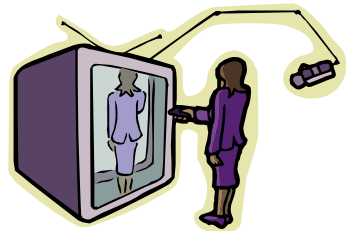
Gates

Security Guards

Physical Security Checklist: Premises

Premises can be protected by:

- Checking for roof/ceiling access through AC ducts
- Use of CCTV cameras with monitored screens and video recorders
- Installing intruder systems
- Installing panic buttons
- Installing burglar alarms
- Windows and door bars
- Deadlocks



CCTV Cameras

Physical Security Checklist: Reception

The reception area is supposed to be a busier area than other areas of the firm with the number of people entering and exiting

The reception area can be protected by:

- Files and documents, removable media, etc. should not be kept on the reception desk
- Reception desks should be designed to discourage inappropriate access to the administrative area by non-staff members
- Computer screens should be positioned in such a way that people cannot observe the screen near the reception desk
- Computer monitors, keyboards, and other equipments at the reception desk should be locked whenever the receptionist is away from the desk and they should be logged off after office hours

Reception

Physical Security Checklist: Server

The server, which is the most important factor of any network, should be given a high level of security

The server room should be well-lit

The server can be secured by the following means:

- Server should not be used to perform day-to-day activities
- It should be enclosed and locked to prevent any physical movement
- DOS should be removed from Windows Servers as an intruder can boot the server remotely by DOS
- Booting from the floppy disk should be disabled and CD-ROM drives on the server or, if possible, avoid having these drives on the server

Server Room

Physical Security Checklist: Workstation Area

This is the area where a majority of employees work

Employees should be educated about physical security

The workstation area can be physically secured by taking the following steps:

- Use CCTV
- Screens and PCs should be locked
- Workstation layout design
- Avoid removable media drives

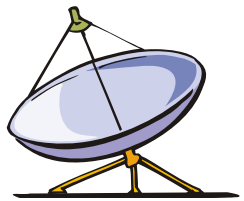
Physical Security Checklist: Wireless Access Points

If an intruder successfully connects to the firm's wireless access points, then he is virtually inside the LAN like any other employee of the firm

To prevent such unauthorized access, the wireless access points should be secured

Guidelines to follow:

- WEP encryption should be followed
- SSID should not be revealed
- Access points should be password protected to gain entry
- Passwords should be strong enough so that they cannot be easily cracked



Physical Security Checklist: Other Equipment

Other equipments, such as fax, and removable media

- Such equipment should be secured by following these steps:
  - Fax machines near the reception area should be locked when the receptionist is not at the desk
  - Faxes obtained should be filed properly
  - Modems should not have auto answer mode enabled
  - Removable media should not be placed in public places, and corrupted removable media should be physically destroyed

Physical Security Checklist: Access Control

Access control is used to prevent unauthorized access to any sensitive operational areas

The types of access controls are:

- Separation of work areas
- Biometric access control
- Entry cards
- Man traps
- Faculty sign-in procedures
- Identification badges

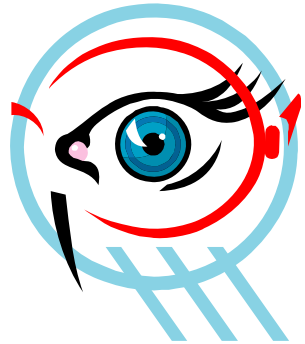
Physical Security Checklist: Biometric Devices

According to www.whatis.com, “Biometrics is the science and technology of measuring and statistically analyzing biological data”

Biometric devices consist of a reader or scanning device, software that converts the scanned information into digital form, and a location for the data to be analyzed; for instance a database that stores the biometric data for comparison with previous records

Methods used by biometric devices for access control are:

- Fingerprints
- Face scan
- Iris scan
- Voice recognition



Biometric Identification Techniques

Fingerprinting

- Ridges and furrows on the surface of a finger are used to identify a person, which are unique

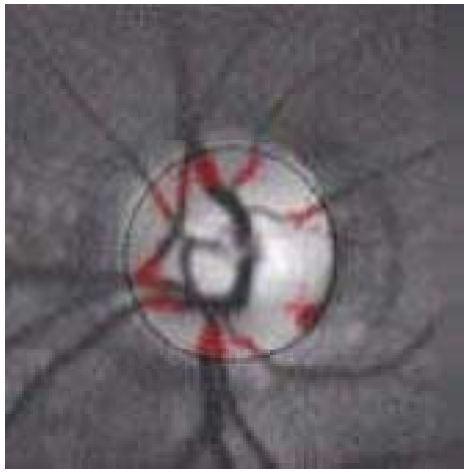
Iris Scanning

- Analyzes the colored part of the eye suspended behind the cornea

Biometric Identification Techniques (cont'd)

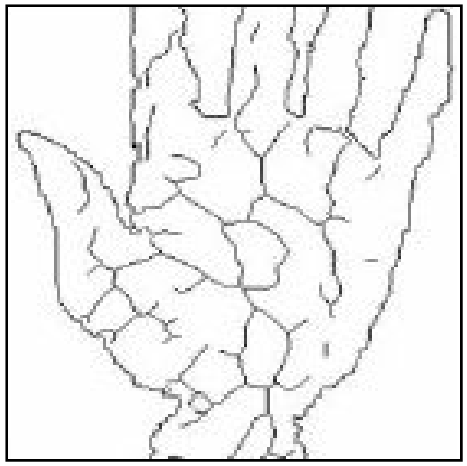
Retinal scanning

- Identifies a person by analyzing the layer of blood vessels at the back of the eye



Vein Structure

- Thickness and location of veins are analyzed to identify person



Authentication Mechanisms

Something you are :

- Use of biometric techniques such as fingerprints, facial recognition, hand geometry, retinal scan, iris scan, vascular pattern, signature dynamics, and voice dynamics

Something you know:

- Based on the traditional password system

Something you have:

- Includes mechanisms such as challenge-response lists, one-time pads, smart cards, and so on

Authentication Mechanism Challenges: *Biometrics*

Fingerprints can be faked with ease

Face recognition systems can be tricked by masquerade techniques

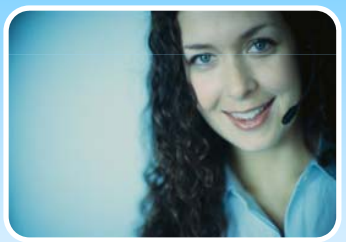
Signature recognition and hand geometry face the common problem of matching the patterns from a large database which might lead to higher number of false positives and false negatives

Retinal scan can hinder accuracy if the user does not focus on a given point for scan. Iris scan machines are very expensive

Some users object to vascular pattern technology that uses infrared light

Voice dynamics is prone to inaccuracy as it relies on the production of a "voice template" that is compared with a spoken phrase

Faking Fingerprints



Identify your target whose fingerprint you want to fake

Glasses, door knobs, and glossy paper can be good sources to obtain fingerprints of the target

Use the traditional forensic method to make the fingerprints visible. Sprinkle the outer surface of the glass with colored powder so that it sticks to the fat. Latent fingerprints are nothing but fat and sweat on the glass used by the target

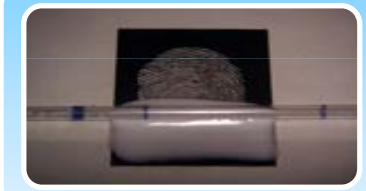
Faking Fingerprints (cont'd)

Photograph the fingerprint and scan the image

Use a professional image editor to work on the scanned image. You need to get the exact image of the fingerprint to use as mold, from which the dummy is made

Take the print of the image on a transparency sheet using a laser printer. Add wood glue to one of the prints on the transparency sheet

Faking Fingerprints (cont'd)



Add a small drop of glycerine to help in the process of making the dummy. Use a roller for letter press printing

After the glue dries up, it is pulled off the foil, and is cut to finger size

Theatrical glue is used to glue the dummy onto your own finger

You have faked the fingerprint!

Physical Security Checklist

Smart Cards

A smart card is a plastic card about the size of a credit card, with an embedded microchip that can be loaded with data

This data can be used for telephone calling, electronic cash payments, and other applications, and then periodically refreshed for additional use

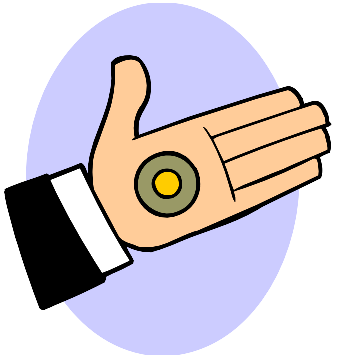
A smart card contains more information than a magnetic strip card and can be programmed for different applications

Security Token

According to the search security definition, “A security token is a small hardware device that the owner carries to authorize access to a network service”

Security tokens provide an extra level of assurance through a method known as two-factor authentication:

- The user has a personal identification number (PIN) that authorizes them as the owner of that particular device
- The device then displays a number that uniquely identifies the user to the service, allowing them to log in



Computer Equipment Maintenance

- Appoint a person who will be responsible for looking after the computer equipment maintenance
- Computer equipment in a warehouse should also be accounted for
- The AMC company personnel should not be left alone when they come for the maintenance of the computer equipment
- The toolboxes and the bags of the AMC company personnel should be thoroughly scanned for any suspicious materials that could compromise the security of the firm

Wiretapping

According to www.freesearch.com wiretapping is the action of secretly listening to other people's conversations by connecting a listening device to their telephone

According to www.howstuffworks.com, "wiretap is a device that can interpret these patterns as sound"

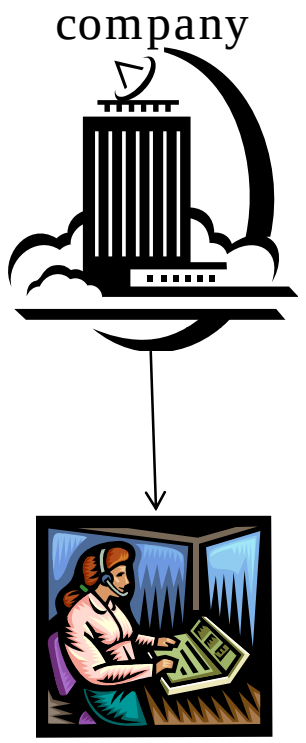
You can do few things to make sure that no one is wiretapping:

- Inspect all the data carrying wires routinely
- Protect the wires using shielded cables
- Never leave any wire exposed

Source: koopla.com/phones.htm

Remote Access

- Remote access is an easy way for an employee of a firm to work from any place outside the company's physical boundaries
- Remote access to the company's networks should be avoided as much as possible
- It is easy for an attacker to remotely access the company's network by compromising the employee's connection
- The data being transferred during the remote access should be encrypted to prevent eavesdropping
- Remote access is more dangerous than physical access as the attacker is not in the vicinity and the probability of catching him is less



Remote access

Lapse of Physical Security

Published February 10, 2008 12:00 am - Across my desk this week came the story of the theft of a laptop computer and digital camera from a high sch...

Physical security just as important as antivirus software

The Norman Transcript

Across my desk this week came the story of the theft of a laptop computer and digital camera from a high school teacher' s locked filing cabinet, which brought to mind the fact that the physical security of our digital devices is just as important as having Internet security software. All of the antivirus/antispyware/anti-Internet-bad-guy software in the world won't protect you from a clever thief stealing your laptop computer.

The fact that the locked filing cabinet containing the stolen merchandise had somehow mysteriously been unlocked was a source of confusion. Perhaps those that were confused by this situation had never heard of this thing called "the Internet," for one need look no further than the Internet for the answer to their confusion.

Source: *http://www.normantranscript.com/*

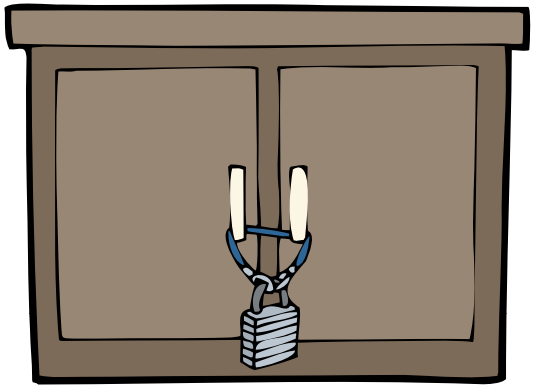
Locks

Locks are used to restrict physical access to an asset

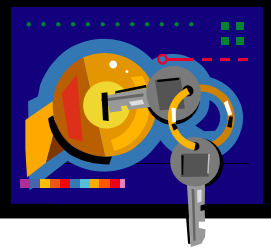
They are used on any physical asset that needs to be protected from unauthorized access, including doors, windows, vehicles, cabinets, and equipment

Different levels of security can be provided by locks depending on how they are designed and implemented

A lock has two modes - engaged/locked and disengaged/opened



Locks (cont'd)



Locks are either mechanical or electrical:

Mechanical Locks

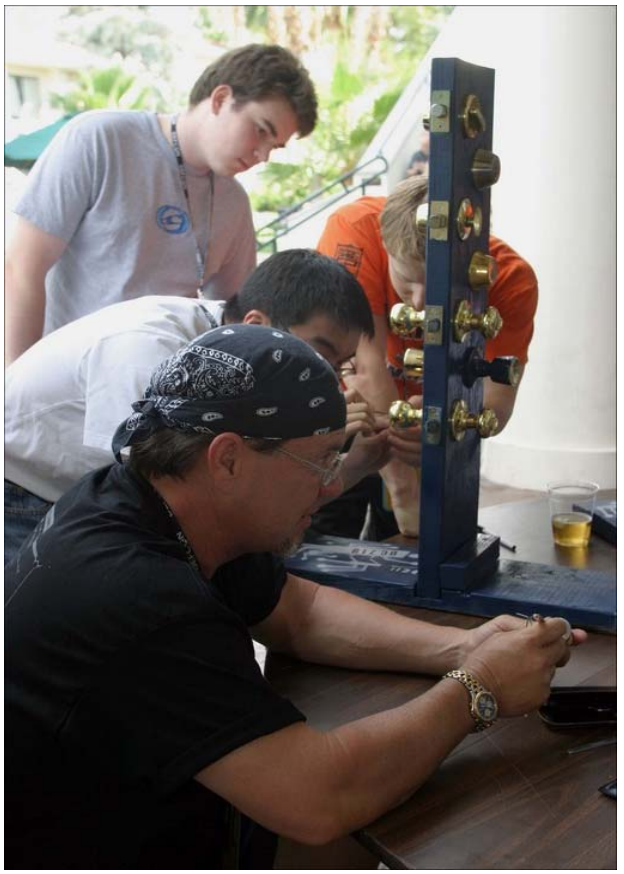
- Mechanical locks have moving parts that operate without electricity
- There are two types of mechanical locks:
  - Warded
  - Tumbler

Electric Locks

- Electric locks are comprised of electronic devices with scanners that identify users and computers that process codes
- Electric locks consist of the following types:
  - Card access systems
  - Electronic combination locks
  - Electromagnetic locks
  - Biometric entry systems

Lock Picking

Lock picking is the art of unlocking a lock without the use of its key



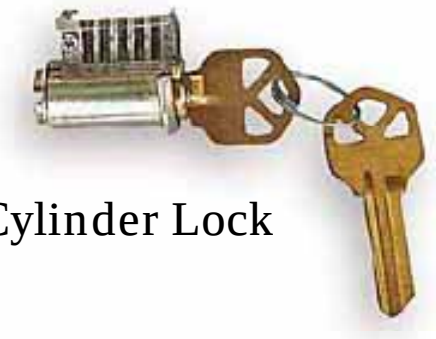
To prevent lock picking:

- Use a better quality of lock
- Do not give the keys to anyone, as key imprints can be taken for making a duplicate key
- Do not reveal the lock codes

Lock Picking Tools

Lock Picking Set

Auto Jigglers



Cylinder Lock

Tubular Lock Picks

Shovit Tool

Jack Knife

Electrick Pick

Broken Key Pullers

Lock Picking Tools (cont'd)

Information Security

Hierarchical view to secure information:

- Password protection / Complex passwords
- Encrypted file system
- Anti virus software
- Firewalls
- Intrusion detection systems
- Patches and updates
- Lock down unwanted ports / devices

EPS (Electronic Physical Security)

An integrated application of a number of electronic security systems

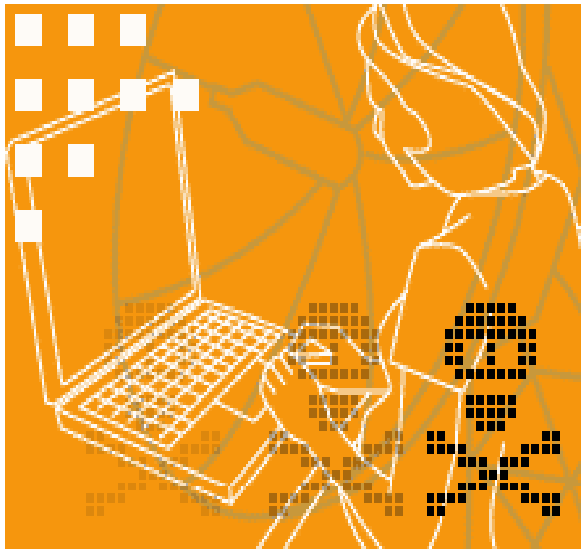
EPS includes:

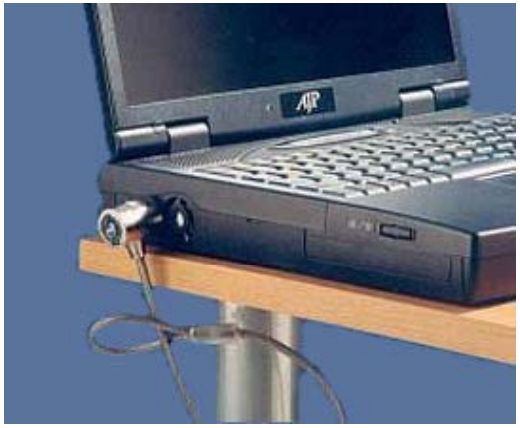
- Addressable fire detection systems
- Automatic gas suppression systems
- CCTV systems (IP Networks, Matrix Switchers, DVR camera specifications, etc.)
- RFID-Biometric- Smart Card Access Control Systems
- Intrusion detection systems
- Law enforcement systems and products (Perimeter fencing, Crash barriers, Automatic Retraceable Bollards, Turnstiles, Undercarriage Scanners, X-ray/Gamma Scanners, Sniffers)
- Guarding equipment and guarding plan

Wireless Security

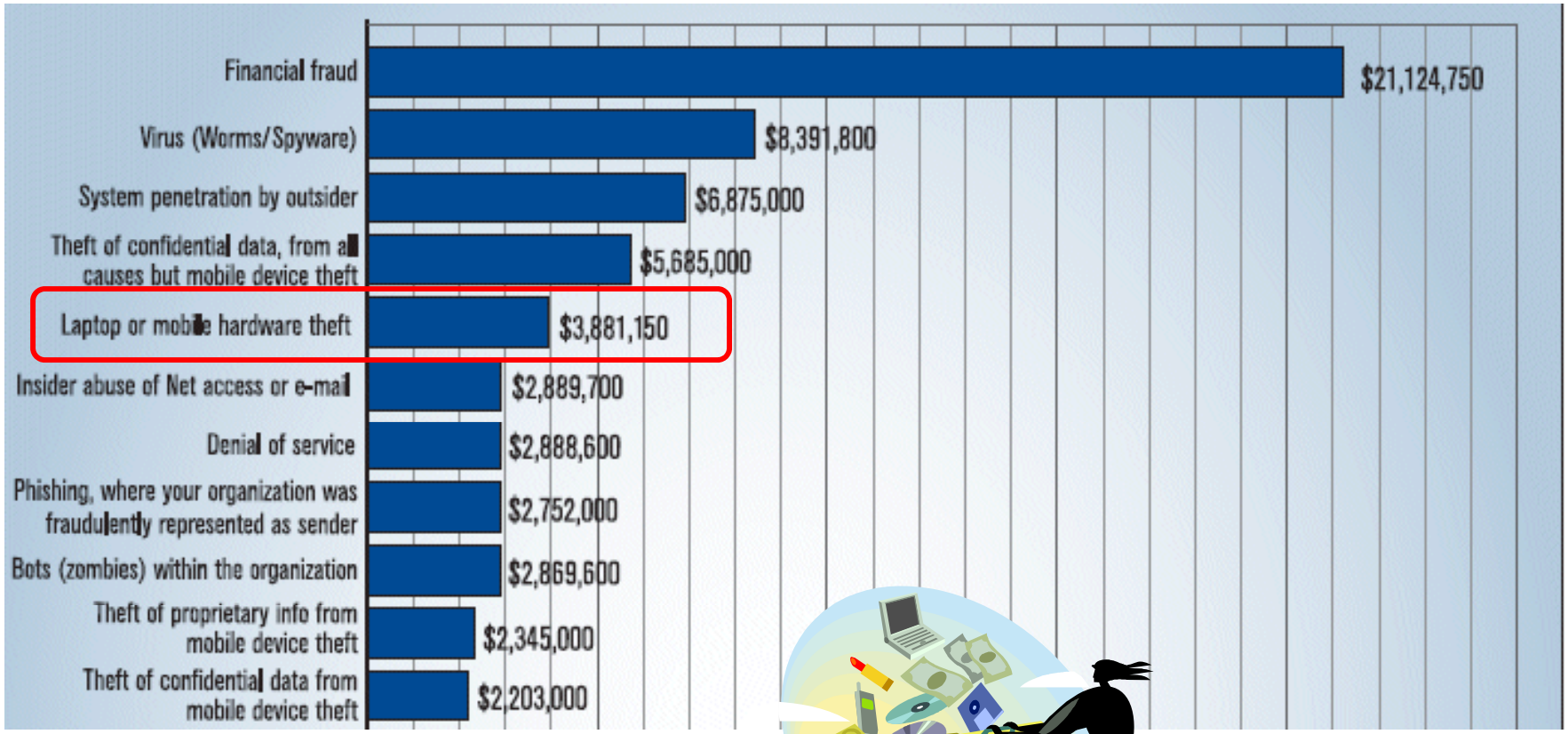
Wireless Security Measures:

- Checking the wireless traffic
- Enabling WEP/WPA on the wireless network
- MAC address control
- End-to-end encryption
- VPN (Virtual Private Network)
- Access points evaluation



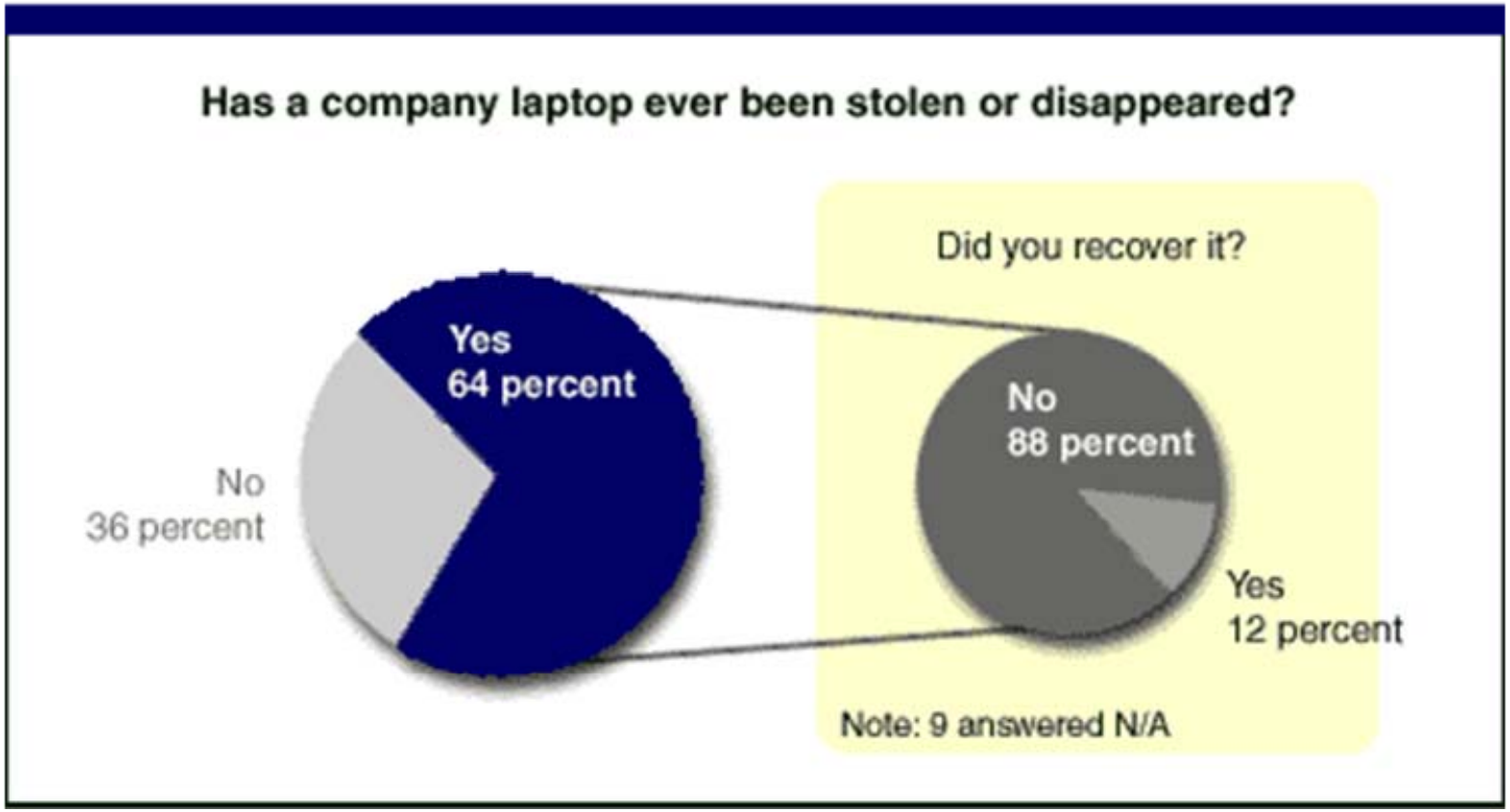


Laptop Theft Statistics for 2007



Source: *http://www.noticebored.com*

Statistics for Stolen and Recovered Laptops



Source: *http://articles.techrepublic.com.com/*

Laptop Theft

If a laptop were lost...

- **What information of a strategic nature would be disclosed?**
  Real examples of this type of information include pending mergers, new product intellectual property, strategies and launch plans, and previously undisclosed financial operating results
- **What information of a tactical nature would be disclosed?**
  Examples include private compensation information, plans for organizational changes, proposals to clients, and the myriad of similar information that can be gained from reading a person's email, calendar, contacts, or collection of documents and spreadsheets

Laptop Theft (cont'd)

If a laptop were lost...

- **What information about the company's network or computing infrastructure would be revealed that would facilitate an electronic attack?**
  Examples of this type of information include usernames and passwords, dial in numbers, IP addressing schemes, DNS naming conventions, ISPs used, primary email servers, and other networking details related to connecting the laptop to the corporate or Internet environment
- **What personal information about the laptop owner can be obtained?**

Laptop theft: Data Under Loss

The University of California, Berkeley, is warning more than 98,000 people that the theft of a laptop from its graduate school admissions office has exposed their personal information.

An individual stole the computer from the offices of the school's Graduate Division on March 11, the university said in a statement released late Monday. Roughly one-third of the files on the laptop contained names, dates of birth, addresses and Social Security numbers of 98,369 graduate students or graduate-school applicants, it said. The files go back three decades in some cases.

"At this time, the campus has no evidence that personal data were actually retrieved or misused," the university said in the statement.

No incidents of identity theft have been reported related to the incident, it added. However, UC Berkeley is urging affected individuals to consider putting a fraud alert out at credit reporting agencies.

The data loss follows a string of high-profile incidents in which the personal information of U.S. citizens was exposed, notably consumer data broker ChoicePoint's admission that it had been duped into selling personal information on about 150,000 individuals to possible fraudsters.

The incident is the second recent loss of sensitive information at UC Berkeley. In August, an attacker broke into computers there and gained access to 1.4 million database records containing identity data.

Source: http://news.com.com

15 February 2008

Patient data lost in hospital laptop theft

IDG staff

Snatched computer holds more than 5,000 records

A laptop holding more than 5,000 patient records has been taken from the outpatients department of a Midlands hospital, the Press Association has reported.

The laptop was taken from the outpatients department at Russells Hall Hospital in Dudley in early January. The hospital has confirmed it contains a database with information on 5,123 patients with a blood disorder.

Affected patients have been sent letters warning that their personal details have been stolen and West Midlands police have launched an investigation.

As well as medical data, the stolen records include names, addresses and birth dates. It is understood the data was password-protected but not encrypted.

Trust chief executive Paul Farenden said the laptop, a Fujitsu Siemens C Series Lifebook, had not been fitted with a new data security system currently being implemented by the hospital.

Source: *http://www.cio.co.uk/*

Laptop Security Tools

Steel Cable Locks

Anti-Theft Tags

Tracking & Recovery Systems

www.computersecurity.com

Portable Laptop Carts

Laptop Locker

Laptop Tie-Down Brackets

Laptop Tracker - XTool Computer Tracker

What happens when your computer has been lost or stolen?

Don't you wish your computer could call you and tell you it's location?

This signature software based transmitter secretly sends a signal to the Stealth Signal Control Center via a telephone or Internet connection, to track its location when lost or stolen

Each signal received by the Control Center provides enough information to track the location of the computer in case of a loss or theft

Source: *www.computersecurity.com*

Tools to Locate Stolen Laptops

These are programs that will report the location of a stolen laptop

They work when the laptop connects to the Internet

Ztrace Gold

- www.ztrace.com

CyberAngel

- www.sentryinc.com

ComputracePlus

- www.computrace.com

Stop's Unique, Tamper-proof Patented Plate

STOP places "Stolen Property" and a toll-free number for verification and anti-theft information

This tattoo cannot be removed by any means without marking or defacing the case, and the police and resellers recognize such a mark as a telltale sign that the property is stolen

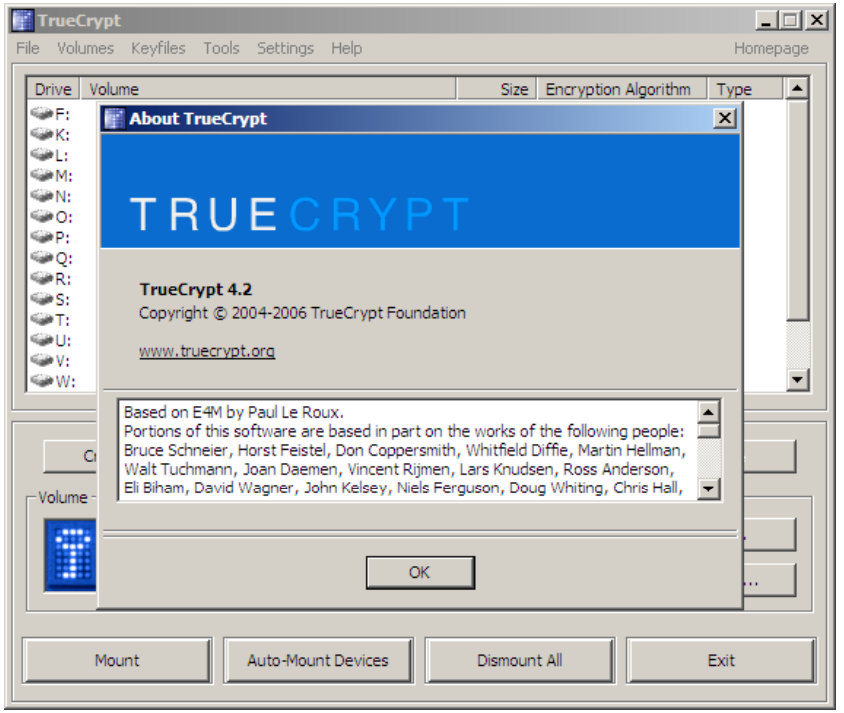
Source: *http://www.securitygroupintl.com/*

Tool: TrueCrypt

TrueCrypt is a software system for establishing and maintaining an on-the-fly-encrypted volume (data storage device)

On-the-fly encryption means that data is automatically encrypted or decrypted right before they are loaded or saved, without any user's intervention

It is a free open source tool



Source: *www.truecrypt.org*

Laptop Security Countermeasures

- Encrypt sensitive data
- Back up everything on the laptop
- Trace a stolen laptop's location
- Set BIOS password on the laptop
- Consider laptop PC insurance
- Add third-party privacy protection for highly sensitive data
- Use physical Kensington Locks
- Use strong hardware-based security

Mantrap

Mantrap provides alternate access for resources

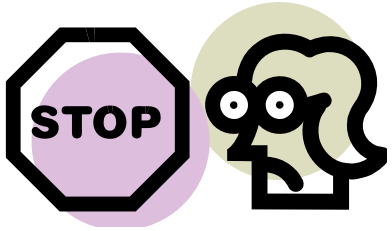
It consists of two separate doors with an *airlock* in between

It restricts access to the secure areas

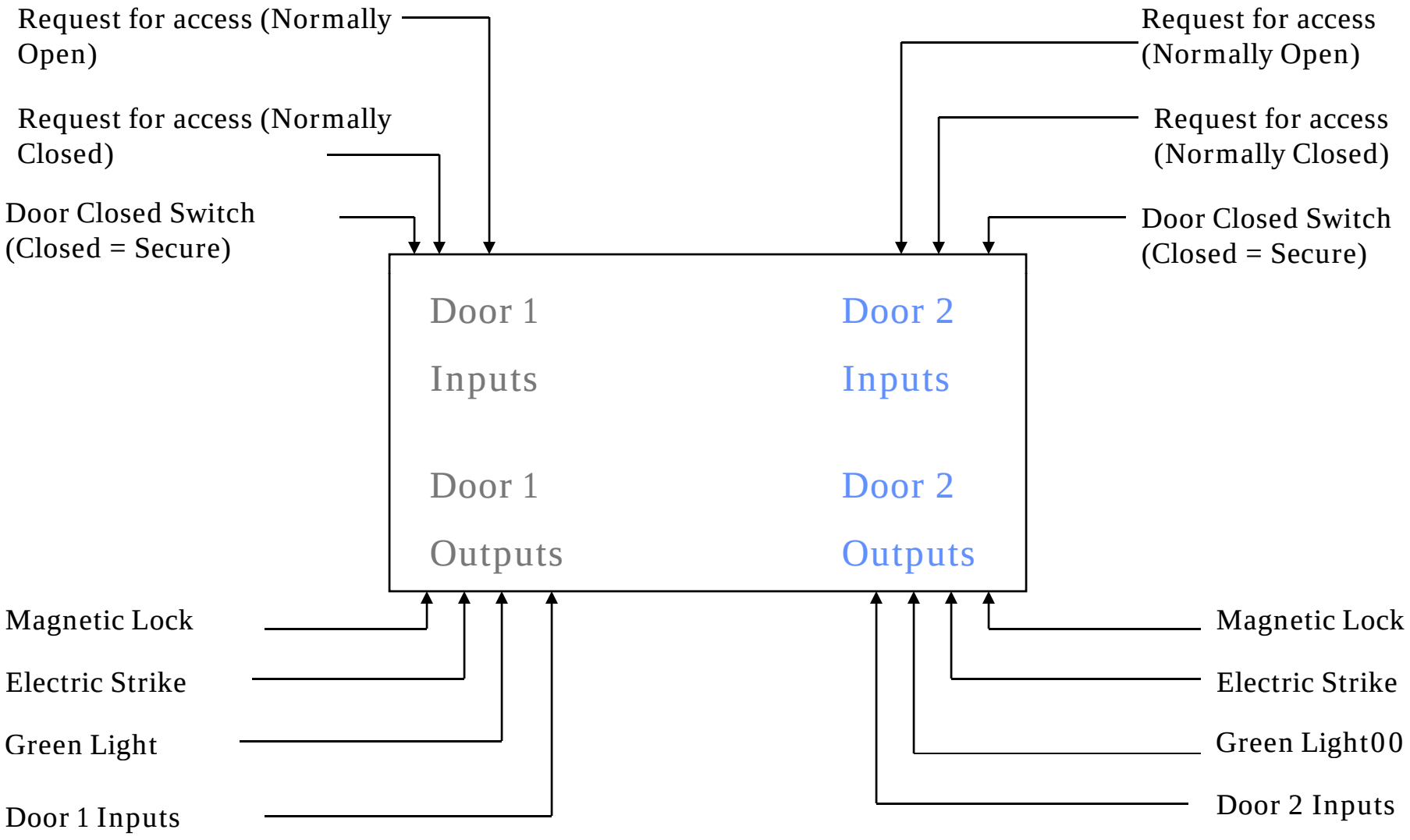
It permits users to enter the first door and requires authentication access to exit from the second door

Security is provided in three ways:

- Pose difficulty in intruding into a single door
- Evaluates a person before discharging
- Permits only one user at a time



Mantrap: Diagrammatical Representation



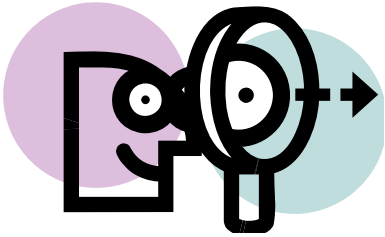
TEMPEST

TEMPEST refers to Transient Electro Magnetic Pulse Emanation Surveillance Technology

Technology for monitoring the devices that emit electromagnetic radiations

Sources of TEMPEST

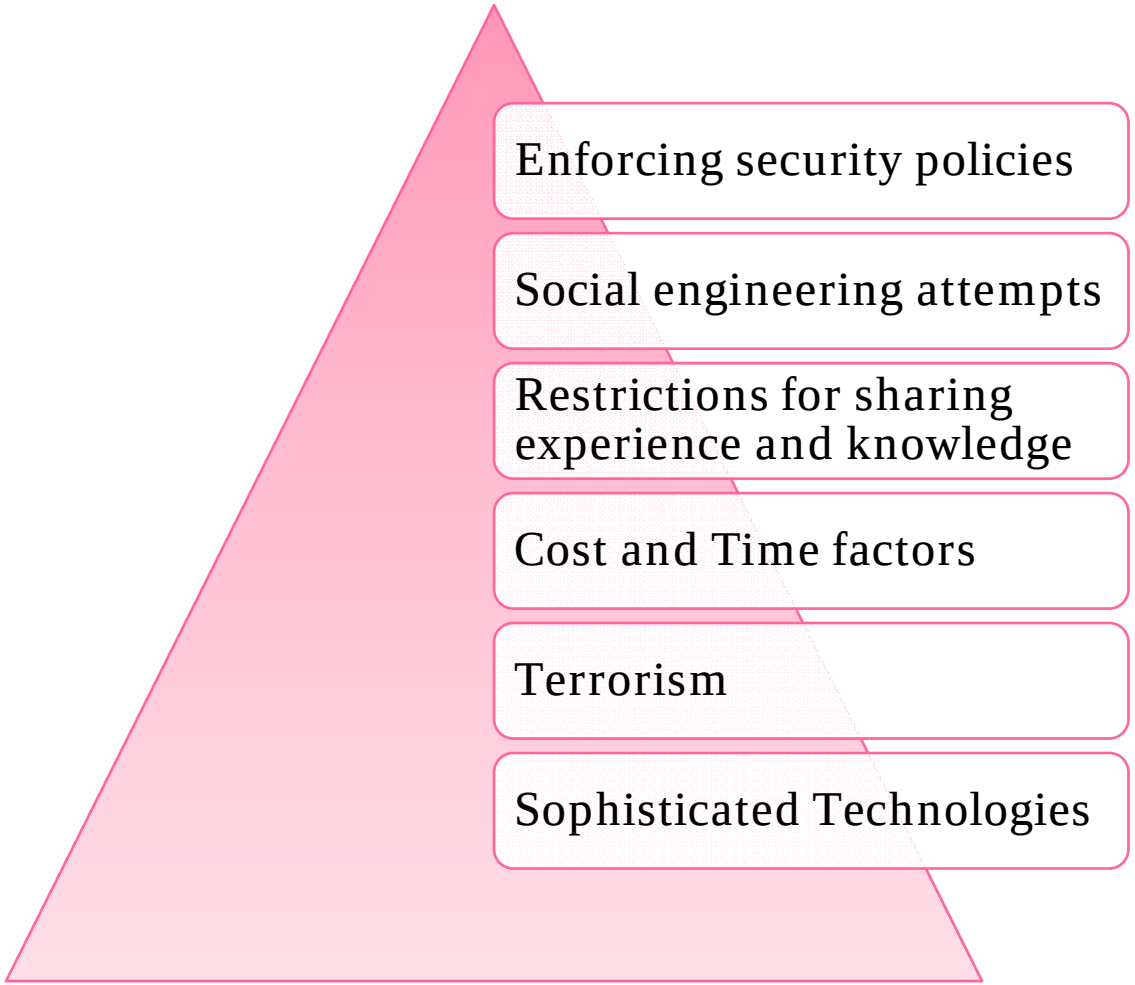
- Functional Sources
  - Generates electromagnetic energy like oscillators and signal generators
- Incidental Sources
  - Do not generate electromagnetic energy such as electromechanical switches and brush-type motors



Types of TEMPEST

- RED Baseband Signals
- Modulated Spurious Carriers
- Impulsive Emanations

Challenges in Ensuring Physical Security



Spyware Technologies

Hidden cameras, voice recorders, and spy cameras carried by your employees can defeat your physical security policy

Categories

- Video Recorders
- Audio Devices
- Bug Detectors
- Home Security
- Spy Gear

Spying Devices

Spy Glasses

Lock Pick Set

Night vision Camera

Spy Camera

Spying Devices (cont'd)

Hibben Claw

Spray to see things

GPS Tracking

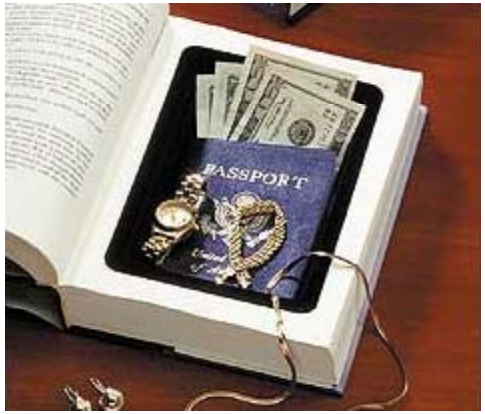
Writes invisibly

Spying Devices (cont'd)

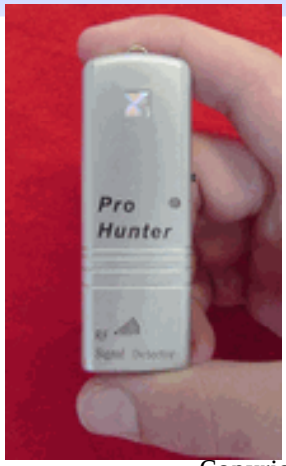
Voice Recorders

Voice Changer

Can Safe and Book Safe



To detect Spy cameras



Spying Devices (cont'd)

Spying Camera

Spy camera hidden inside a ceiling fan

Phishing Intrusion Cell

Physical Security: Lock Down USB Ports

Sometimes, it may not assure guaranteed protection against stealing of data

What if the intruder carries his own USB memory sticks and connects them to the computers at their office?

In a fraction of a second, an intruder can steal all the business information needed for establishing his own company where he can get the customer's database

To prevent the above situations, there is a need for the administrator to lock down the USB ports

Administrators secure their networks behind firewalls by:

- Installing email filters on their SMTP servers
- Installing anti-virus software on all client workstations

USB stick can be used to:

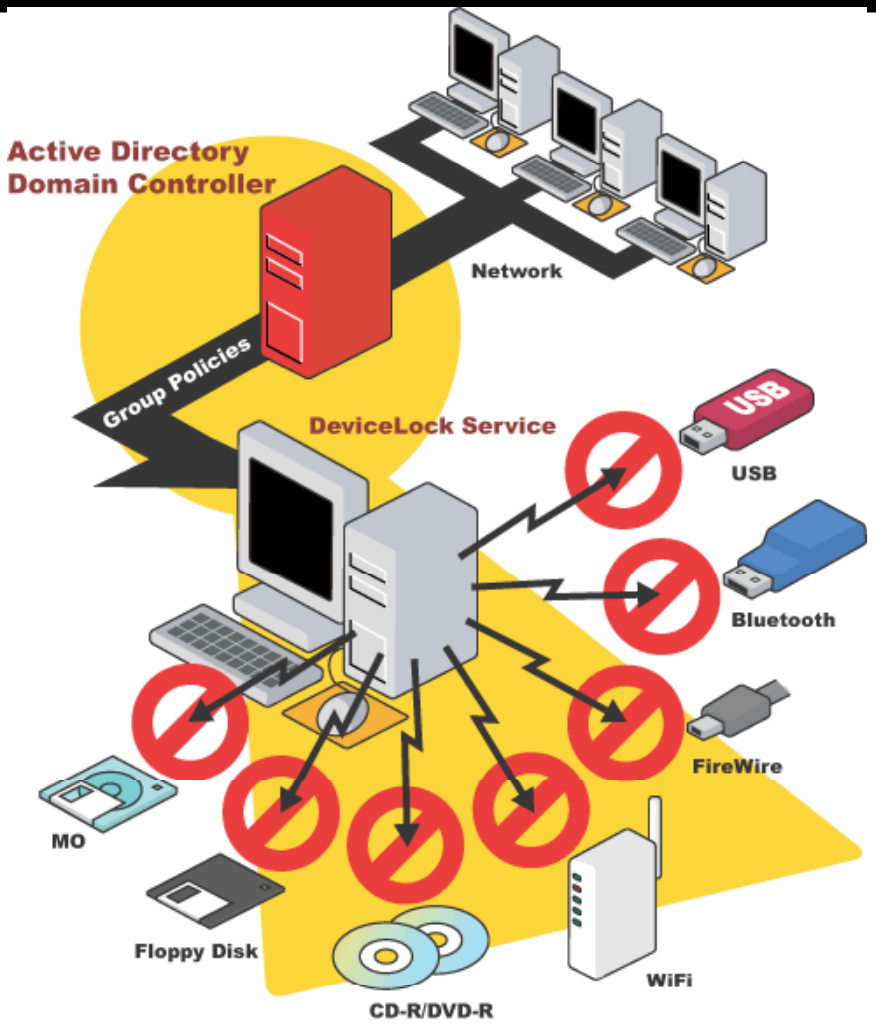
- Hold an entire company's vital data
- Compromise the network with an infected stick

Tool: DeviceLock

Device Lock is a device control solution to safeguard network computers against internal and external attacks

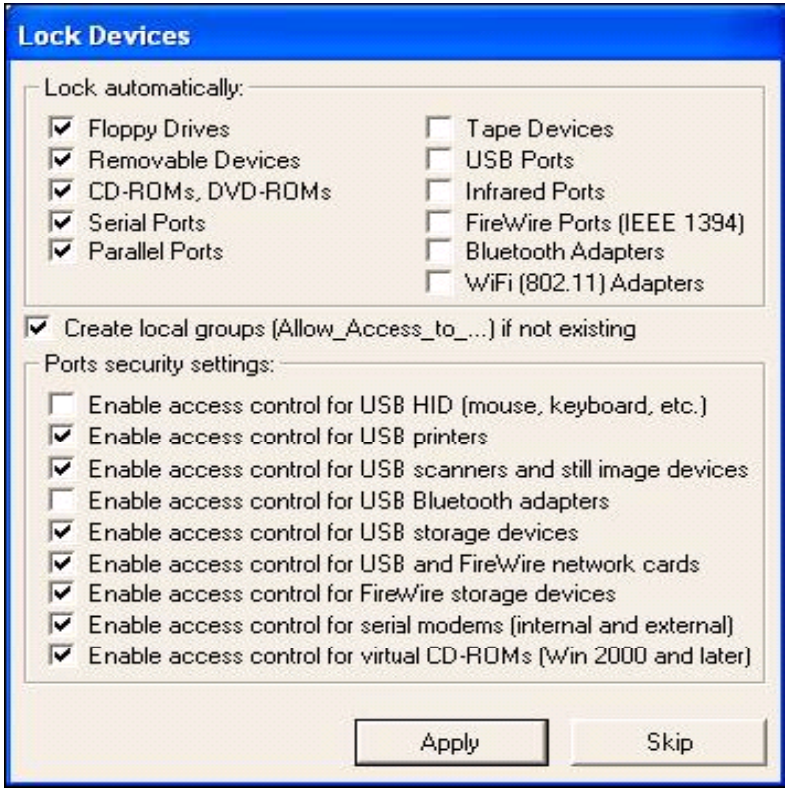
Using Device Lock:

- Network administrators can lock out unauthorized users from USB
- Administrators can control access to any device like floppies, serial and parallel ports, Magneto-Optical disks, CD-ROMs, ZIPs, and USB
- Generate a report concerning the permissions that have been set
- Provide a level of precision control over device resources unavailable
- Grant users temporary access to USB devices when there is no network connection
- Control the system remotely using the centralized management console
- Generate a report displaying the USB, FireWire, and PCMCIA devices



Source: *www.devicelock.com*

Blocking the Use of USB Storage Devices



DeviceLock Screenshots

Track Stick GPS Tracking Device

Track Stick records its own location, time, date, speed, heading, and altitude at preset intervals

It can store months of travel information

It receives signals from 24 satellites orbiting the Earth, where it can calculate its own position anywhere to within 15 meters

Advantages:

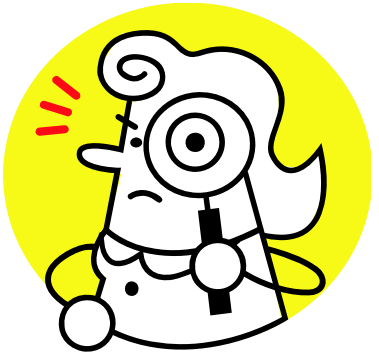
- If the laptop is stolen, this device is able to keep track of its location, so that it is found easily
- Tells you how long the “target” has stayed in one place

What Happened Next

Michael examined organization premises, access control systems, and questioned personnel

He pointed out the following loopholes:

- Poor access control systems
- Absence of monitoring mechanisms
- No dedicated officer looked after physical security matters



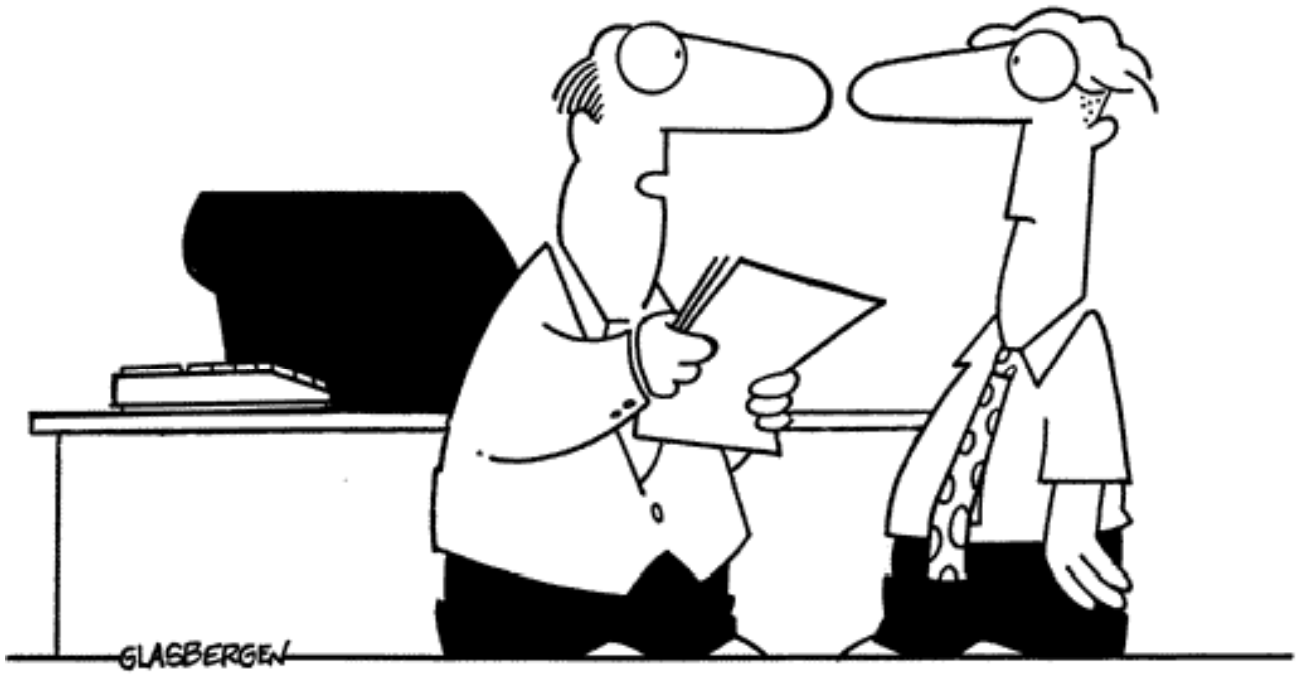
He suggested the following measures:

- Install Biometric and CCTV systems for controlling access to the restricted areas
- Precautionary arrangements for nature caused disasters
- Deployment of physical security officers
- Maintain physical security checklist
- Proper fencing of organization's physical structures

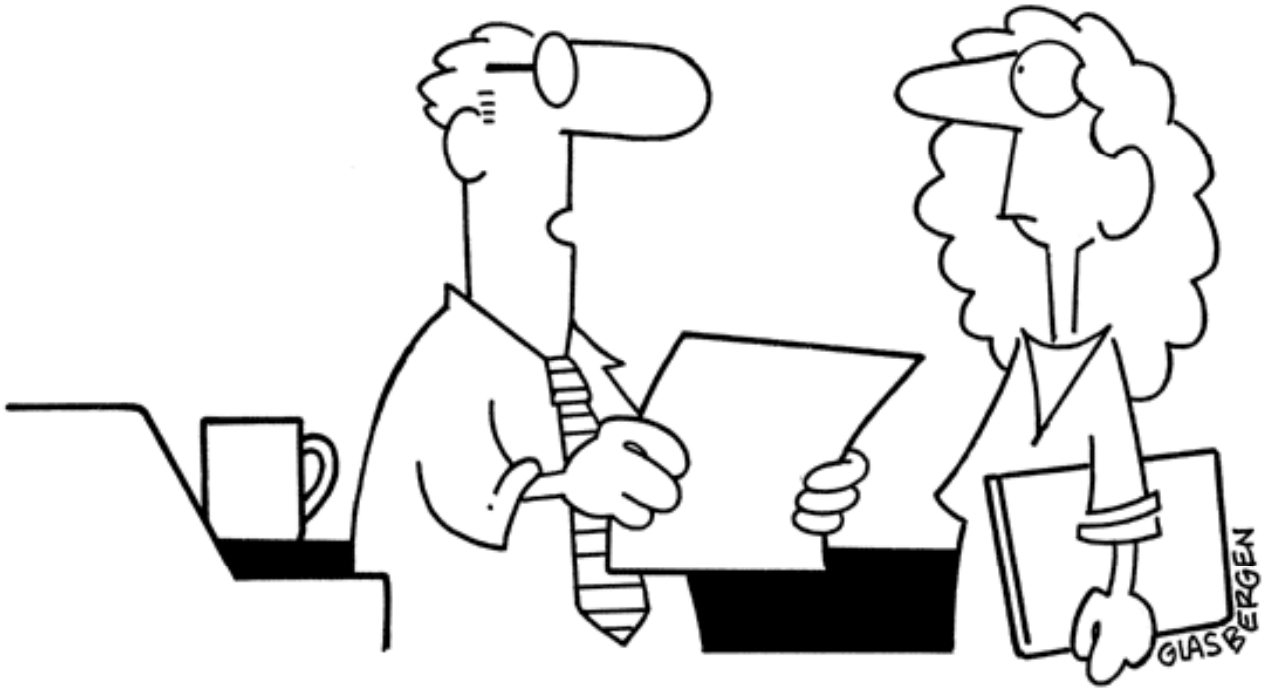
Summary

- Appoint Security officers, who would be accountable for any security breach in a firm
- Device Lock is a device control solution to safeguard the network computers against internal and external attacks
- All organizations should have a checklist for physical security as a part of their security check-ups
- You cannot do anything to prevent natural disasters, but the loss can be decreased substantially if a security policy is properly implemented
- All the employees should take responsibility in handling security issues
- Physical security checklist should be maintained for performing regular checks on physical security
- Biometrics can be used as an effective access control of restricted areas
- Implementation of physical security policy and social engineering tactics are the two big challenges for physical security

"According to new government safety regulations, employees must wear goggles and protective clothing when exposed to sharp criticism or cutting remarks."



"To conform to government safety regulations, no one may climb the ladder of success without wearing a harness and special non-slip shoes."



"New safety regulations won't allow us to think outside of the box anymore because boxes have sharp corners."