LNMIIT
The LNM Institute of Information Technology

Security Management

Classroom Code:o7l60yk

LNMIIT
The LNM Institute of Information Technology

Outline

- Security Policy
- Risk Analysis
- Physical threats and controls

LNMIIT
The LNM Institute of Information Technology

Security Policy

- **A security policy is a high-level statement of purpose and intent.**

- **A security policy documents an organization's security needs and priorities.**

LNMIIT
The LNM Institute of Information Technology

Most Precious Asset

- What does an organization consider its most precious asset?
- For pharmaceutical company scientific research on new drugs and its sales and marketing strategy are its most important assets.
- A hospital would likely find protecting the confidentiality of its patients' records most crucial.
- A television studio could decide its archive of previous broadcasts is most important.

LNMIIT
The LNM Institute of Information Technology

Most Precious Asset

- An online merchant might value highly its web presence, and the associated back-end order receiving and processing system.
- A securities trading firm would be most concerned with the accuracy and completeness of its transaction records, including its log of executed trades.
- As you can see, organizations value different things, the most significant threats will differ among organizations.
- In some cases confidentiality is paramount, but in others availability or integrity matters most.

Policy Statement

LNMIIT
The LNM Institute of Information Technology

- There are trade-offs among the strength of the security, the cost, the inconvenience to users, and more. For example, we must decide
- whether to implement very stringent—and possibly unpopular—controls that prevent all security problems.
- OR simply mitigate the effects of security breaches once they happen.

Policy Statement

LNMIIT
The LNM Institute of Information Technology

So the policy statement must answer three essential questions:

- ***Who* should be allowed access?**
- **To what system and organizational *resources* should access be allowed?**
- **What *types* of access should each user be allowed for each resource?**

Policy Statement

LNMIIT
The LNM Institute of Information Technology

- **The policy statement should specify the following:**
- **The organization's *goals* on security**. For example,
- should the system protect data from leakage to outsiders,
- protect against loss of data due to physical disaster,
- protect the data's integrity, or
- protect against loss of business when computing resources fail?
- What is the higher priority: serving customers or securing data?

Policy Statement

LNMIIT
The LNM Institute of Information Technology

- The policy statement should specify following:
- **Where the *responsibility* for security lies.**
  - For example, should the responsibility rest with a small computer security group, with each employee, or with relevant managers?
- **The organization's *commitment* to security.**
  - For example, who provides security support for staff, and where does security fit into the organization's structure?

Risk Analysis

- A **risk** is a potential problem that the system or its users may experience.
- We distinguish a risk from other project events by looking for three things:
- *A loss associated with an event*. The event must generate a negative effect: compromised security, lost time, diminished quality, lost money, lost control, lost understanding, and so on. This loss is called the **risk impact**.

Risk Analysis

- *The likelihood that the event will occur*. The probability of occurrence associated with each risk is measured from 0 (impossible) to 1 (certain). When the risk probability is 1, we say we have a problem.
- *The degree to which we can change the outcome*. We must determine what, if anything, we can do to avoid the impact or at least reduce its effects. **Risk control** involves a set of actions to reduce or eliminate the risk.

Risk Analysis

Risk analysis

- is an organized process for identifying the most significant risks in a computing environment,
- determining the impact of those risks, and
- weighing the desirability of applying various controls against those risks.

Risk Analysis

- We usually want to weigh the pros and cons of different actions we can take to address each risk. To that end, we can quantify the effects of a risk by multiplying the risk impact by the risk probability, yielding the **risk exposure**.
- For example, if the likelihood of virus attack is 0.3 and the cost to clean up the affected files is $10,000, then the risk exposure is $3,000. So we can use a calculation like this one to decide that a virus checker is worth an investment of $100, since it will prevent a much larger expected potential loss.

LNMIIT
The LNM Institute of Information Technology

Risk Analysis

- Risk is inevitable in life: We can identify, limit, avoid, or transfer risk but we can seldom eliminate it. We have three strategies for dealing with risk:
- ***avoid*** the risk by changing requirements for security or other system characteristics
- ***transfer*** the risk by allocating the risk to other systems, people, organizations, or assets; or by buying insurance to cover any financial loss should the risk become a reality
- ***assume*** the risk by accepting it, controlling it with available resources and preparing to deal with the loss if it occurs

LNMIIT
The LNM Institute of Information Technology

Risk Leverage

- The costs are associated not only with the risk's potential impact but also with reducing it.
- **Risk leverage** is the difference in risk exposure divided by the cost of reducing the risk.

$$\frac{\text{(risk exposure before reduction) – (risk exposure after reduction)}}{\text{(cost of risk reduction)}}$$

- A risk reduction of $100 for a cost of $10, a 10:1 reduction, is quite a favorable result.
- If the leverage value of a proposed action is not high enough, then we look for alternative but less costly actions or more effective reduction techniques.
- **Risk leverage is The leverage measures value for money spent** OR **Risk leverage is the amount of benefit per unit spent.**

Risk Analysis

- **Risk analysis** is the process of examining a system and its operational context to determine possible exposures and the potential harm they can cause.
- Thus, the first step in a risk analysis is to identify and list all exposures in the computing system of interest.
- Now for each exposure, we identify possible controls and their costs.
- The last step is a cost–benefit analysis: Does it cost less to implement a control or to accept the expected cost of the loss?

LNMIIT
The LNM Institute of Information Technology

Steps in Risk Analysis

- Risk analysis for security is adapted from more general management practices, placing special emphasis on the kinds of problems likely to arise from security issues. By following well-defined steps, we can analyze the security risks in a computing system.

The basic steps of risk analysis are listed below.

- Identify assets.
- Determine vulnerabilities.
- Estimate likelihood of exploitation.
- Compute expected annual loss.
- Survey applicable controls and their costs.
- Project annual savings of control.

LNMIIT
The LNM Institute of Information Technology

Assets

- *hardware:* processors, boards, keyboards, monitors, terminals, microcomputers, workstations, tape drives, printers, disks, disk drives, cables, connections, communications controllers, and communications media
- *software:* source programs, object programs, purchased programs, in-house programs, utility programs, operating systems, systems programs (such as compilers), and maintenance diagnostic programs
- *data:* data used during execution, stored data on various media, printed data, archival data, update logs, and audit records

LNMIIT
The LNM Institute of Information Technology

Assets

- *people:* skilled staff needed to run the computing system or specific programs, as well as support personnel such as guards
- *documentation:* on programs, hardware, systems, administrative procedures, and the entire system
- *supplies:* paper, forms, laser cartridges, recordable media, and printer ink, as well as power, heating and cooling, and necessary buildings or shelter
- *reputation*: company image
- *availability:* ability to do business, ability to resume business rapidly and efficiently after an incident

Determine Vulnerabilities

- The next step in risk analysis is to determine the vulnerabilities of these assets. This step requires imagination; we want to predict what damage might occur to the assets and from what sources. We can enhance our imaginative skills by developing a clear idea of the nature of vulnerabilities.
- This nature derives from the need to ensure the three basic goals of computer security: confidentiality, integrity, and availability. Thus, a vulnerability is any situation that could cause loss of confidentiality, integrity, and availability.

LNMIIT
The LNM Institute of Information Technology

Estimate the Likelihood of exploitation

- The third step in conducting a risk analysis is determining how often each exposure is likely to be exploited. Likelihood of occurrence relates to the stringency of the existing controls and the likelihood that someone or something will evade the existing controls.

Compute Expected Loss

- Upto this time we have an understanding of the assets we value, their possible vulnerabilities, and the likelihood that the vulnerabilities will be exploited.
- Next, we must determine the likely loss if the exploitation does indeed occur. As with likelihood of occurrence, this value is difficult to determine.
- Some costs, such as the cost to replace a hardware item, are easy to obtain. The cost to replace a piece of software can be approximated reasonably well from the initial cost to buy it (or specify, design, and write it).
- there are costs in restoring a system to its previous state, reinstalling software, or deriving a piece of information. These costs are substantially harder to measure.

Survey and Select New Controls

- By this point in our risk analysis, we understand the system's vulnerabilities and the likelihood of exploitation. We turn next to an analysis of the controls to see which ones address the risks we have identified.
- We want to match each vulnerability with at least one appropriate security technique.
- Once we do that, we can use our expected loss estimates to help us decide which controls, alone or in concert, are the most cost effective for a given situation.

LNMIIT
The LNM Institute of Information Technology

Project Cost and Savings

- The next step is to determine whether the costs outweigh the benefits of preventing or mitigating the risks.

LNMIIT
The LNM Institute of Information Technology

Argument for and Against Risk Analysis

Favor	Against
Improve awareness	*False sense of precision and confidence*
Relate security mission to management objectives	*Hard to perform.*
Identify assets, vulnerabilities, and controls	*Lack of accuracy*
Improve basis for decisions	
Justify expenditures for security	

Physical Threats

- **Up to now, we have discussed** technical issues in security and their technical solutions: firewalls, encryption techniques, malware scanners, and more.
- However, many threats to security involve human or natural disasters, events that should also be addressed in the security plan.

Physical Threats

- Natural Disasters (Flood, Fire etc.)
- Power Loss (Solution Uninterruptible Power Supply, Surge Suppressor)
- Human Vandals:
  - Unauthorized Access and Use
  - Theft (Solution Preventing Access, Preventing Portability)
- Interception of Sensitive Information (Solution Proper disposal of documents like draft, Overwriting Magnetic Data)

Physical Threats

Contingency planning:

- **Backup permits recovery from loss or failure of a computing device.**
- **If the purpose of backup is to protect against disaster, the backup must not also be destroyed in the disaster.**

Backup, Offsite Backup, Networked Storage, Cloud Backup

LNMIIT
The LNM Institute of Information Technology

Privacy, Legal Issues and Ethics

Classroom Code:o7l60yk

LNMIIT
The LNM Institute of Information Technology

Outline

- Privacy
- Legal Issues
- Ethics Issues

LNMIIT
The LNM Institute of Information Technology

Information Privacy

- **Information privacy has three aspects: sensitive data, affected parties, and controlled disclosure.**
- ***Privacy is the right to control who knows certain things about you.***
- ***What one person considers private is that person's decision: There is no universal standard of what is private.***

LNMIIT
The LNM Institute of Information Technology

Information Privacy

Sensitive Data

- *Identity*: name, identifying information, the ownership of private data and ability to control its disclosure
- *Finances*: credit rating and status, bank details, outstanding loans, payment records, tax information
- *Legal*: criminal records, marriage history, civil suits

LNMIIT
The LNM Institute of Information Technology

Sensitive Data

- *Health*: medical conditions, drug use, DNA, genetic predisposition to illnesses
- *Opinions, preferences, and membership*: voting records, expressed opinions, membership in advocacy organizations, religion, political party, reading habits, web browsing, favorite pastimes, close friends
- *Biometrics*: physical characteristics, polygraph results, fingerprints
- *Documentary evidence*: surface mail, diaries, poems, correspondence, recorded thoughts

Sensitive Data

- *Privileged communications*: with professionals such as lawyers, accountants, doctors, counselors, and clergy
- *Academic and employment information*: school records, employment ratings
- *Location data*: general travel plans, current location, travel patterns
- *Digital footprint*: email, telephone calls, spam, instant messages, tweets, and other forms of electronic interaction, social networking history

Computer Related Privacy Problems

- Computers and networks have affected only the feasibility, speed, and reach of some unwanted disclosures.
- Public records offices have long been open for people to study the data held there, but the storage capacity and speed of computers have given us the ability to amass, search, and correlate faster and more effectively than ever before.
- With search engines we can find one data item out of billions, the equivalent of finding one sheet of paper out of a warehouse full of boxes of papers.
- Furthermore, the openness of networks and the portability of technology (such as laptops, tablets, cell phones, and WiFi-enabled devices) have greatly increased the risk of disclosures affecting privacy.

Eight Dimension of Privacy

- *Information collection*: Data are collected only with knowledge and explicit consent.
- *Information usage*: Data are used only for certain specified purposes.
- *Information retention*: Data are retained for only a set period of time.
- *Information disclosure*: Data are disclosed to only an authorized set of people.

Eight Dimension of Privacy

- *Information security*: Appropriate mechanisms are used to ensure the protection of the data.
- *Access control*: All modes of access to all forms of collected data are controlled.
- *Monitoring*: Logs are maintained showing all accesses to data.
- *Policy changes*: Less restrictive policies are never applied after-the-fact to already obtained data.

Privacy Principles and Policies

- **Fair Information Practices : Focuses on privacy rights of individuals to sensitive data.**
- *Collection limitation*. Data should be obtained lawfully and fairly.
- *Data quality*. Data should be relevant to their purposes, accurate, complete, and up to date.
- *Purpose specification*. The purposes for which data will be used should be identified and the data destroyed if no longer necessary to serve that purpose.

Fair Information Practices Contd..

- ***Use limitation***. **Use for purposes other than those specified is authorized only with consent of the data subject or by authority of law.**
- ***Security safeguards***. **Procedures to guard against loss, corruption, destruction, or misuse of data should be established.**
- ***Openness***. **It should be possible to acquire information about the collection, storage, and use of personal data systems.**

LNMIIT
The LNM Institute of Information Technology

Fair Information Practices Contd..

- ***Individual participation*. The data subjects normally have a right to access and to challenge data relating to them.**
- ***Accountability*. A data controller should be designated and accountable for complying with the measures to effect the principles.**

LNMIIT
The LNM Institute of Information Technology

Legal and Ethical Issues

- Here we will discuss human controls applicable to computer security: the legal system and ethics.
- The legal system has adapted quite well to computer technology by reusing some old forms of legal protection (copyrights and patents) and creating laws where no adequate ones existed (malicious access).

Law	Ethics
Described by formal, written documents	Described by unwritten principles
Interpreted by courts	Interpreted by each individual
Established by legislatures representing all people	Presented by philosophers, religions, professional groups
Applied to everyone	Chosen personally
Priority determined by courts if two laws conflict	Priority determined by an individual if two principles conflict
"Right" arbitrated finally by court	Not arbitrated externally
Enforced by police and courts	Enforced by intangibles such as principles and beliefs

LNMIIT
The LNM Institute of Information Technology

Self Study

Chapter 11:

- **11.1 Protecting Programs and Data**
- 11.2 Information and the Law
- 11.3 Rights of Employees and Employers
- 11.5 Computer Crime
- **11.6 Ethical Issues in Computer Security**
- 11.7 Incident Analysis with Ethics

LNMIIT
The LNM Institute of Information Technology

Thank you, for your time and attention!




The LNMIIT: Where young dreams take shape .....