MBA9009
E-Security
&
Business Continuity Management

Learning objectives
• Document the rapid rise of computer and network security
• Understand the factors contributing to the rise in EC security breaches
• Basic types of network security attacks
• Risk management system
• Types of attacks against EC systems
• Major technologies for securing EC
• BCM

The need for security
• The variety of attacks
  • Sabotage
  • Theft of proprietary information
  • Penetration from the outside
  • Denial of service
  • Unauthorised access by insiders
  • Employee abuse of Internet service privileges
  • Viruses

• The reporting of serious crimes to law enforcement declined
  • Reasons
    • 52% negative publicity
    • 39% competition will use it against them
    • 13% did not know they could report it

Factors contributing to cyber attacks
• Security systems are only as strong as their weakest points
• Security takes a back seat to market pressure
• Security of EC site depends on the security of the Internet as a whole
• Security vulnerabilities are increasing faster than they can be combated
• Security compromised by common application

Basic security issues
• Authentication
  • The process by which one entity verifies that another entity is who they claim to be
  • Password, Smartcard, signature
• Authorisation
  • The process of establishing whether the person or a program has the right to access particular data, programs, resources, etc.
• Comparing info about the person/program with access control information
• Auditing
• The process of collecting information about accessing particular resources, using particular privileges, etc.
• Confidentiality or privacy
• Information that is private or sensitive should not be disclosed to unauthorized individuals, entities, or computer software
• Integrity
• The ability to protect the data from being altered or destroyed in an unauthorized or accidental manner

• Availability
• A person or a program should be able to gain access to pages, data or services provided by the site when they are needed – real time
• Non-repudiation
• The ability to limit parties from refuting that a legitimate transaction took place

• Security risk management
• Risk management consists of four phases: assessment, planning, implementation and monitoring
• Assessment
• Determine organisational objectives
• Inventory assets
• Delineate threats
• Identify vulnerabilities
• Quantify the value of each risk

• Planning
• Define specific policies
• Establish process for audit and review
• Establish an incident response team and contingency plan
• Implementation
• Monitoring

• Types of threats and attacks
• Non-technical (social engineering)
• A perpetrator uses a form of persuasion to trick people into revealing sensitive information
• Technical
• An expert hacker uses a methodological approach to perpetrate technical attacks
• Steps
• Step1 Discovering the key elements of the network
• Step2 Scanning for vulnerabilities
• Step3 Hacking the system to gain privileges
• Step4 Disabling auditing
• Step5 Stealing files, codes, valuable information
• Step6 Installing back doors and Trojan horses
• Step7 Returning to inflict more damage
- Types of threats and attacks
- System and software bugs and misconfigurations
- Ability to exploit various bugs and flaws in operating systems, web servers, database servers, etc.
- Denial-of-service (DoS) attacks
- Taking advantage of the Internet’s openness to overwhelm a victim site with seemingly legitimate communications.
  - IP fragmentation
  - DNS spoofing
  - Ping of death, etc.

- Malicious code: viruses, worms and Trojan horse
- Virus is a piece of code that inserts itself into a host, and propagate locally
- Can not run independently it requires that the host program be run to activate it.
- Sometimes the execution is triggered by a particular event

- Worm is a program that can run independently, consumes the resources of its host from within and can propagate a complete working version of itself onto another machine
- Trojan horse is a program that appears to have a useful function but also contains a hidden function that presents a security risk
- Back Orifice
- NetBus
- Whack-A-Mole, etc

- Security technologies
- Firewalls
- A network node consisting of both software and hardware that isolates a private network from a public network.
- Have set of rules that determine if the data should be allowed entry
- Is located at at the point of entry where the data attempts to enter the computer from the internet

- Types of firewalls
- Packet filtering routers
- Rules that can accept or reject incoming packets based on source and destination IP addresses
  - Block any packet coming from a given IP address
- Application-level proxy
- Any request coming from unsupported proxy service is blocked by the firewall
• Virtual Private Networks
• Uses the public Internet to carry information but remains private by using a combination of:
• Encryption to scramble the communication
• Authentication to ensure that the information has not been tampered with and comes from a legitimate source
• Access control to verify the identity of anyone using the network

• Intrusion Detection Systems (IDS)
• It is a software that can monitor activity across a network or on a host computer, watch a suspicious activity, and take automated action based on what it sees.
• Host based IDS
  – resides on the server that is being monitored
• Network based IDS
  – usually consists of a monitor (a software package that scans the network) and software agents that reside on various host computers and feed information back to the monitor

• Managerial issues
• Recognise the business consequences of poor security
• Security through obscurity doesn’t work
• It’s the business that counts not the technology
• Security is an ongoing, closed loop process
• Internal breaches are more prevalent than external

• Business Continuity Plan (BCP)
• A plan to get a company “up and running” as soon as possible after any sort of disaster.
• A company must identify critical processes and put plans in place to ensure that these processes can be resumed as quickly as possible.
• The plan includes all aspects of a company’s business, not just the information technology (IT) department

• Business Continuity Management
• All sections of a business ‘own’ the BCP
• Business continuity management is everyone’s responsibility
• Insurance is not enough!
• designed to cover specific consequential losses, such as new equipment and recovery of lost revenue
• claims may take time to process and it may not be possible to replace specialised equipment straightaway

• Disaster
• Any event that interrupts the normal business of an organisation and prevents it from delivering products and services to its customers for an unacceptable period of time.
• Natural disasters (such as floods and lightning strikes)
• Deliberate acts (such as terrorist activity)
• Accidents (for instance, accidental cutting of electrical cables).
BCM and E-Business

- Increasing use of the Internet for business has brought new problems for business continuity
- The scope of disasters has widened with the greater use of technology
  - Vulnerability is now a supply chain issue
- Any interruption in service is immediately obvious to customers
  - Competitors have an immediate opportunity to fill the gap

Spending on BCM

- Awareness has increased generally and there is some evidence that more resources are being put into BCM
- However, it is still seen in many instances as a discretionary expenditure
- It can be the first to have its budget cut during a cost cutting exercise
- It suffers from a “it won’t happen to us” attitude in many instances

Significant Events in BCM

- Year 2000 (Y2K)
  - provided an impetus to look at the risks faced and how they could be dealt with
  - Raised the visibility of BCM as not just as a matter of recovering from a computer failure, but as a need for contingencies for how all work is carried out
  - Some plans were put aside after Y2K passed with little event

- September 11, 2001
  - Buildings surrounding the WTC were also severely damaged
  - So swift and devastating that some businesses located in the WTC had no chance of carrying out a BCP, however well it had been tested
  - Again: insurance did not help in the short term
  - Many businesses had underestimated the effects of a disaster

Recent Lessons

- Some plans failed because they were written on the assumption that any incident would only affect an individual building
- Plans that were too detailed were often less effective
- Many organisations need to be more realistic about what is actually possible in the aftermath of a disaster
  - Access to computers? telephones? transport?
- Key employees may be unable to cope with the emotional trauma of the disaster and may not be able to carry out their assigned duties

Expanded View of BCM

- As stated earlier, BCM is more than just recovering PCs and networks
  - This is a shift in viewpoint from the early 1990s
  - Covers all aspects of the business, including
    - Employees
    - Supply chain partners