Ethical Hacking

Version 5

Module XVII

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 News

Source Courtesy : http://www.securitypark.co.uk/article.asp?articleid=25772&CategoryID=1

Posted in Security News - Access Control - CCTV - Intruder Alarm - Physical Security - Remote Monitoring and Surveillance - Perimeter Protection - on 07/09/2006 RSS

Australian airport uses video analytics system with Artificial Intelligence for airport security

Port Macquarie Airport in Australia is using the latest video analytics system to keep track of events. The system's in-built artificial intelligence actually analyses the airport's video surveillance, instantly alerting airport personnel of any behaviors or activities that appear hazardous or suspicious, whilst ignoring anything that is unimportant.

Port Macquarie Airport is located along the coastal region 420kms north of Sydney, Australia. The airport caters to around 2,500 passengers a week, including scheduled flights to major cities throughout Australia. The airport is also home to aircraft, which are kept at the airport every night.

According to the airport's manager, Lane Dechaineux, it's an extremely busy airport with many third party services using their facilities including air charter operations, flying schools, air freight transport and aerial ambulance operations.

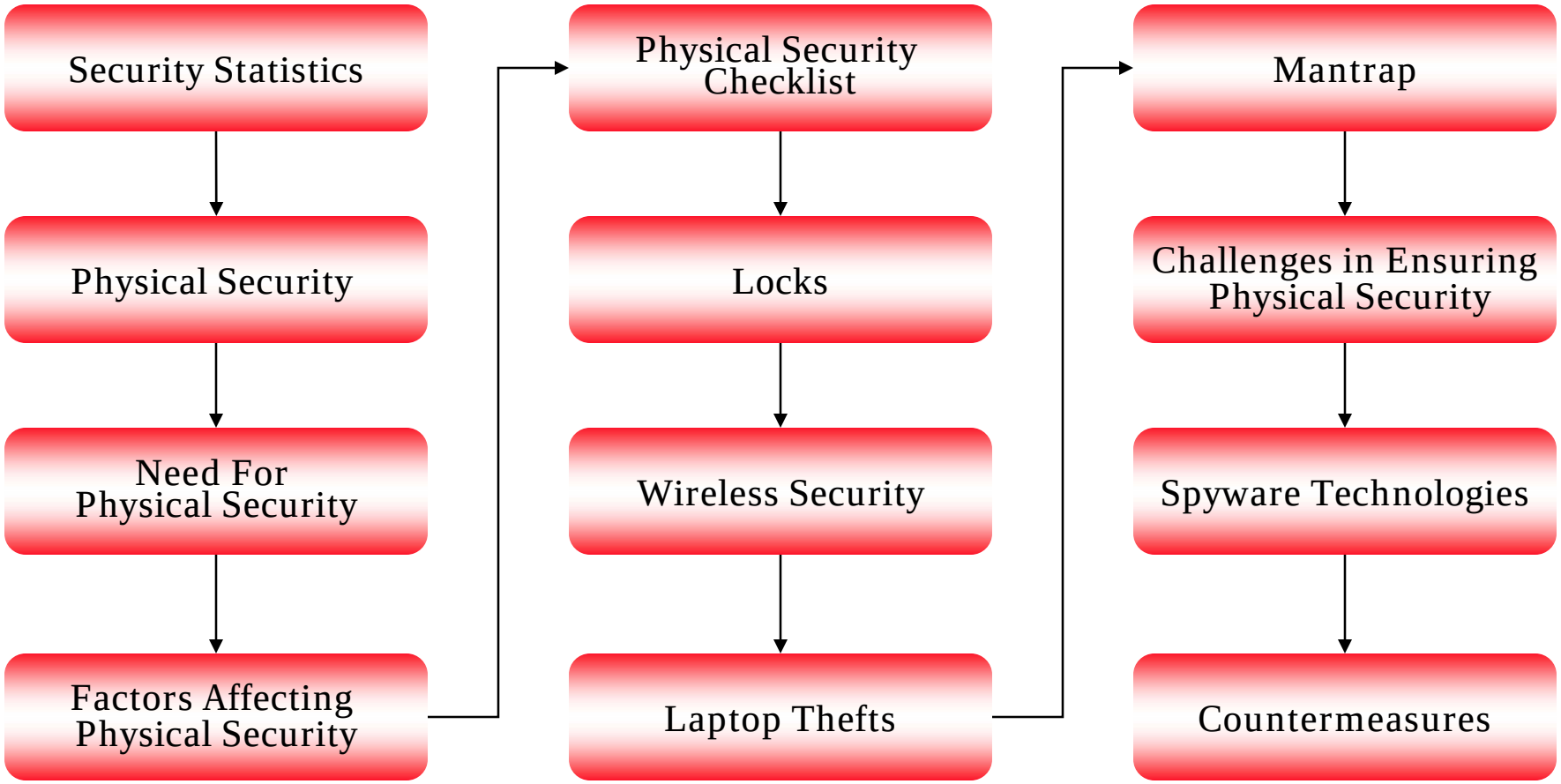
Following the release of the Aviation Transport Security Act outlining airport security procedures, Port Macquarie Airport conducted a risk assessment and it became clear that an upgrade of their entire security system was needed.

Module Objective

This module will familiarize you with the following:

- 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 Statistics

- In the US, during the year 2001, 53 percent more notebooks were stolen than in 2000

  Source: Safeware Insurance Group

- The average financial loss resulting from a laptop theft grew by 44 percent from 2000 to 2001 ($62,000 to $89,000)

  Source: 2001 and 2002 Computer Security Institute/FBI Computer Crime & Security Survey

- Although the laptop's claim to fame is its mobility, according to a recent survey in Support Republic, respondents indicated that laptops were most often lost or stolen on corporate property, not while traveling

- "Across campus, laptop theft is a rising problem, up 37 percent in 2003 from the previous year. For police, the thefts are frustrating because they are difficult to solve and easy to stop" - Yale Daily News, February 12, 04

  Source: TechRepublic, June 4, 2001

Physical Security Breach Incidents

- In 2001, Yasuo Takei, the chairman of Japan's biggest consumer lender Takefuji, was arrested on charges of wiretapping
- In September 2001, a terrorist outfit created havoc in the U.S., and the offices of major firms were physically damaged
- On December 15, 2003, Jesus C. Diaz, who once worked as an AS/400 programmer for Hellmann Worldwide Logistics, was sentenced for one year imprisonment for accessing the company's computer system remotely and deleting critical OS/400 applications
- In the year 2003, a laptop containing the names, addresses, and Social Security numbers of about 43,000 customers, was stolen from the Bank of Rhode Island's principal data-processing provider

Understanding Physical Security

- Since man has had something important to protect, he has 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 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

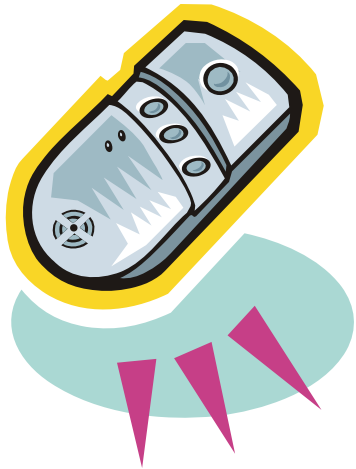
- Describes measures taken to protect personnel, critical assets, and systems against deliberate and accidental threats
- Physical security measures can be
  - Physical
    - Physical measures taken to secure assets e.g. deploying security personnel
  - Technical
    - Measures taken to secure services and elements that support Information Technologies e.g. security for Server rooms
  - Operational
    - Common security measures 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
- The following people should be made accountable for the security of a firm, which includes both physical and information security:
  - The plant's security officer
  - Safety officer
  - Information systems analyst
  - Chief information officer



Factors Affecting Physical Security

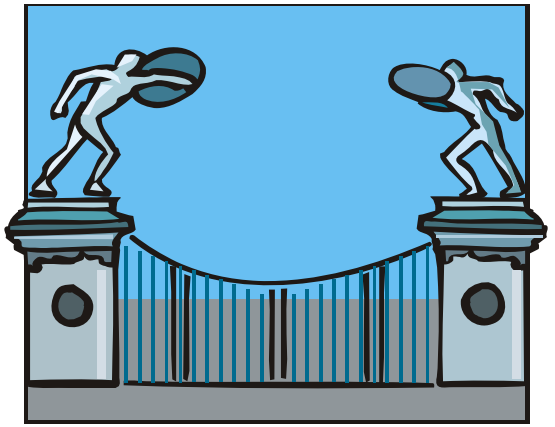
- Following are the factors which affect the physical security of a particular firm:
  - Vandalism
  - Theft
  - Natural calamities:
    - Earthquake
    - Fire
    - Flood
    - Lightning and thunder
  - Dust
  - Water
  - Explosion
  - Terrorist attacks

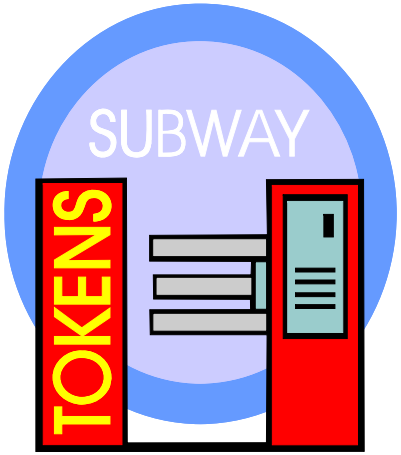
Physical Security Checklist

- 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
- The following is the checklist for securing the company surroundings:
  - Fences
  - Gates
  - Walls
  - Guards
  - Alarms



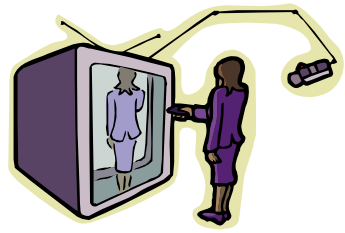


Gates

Security Guards

Physical Security Checklist: Premises

- Premises can be protected by the following:
  - 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 the following:
  - 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 equipment 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
  - Disable booting from the floppy disk and CD-ROM drives on the server or, if possible, avoid having these drives on the server

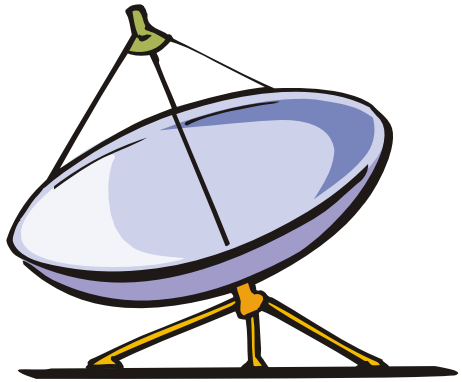
Server Room

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
- The following guidelines should be followed:
  - 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

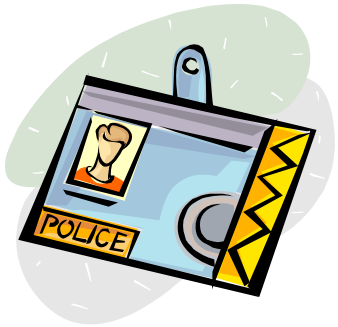


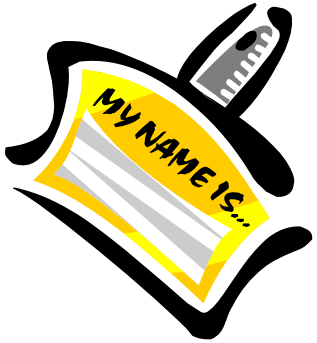
Physical Security Checklist: Other Equipment

- Other equipment, 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

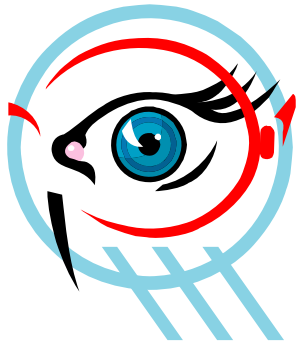
- Access control is used to prevent unauthorized access to any highly sensitive operational areas
- The types of access controls are:
  - Separation of work areas
  - Biometric access control
  - Entry cards
  - Man traps
  - Faculty sign-in procedures
  - Identification badges





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
- The following methods are used by biometric devices for access control:
  - Fingerprints
  - Face scan
  - Iris scan
  - Voice recognition

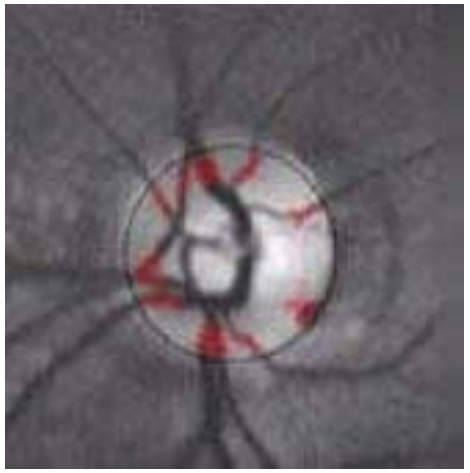


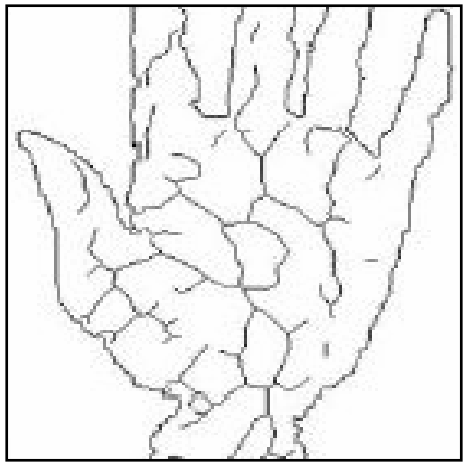
Biometric Identification Techniques

- Physiological Biometric 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



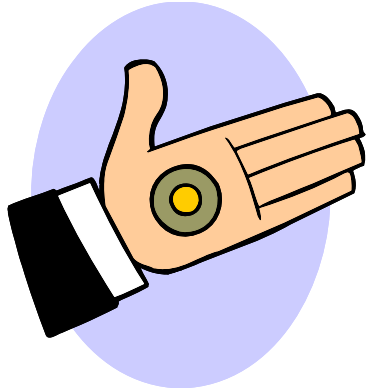


Physical Security Checklist: Smart Cards

- 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

Physical Security Checklist: 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), which authorizes them as the owner of that particular device; the device then displays a number which uniquely identifies the user to the service, allowing them to log in



Physical Security Checklist: 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

Physical Security Checklist: 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: keepla.com/phones.htm

Physical Security Checklist: 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

Lapse of Physical Security

Source: *www.cbsnews.com*

Bank Of America Security Lapse

Personal Information On 1.2 Million Federal Employees Lost

CHARLOTTE, N.C., Feb. 25, 2005

A passer-by exits a Bank of America location in Boston, Friday, Jan. 28, 2005. **(AP)**

(CBS/AP) Bank of America Corp. has lost computer data tapes containing personal information on 1.2 million federal employees, including some members of the U.S. Senate.

The lost data includes Social Security numbers and account information that could make customers of a federal government charge card program vulnerable to identity theft.

Sen. Pat Leahy, D-Vt., is among those senators whose personal information is on the missing tapes, spokeswoman Tracy Schmaler said.

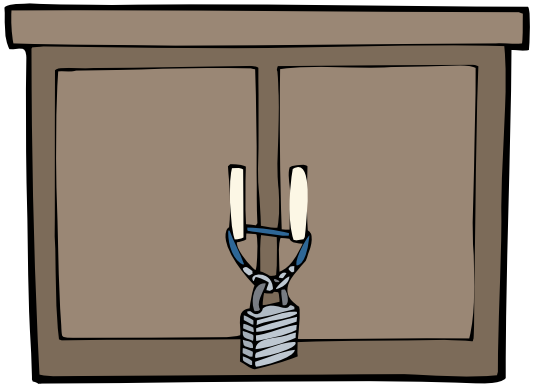
"There were some senators' Visa credit card accounts involved," Schmaler said. "We don't know how many, but he was one of them."

The bank issued an apology.

"We deeply regret this unfortunate incident," said Barbara Desoer, who is in charge of technology, service and fulfillment for the Charlotte-based bank. "The privacy of customer information receives the highest priority at Bank of America, and we take our responsibilities for safeguarding it very seriously."

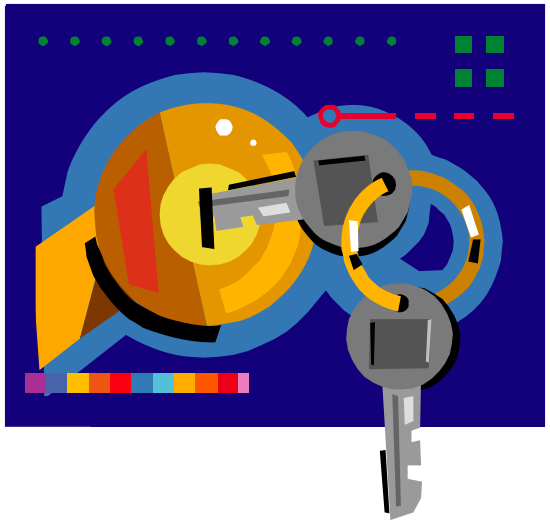
Locks

- 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



Locks (cont'd)

- 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

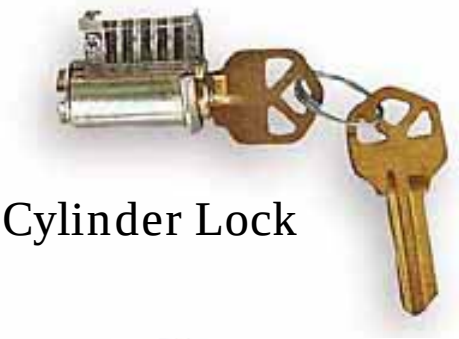
Lock Picking

- The art of unlocking a lock without the use of its key
- Preventing 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

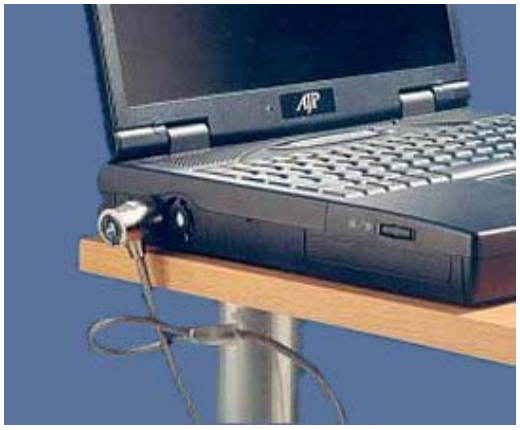
- Hierarchical view to secure information:
  - Password protection / Complex passwords
  - Encrypted File System
  - Anti virus software
  - Firewalls
  - Intrusion detection systems
  - Patches and Updates
  - Lock down unwanted ports / devices

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: Security Statistics

- Medium and large sized companies lose an average of 11.65 notebook computers every year by theft
- Financial losses from unauthorized access of data and theft of proprietary information went up slightly from August 09,2005
- As per the research carried out by Safeware Insurance in 2004, it was found that more than 600,000 laptop thefts occurred in 2004, totaling an estimated $720 million in losses
- As per FBI security research reports
  - 97% of stolen computers are never recovered
  - 73% of companies do not have specific security policies

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

http://news.com.com

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.

CNN.com

PRINT THIS

Powered by Clickability

Click to Print

SAVE THIS | EMAIL THIS | Close

Agency chief: Data on stolen VA laptop may have been erased

WASHINGTON (CNN) -- Thieves may have erased personal data on millions of veterans that was on a laptop they stole, the secretary of veterans affairs said Thursday.

At least, that's the burglars' modus operandi, Secretary James Nicholson said at a hearing before the House Government Reform Committee.

The laptop was stolen in May from the home of a Veterans Affairs employee who, in violation of agency regulations, took it to a private residence.

It contained Social Security numbers, names and addresses for more than 26 million veterans as well as possibly millions of current service members and reservists.

Nicholson said the burglars in this case may have been the same ones who committed similar burglaries in the area. In other cases, information on the computers was quickly erased and the units resold.

"(Authorities) think their M.O. is to take these things, clean them up actually, erase them and fence them into a market for college campuses and high schools," Nicholson told lawmakers, although he admitted authorities could not be certain that was the case with the VA laptop.

He said authorities have apprehended some suspects and recovered some computer equipment, but not the VA laptop.

The incident has led to calls for reform in the Veterans Affairs department.

Nicholson told the committee that the department needs a massive culture change to ensure that staffers follow rules, including policy on protecting information.

"It is too hard, in my opinion, to discipline people in civil service," Nicholson said. "I have multiple examples ... of people in each strata, leadership of the VA, that due to cultural lapses have violated existing policies."

Laptop Security Tools

Steel Cable Locks

Anti-Theft Tags

Stolen Property
1-800-488-STOP

www.computersecurity.com

Tracking & Recovery Systems

Portable Laptop Carts

Laptop Locker

Laptop Tie-Down Brackets

Laptop Tracker - XTool Computer Tracker

http://www.computersecurity.com

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

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

- http://www.securitygroupintl.com/Products/SECOM/STOP/index.html
- 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

Tool: TrueCrypt

www.truecrypt.org

- 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 intervention
- It is a free open source tool

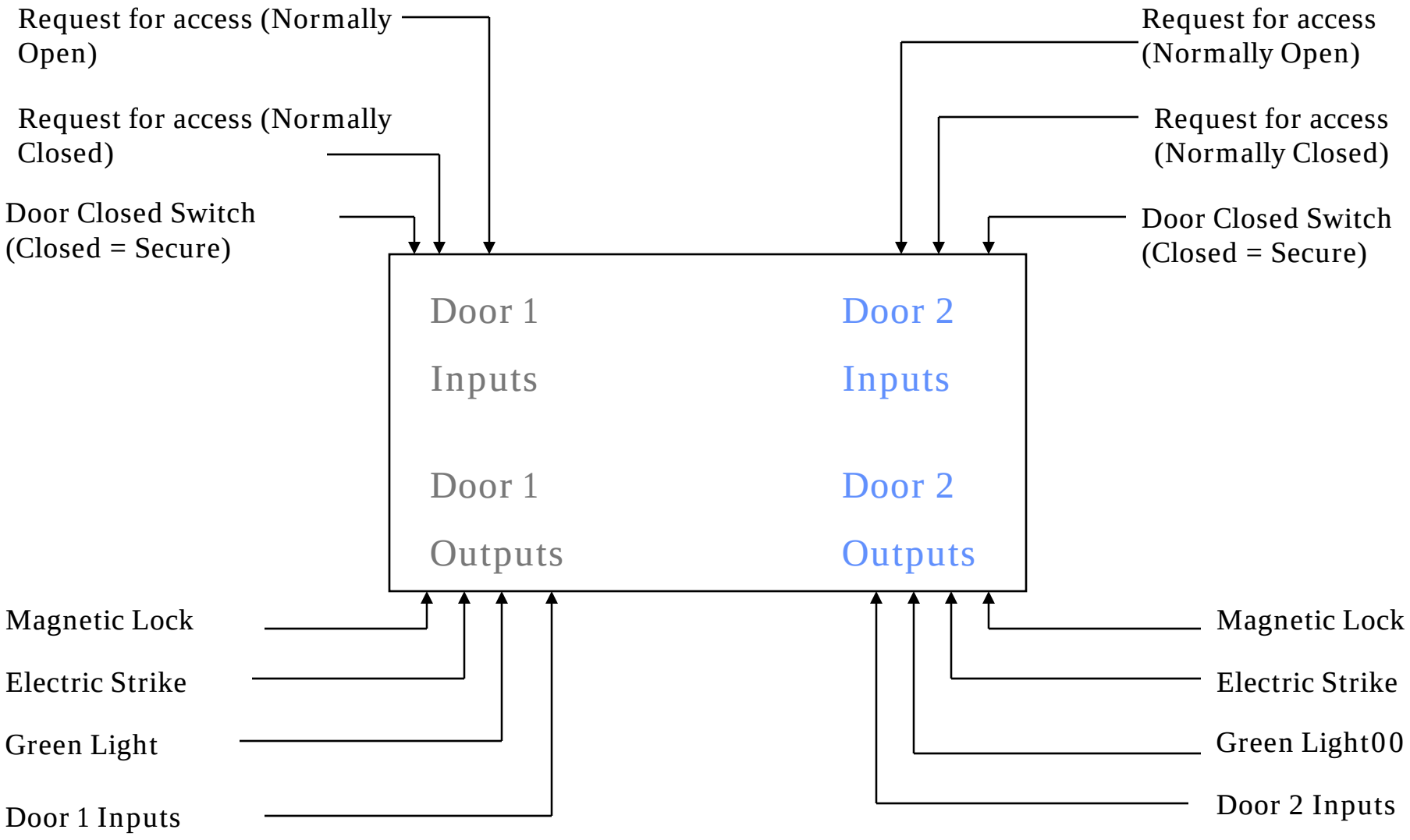
Laptop Security Countermeasures

- 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

- Provides alternate access for resources
- Consists of two separate doors with an *airlock* in between
- Restricts access to secure areas
- 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

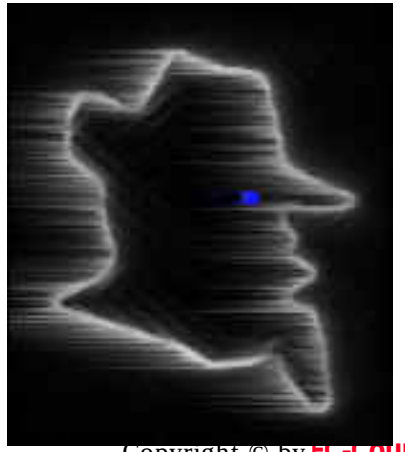
- TEMPEST refers to Transient Electro Magnetic Pulse Emanation Surveillance Technology
- Technology for monitoring the devices that emit electromagnetic radiations
- Sources of TEMPEST
  - Functional Sources
    - Generates electromagnetic energy like oscillators, signal generators
  - Incidental Sources
    - Does 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

- Enforcing security policies
- Social engineering attempts
- Restrictions for sharing experience and knowledge
- Cost and Time factors
- Terrorism
- Sophisticated Technologies

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

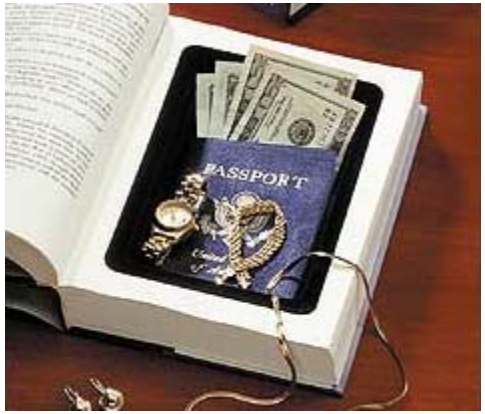
- Writes invisibly

Spying Devices (cont'd)

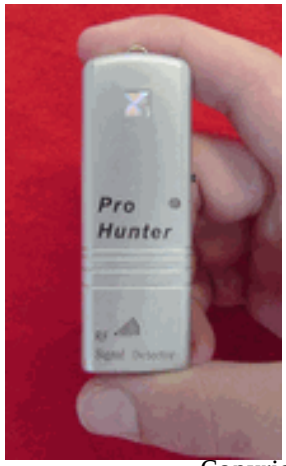
- Voice Recorders

- Voice Changer

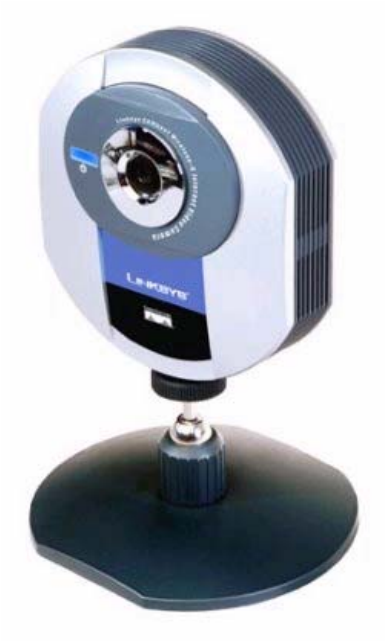
- Can Safe and Book Safe



- To detect Spy cameras



Spying Devices (cont'd)



- Spying Camera

- Spy camera hidden inside a ceiling fan

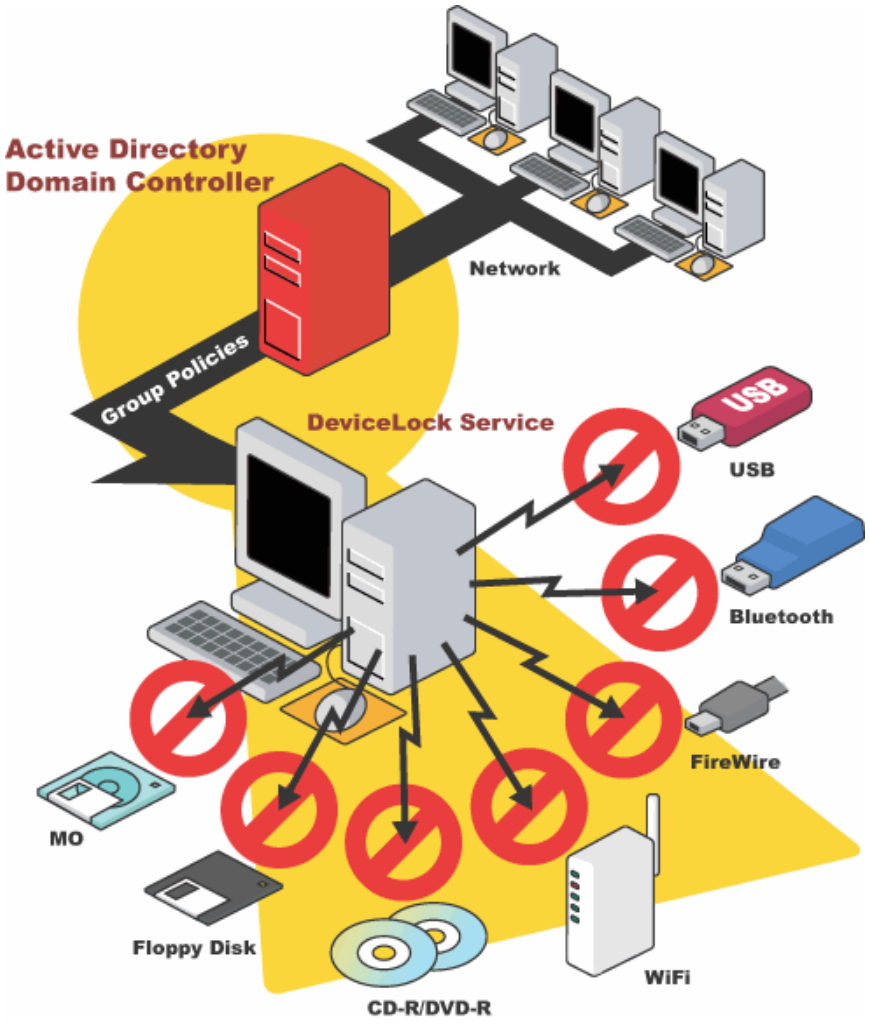
- Phishing Intrusion Cell

Physical Security: Lock Down USB Ports

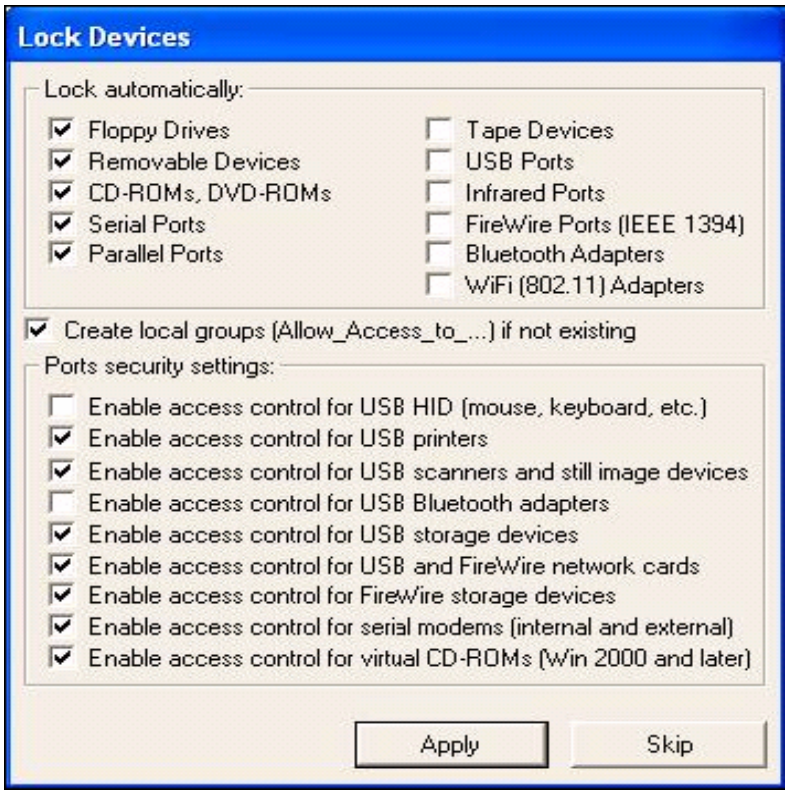
- Administrators secure their networks behind firewalls by
  - installing email filters on their SMTP servers
  - installing anti-virus software on all client workstations
- Sometimes, it may not assure guaranteed protection against the stealing of data
- What if the intruder carries his own USB memory 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 database
- USB stick can be used to:
  - Hold an entire company's vital data
  - Compromise the network with an infected stick
- To prevent the above situations, there is a need for the administrator to lock down the USB ports

Tool: DeviceLock (www.devicelock.com)

- 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, 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



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

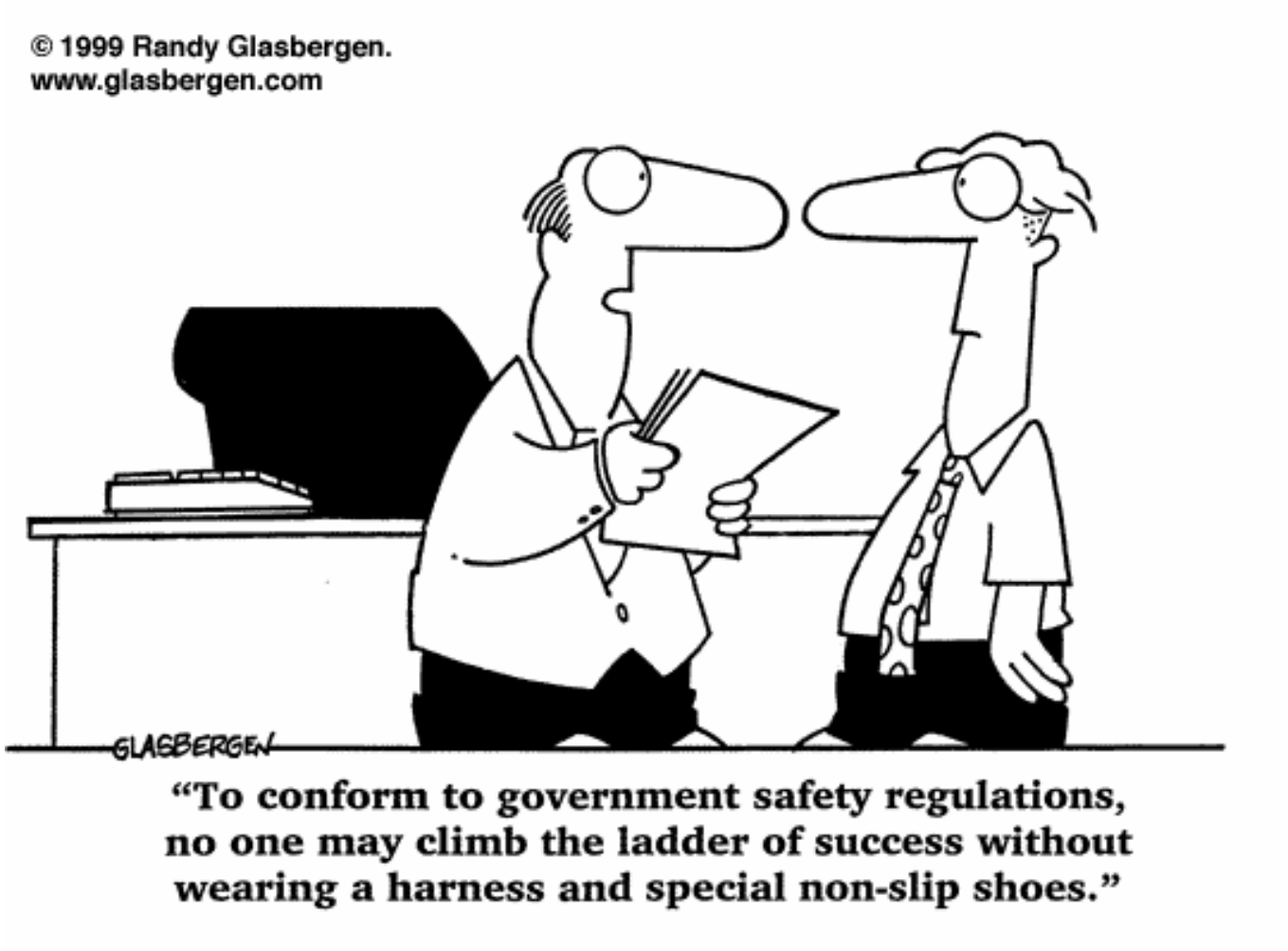
- Poor access control systems
- Absence of Monitoring mechanisms
- No dedicated officer looking after Physical Security matters

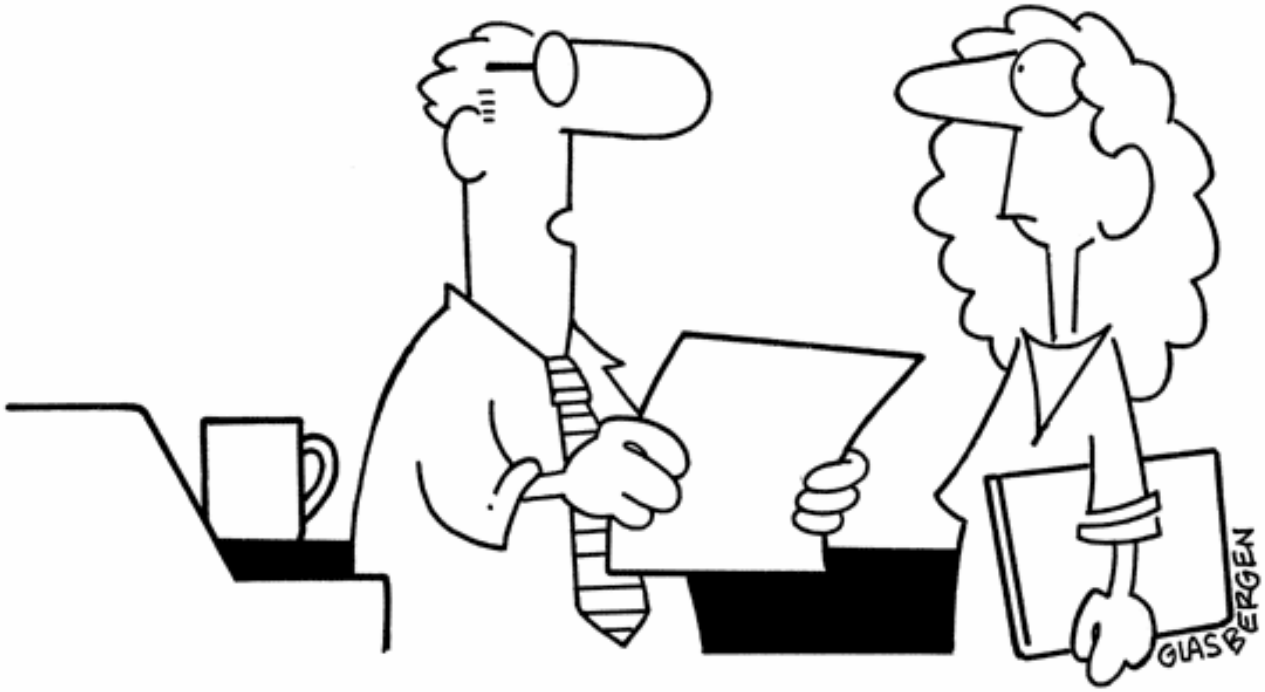
He suggested following measures:

- Install Biometric, CCTV systems for controlling access to restricted areas
- Precautionary arrangements for nature caused disasters
- Deployment of Physical Security officers
- Maintain Physical Security Checklist
- Proper fencing of organization 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





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