INFORMATION SECURITY

S. K. D. Biswas

Guest Lecture delivered at BIC Workshop, JBTDRC, Sept.-Oct. 2003

Information Security

S.K.Dey Biswas
Indian Council of Medical Research
New Delhi

1

Information- The three pillars

- Availability
- Integrity
- Confidentiality

2

The need for security

On the internet, information you send from one computer to another passes through numerous systems before reaching its destination. Normally, the users of these intermediary systems don't monitor the Internet traffic routed through them, but someone who's determined can intercept and eavesdrop on your private conversations or credit card exchanges. Worse still, they might replace your information with their own and send it back on its way.

Due to the architecture of the Internet and intranets, there will always be ways for for unscrupulous people to intercept and replace the data in transit. Information may be stolen, but there may be no trace of the theft, nothing is physically missing.

3

Security in an organization

- Physical Security
- Internal Access Security
- External Access Security

4

Physical Security

- Are the computers accessible only to those authorized to do so?
- Are the infrastructure components (hubs, switches, routers) kept in secure areas controlled in some way?
- Is there any way to track who has access to these devices and when they have used that access?
- Are these measures in place to prevent someone from removing computers or other devices from the organization premises?

5

Internal Access Security

- What are the administrative levels at which employees are granted different levels of system and data access?
- What are the procedures for determining and granting an appropriate access level to each employee?
- What procedures exist to determine if an employee has been granted greater than is appropriate?
- What procedures are in place to determine successful and unsuccessful attempts to exercise inappropriate access level?

6

External Access Security

Areas of concern:

- Internet connections
- Dial in servers
- Connections to public carriers
- Connections to external networks owned by partners, suppliers or clients

7

External Access Security

- Where are the internal network potentially vulnerable to unauthorized access?
- What methods have been employed to prevent unauthorized access in these areas?
- What methods are in place to identify unauthorized access attempts to alert the appropriate people?
- What methods are in place to identify the source of unauthorized access attempts?

8

How do I protect my data?

Encryption & Digital certificates used together protect the data as it travels over the Internet.

Encryption is the process of using a mathematical algorithm to transform into a format that can't be read (this format is called cipher text)

Decryption is the process of another algorithm to transform encrypted information back into readable format (this format is plain text)

Digital certificates are the digital passport, an Internet ID. They are the verification of identity and the integrity of the data.

9

Data Protection

Combined encryption and digital certificates protects and secures data in the following ways:

Authentication: This is digital verification of identity. With digital signatures and certificates, the proof of identification is digitally encoded into the e-mail.

Integrity: Verification that the data sent has not been altered.

Encryption: This ensures that the data was unable to be read or utilized by any party while in transit

Token verification: Digital tokens replace the password

10

Viruses

A virus is a program that runs when an infected program is executed, usually only executable files with extensions like .EXE, .BAT, .COM and .SYS can become infected.

Viruses can be acquired from the network, downloaded files, shareware and freeware programs, or even off-the shelf software.

Virus scanners and virus shields are two types of devices that protect your system.

Virus scanners do a thorough job of inspecting whatever files are selected, they attempt to find and remove any viruses that may be detected.

Virus shield is a program that runs when the system boots and keeps running in memory the entire time the system is on.

11

Need of an IT policy

1. What are the information assets of an organization in terms of hardware and software, including network as well as the future investment plan in IT/IS
2. What is the organization's dependence on IT in real measurable terms like financial benefits, better service to clients, improved image and market share.
3. How much the organization will suffer due to any loss, leakage or distortion of information

The analysis should be very dispassionate and realistic

12

Risk assessment

? Business risks

? Physical risks

? Environmental risks

? Technological risks

? Human risks

? Other risks

13

Risk mitigation

- Administrative measures
- Physical measures
- Technical measures

14

Administrative measures

- Policies
- Procedures
- Standards and guidelines
- Personnel screening
- Security awareness training

15

Physical measures

- Perimeter control measures
- Physical access control
- Intruder detection
- Fire protection
- Environmental monitoring

16

Technical measures

- Logical access control
- Network access controls
- Identification and authentication devices
- Data encryption

17

Anatomy of a Policy document

- **Policy statement**: Outline the objective of the policy. Emphasize the actual risks that will be addressed. Necessity of the policy
- **Policy scope**: Specify the areas of concern that the policy will address. Will list the organizational units, individuals and technical system covered by the policy
- **Validity**: Define the life span of the policy and when it will be reviewed next
- **Owner**: Author of the policy should be a respected IS professional. This will ensure responsibility and accountability
- **Review details**: Record of previous review and the changes
- **Compliance requirements**: Punitive actions that should be taken if the policy is not adhered to. Name the persons who will enforce these policies

18

Anatomy of a Policy document

- **Policy details**: Specific issues that the policy is addressing:Give the background, describe the risks that have been identified, state the security expectations that the policy will fulfill
- **Best practices**: Detailed list of the best practices
- **Mandatory practices**: The minimum standard that has to be implemented
- **Procedure for implementation**: Step by step procedure which will be followed for the implementation of the policy. There will be references to forms, templates, standards, guidelines etc. Monitoring and reporting mechanism to ensure proper implementation. How compliance will be monitored. How non compliance will be reported and what actions would be taken
- **Annexure**: Forms, templates, standards, technical guidelines

19

Policies

- **Natural and Environmental threats:** Disaster recovery, Backup and recovery, WAN recovery
- **Human threats**: Password security & controls, Internet access and security
- **Email security**: Technical controls, Logical access controls, Program change controls, version controls, application software security
- **Database security**: Network and Telecommunication security
- **Operating systems security**: Firewall, Data classification, Web server security, Intranet security, Virus-Protection, E-commerce security, Data encryption
- **Administrative controls**: Physical security, Incidence response management, punitive actions

20

The BS 7799 Standard

The British Standards Institute (BSI) has established a standard for Information Security Management System (ISMS)

The BS 7799 standard comprises of two parts:

1. Code of Practice for Information security management
2. Specifications of Information Security Management systems

21

ISO17799

ISO has adapted the BS7799 Part 1 and numbered it as ISO 17799. This only provides Code of Practice and as such provides only guidelines. ISO has not yet adopted Part 2 so there are no specifications, which an implementer or an auditor can refer to.

22