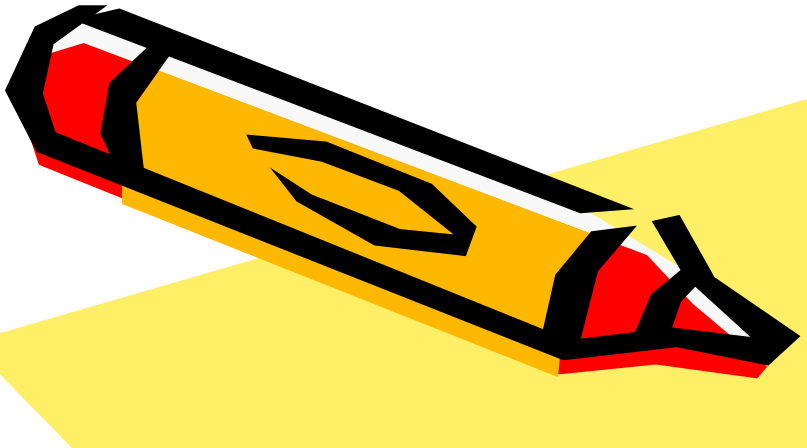


CHAPTER FIVE: SECURITY RISKS AND HAZARDS

SECURITY RISKS AND HAZARDS

Introduction

- *Risk* is the probability that a vulnerability will be exploited.
- Security management must manage risks in terms of causes, effects and costs of a security loss.
  - The costs resulting from a security fault must be balanced with the costs resulting from enhanced security measures.
    - This means that systematic security management allows counter-measures to be chosen in a planned and managed way,
      - since too much security wastes money while
      - too little security wastes Information System resources (IS) capability.
- N.B:
  - management of security comes down to the following distinct stages:
    - ***Risk Identification.***
    - ***Risk Analysis or Assessment.***
    - ***Risk Handling***
    - ***Disaster Recovery***

4.1 . Security Planning

Introduction

- Years ago, most computing was done on mainframe computers:-
  i. data processing centers were responsible for protection.
  ii. Responsibility for security rested neither with the programmers nor the users but instead with the computing centers themselves.
  iii. These centers developed expertise in security, and they implemented many protection activities in the background, without users having to be conscious of protection needs and practices.
- 1980s, the introduction of personal computers:-
  - a significant amount of the responsibility for security has shifted to the user and away from the computing center.
    - But many users are unaware of (or choose to ignore) this responsibility, so they do not deal with the risks posed or do not implement simple measures to prevent or mitigate problems.
- For these reasons, every organization using computers to create and store valuable assets should perform thorough and effective security planning.

SECURITY RISKS AND HAZARDS

Stagesbin risk management

i) Risk identification: Cont.

- On top of this classification of threats to the IT resources, another classification with respect to the specific resources is shown below:

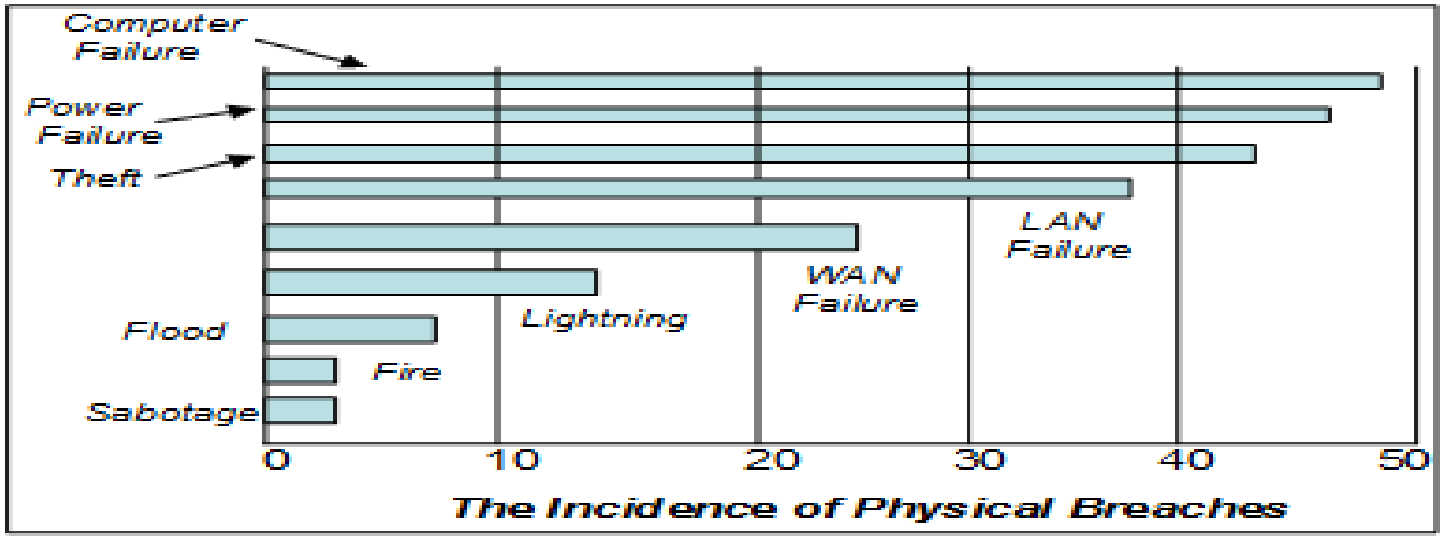
Nature of Threat	Features
PCs	Physical Theft, Viruses (on disks), fraudulent identification, illegal leakage of authorized information.
Database	Unauthorized access, theft, copying
Internet connection/Server	Denial of services; changing information; putting undesirable content
LAN/WAN cabling	Wiretapping/decoding

Proper risk identification will require an appreciation of likely vulnerability areas (likely threats) and detailed knowledge of the organization (specific threats).

SECURITY RISKS AND HAZARDS

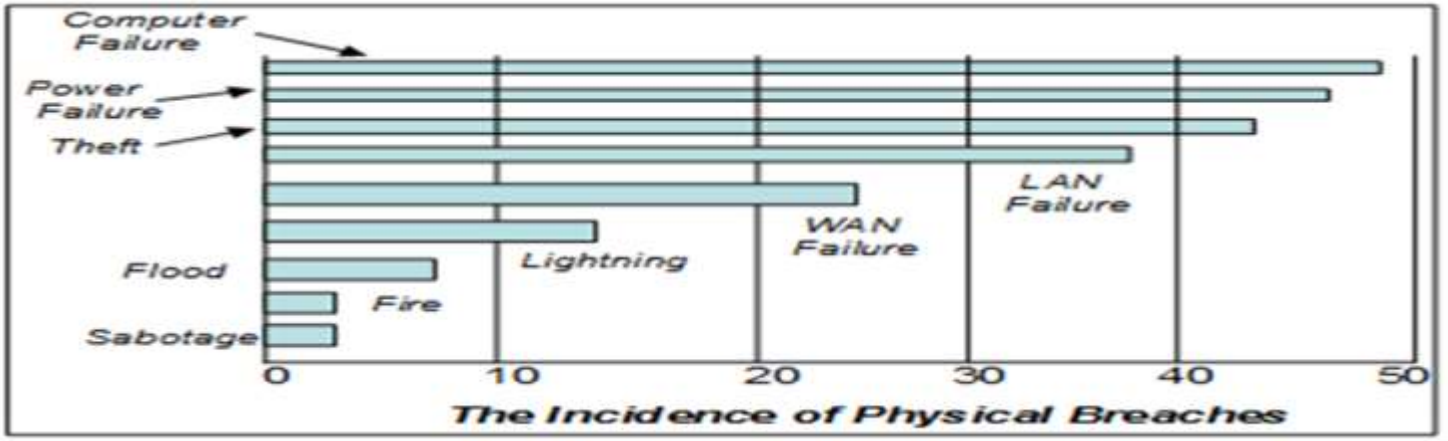
i) Risk identification: Cont.

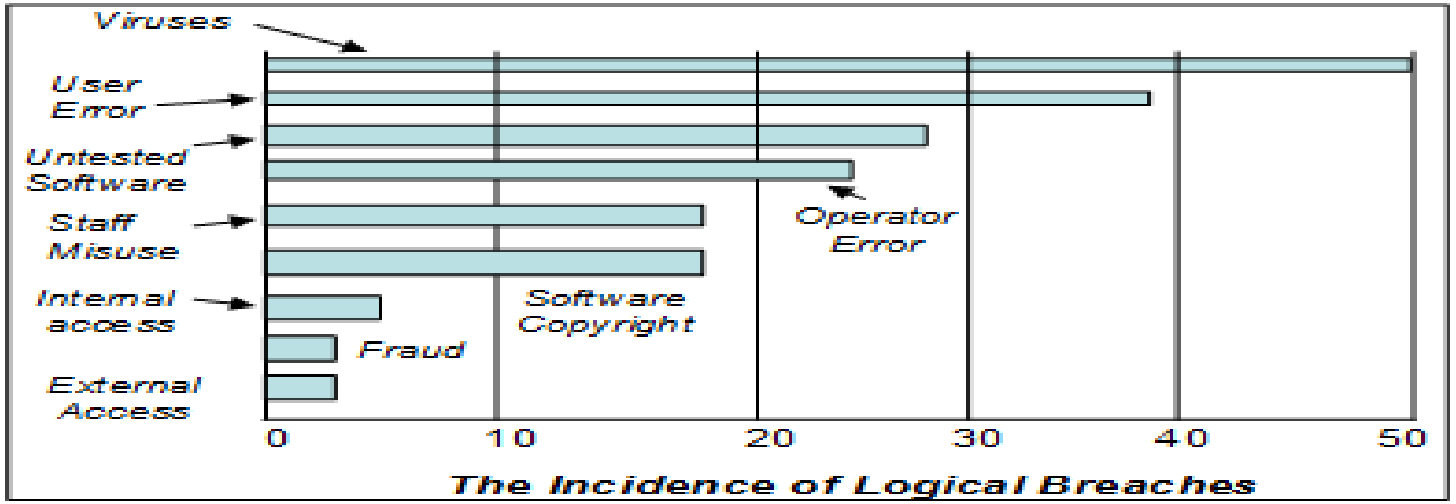
- Full risk identification is a process that involves identifying:
  - ***Source of potential threats;***
  - ***Assets which are vulnerable to loss;*** and
  - ***location of these assets.***
- The relative incidences of physical and logical security breaches are shown below.



SECURITY RISKS AND HAZARDS

i) Risk identification: Cont.





SECURITY RISKS AND HAZARDS

ii) Risk Analysis:

- The organization quantifies the probability and expected frequency of occurrence of each identified risk and also
  - assess the likely damage of the consequences.
- During this stage, the potential impact of the identified threats is established. The analysis seeks to assess the expected loss caused by a particular threat
  - This means the business costs arising from the violation of security have to be determined for the following IS elements:
    i. **Hardware:** This loss is easy to value (most of these elements being insured)
    ii. **Data and Information:** Most serious loss and hardest to quantify.
    iii. **Software:** Also difficult to quantify because the cost of replacement of the software is not the same as the cost of development.
    iv. **Processing Capability:** The length of the disruption of the processing capability determines the value of this kind of loss.
    v. **Complex real-time systems** will generate great losses after just a few seconds, whereas other systems may only need periodic processing.

SECURITY RISKS AND HAZARDS

ii) Risk Analysis: Cont.

- Risk analysis provides the following benefits:
  - **Improve awareness:**
    - Discussing issues of security can raise the general level of interest and concern among employees.
  - Identify assets, vulnerabilities and controls:
    - *Some companies may be unaware of their computing assets and the vulnerabilities associated with those assets, and a systematic analysis produces a comprehensive list of assets and vulnerabilities.*
  - Improve basis for decisions:
    - *Controls reduce productivity through increased overhead and inconvenience to users.*
    - *Some controls can not be justified from the perspective of the protection they provide. Also, some risks are so serious that they warrant a continuing search for more effective controls. Thus, the seriousness of the risk affects the desirability of controls.*
  - Justify expenditures for security:
    - Some security mechanisms or controls are very expensive without an obvious benefit.
    - *A risk analysis can help identify instances that are worth the expense of a major security mechanism.*

SECURITY RISKS AND HAZARDS

ii) Risk Analysis: Cont.

- Sometimes it is difficult to predict the frequency of occurrence of a certain threat; in this case, relative values can be assigned High, Medium, and Low, as shown:

Threat	{Probability of attack}	X	{Probability of Success}	= Frequency
Incorrect data entry	V. High 90%		Medium 50%	45%
Fire	Medium 50%		High 70%	35%
Hacking	Low 20%		Medium 50%	10%

- The expected annual loss is then given as below:

$$\underbrace{\{\text{Cost (from consequences)}\} \times \{\text{Frequency (from estimates)}\}}_{\text{Annual Loss Exposure}}$$

SECURITY RISKS AND HAZARDS

ii) Risk Analysis: Cont.

- Estimating the worth of data is often difficult;
  - business needs may place a higher value on some data because of its potential patent royalty or other monetary gains.
- Classifying data in terms of its criticality can be a preliminary step in establishing its value.
- Shown below is an example of you can classify different types of data and apply a criticality rating.

Type of data	***Classification***	***Criticality***
Clinical trial data	*Research*	*High*
Market	*Research*	*Low*
Pending Patents	*Proprietary*	*High*
Corporate Memos	*Administration*	*Low*
Employee Locator File	*Administration*	*Low*
New Product Features	*Proprietary*	*Medium*
Trade secrets	*Proprietary*	*High*
Acquisition data	*Financial*	*High*
Employee salaries	*Financial*	*Medium*

SECURITY RISKS AND HAZARDS

iii) Risk Handling:-

- is the application of controls, and counter measures appropriate to the risk, subject to constraints – such as available funds.
- Risk handling strategies include the following:
  - Risk Avoidance:
    - Can the risk be avoided?
    - This may mean setting IT systems away from obviously dangerous/insecure areas, deciding against centralization of IT resources, telecommuting, etc.
  - Risk Retention:
    - Is applied only where the organization feels that it can bear with the expected losses. This is applied to risks that have been identified to have low associated costs.
  - Risk Reduction:
    - is the policy of introducing controls and counter measures to reduce the likelihood of occurrence or reduce the losses that will result violation of security.
  - Risk Transfer:
    - This strategy passes over the costs resulting from the violation of security to a third party (insurance policies, maintenance contracts, standby agreements, etc)

SECURITY RISKS AND HAZARDS

iii) Risk Handling Cont.

- Below is a summary of the severity of risk and the risk handling approach:

Threat severity	***Risk Handling Strategy***
Total calamities	*Risk avoidance* *Risk transfer*
Low-loss threats	*Risk retention*
Others	*Risk retention* *Risk transfer*

SECURITY RISKS AND HAZARDS

iv). Contingency Planning and Disaster Recovery Cont.

- This is where the organization develops a contingency plan to deal with and recover from the inevitable security break-downs.
- The contingency plan should include the following –
  - The interim methods of working that will allow the organization to survive the disaster;
    - this stage is concerned with coping with the disaster itself by ensuring safety, minimizing damage and enabling a return to work.
  - The long-term processes that will allow the organization to recover from the disaster; this stage is concerned with minimizing the consequences of the disaster.
    - Typically, the first step in contingency planning is to classify systems and applications in order of their necessity to business operation.
    - This enables the organization to know when each must be functioning again for the business to survive. Through this knowledge, efforts are channeled in the most productive way.
    - If the business is not kept running in the short-term, then long term recovery will not be relevant and therefore immediate standby arrangements are critical to the organization's chances of disaster recovery and to the overall costs involved.

SECURITY RISKS AND HAZARDS

iv). Contingency Planning and Disaster Recovery Cont.

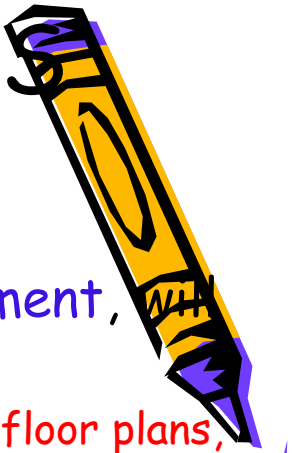
- Standby arrangements include:
  - **Hot site facilities/replica of data center with all s/w, h/w running concurrently with primary site:**
    - In this case, everything to enable IS operation is already installed. These sites allow almost instantaneous business operation, provided that back-ups are available.
  - **Cold site facilities: no server, h/w or s/w nothing** Where an equipped but empty data center is available. These sites are general purpose and therefore cheaper than hot sites. They, however, make it slower to get business operations running since there is the need to install business appropriate features in them after the disaster.
  - ***Portable facilities:*** Provision is made from portable vehicles, or semi-portable prefabricated buildings. These are a popular option.
- Other arrangements include the following:
  - reciprocal arrangements between firms;
  - priority replacement agreements;
  - commercial service providers, etc.

SECURITY RISKS AND HAZARDS

iv). Contingency Planning and Disaster Recovery Cont.

- The suggested structure of the disaster-planning document includes the following key elements:
  i. **Introduction and Index**: Including a brief description of the manual, how it is structured, who holds the copies of the plan, how to use the plan, etc.
  ii. **Definition of computer disaster**: Provided should be a definition of what, to the organization, a disaster is (say a loss of service or loss of revenue). Also included should be the organization's policy on disaster planning. Because there will be different recovery strategies for different types of disaster, the document should define levels of disasters (say a small fire causing little damage or interruption to a major fire that destroys an entire data area).
  iii. **Assumptions:** The assumptions upon which the plans are based should be explained and the assumptions should be reviewed/tested regularly. The plan may, for example, assume that all key personnel will be available, which may not be the case.
  iv. **Disaster exclusions:** Even those disasters that the plan does not cover for will need to be identified in the document (say a nuclear attack, etc).

SECURITY RISKS AND HAZARDS



v) **Inventories:**

- All the software and hardware,
  - including data and voice communications equipment, need to be itemized.
  - Other things to itemize include staff organization charts, floor plans, wiring diagrams, and entrance and exit routes.
  - Availability of standby systems, contractual agreements and commitments, and supply of replacement equipment should be highlighted.

vi) **Emergency budgets:**

- This section should detail how urgent cash flows will be generated during the disaster. Claims from insurance companies should be identified.

vii) . **Invocation:**

- details how the alarm is raised and the disaster recovery plan invoked.
- Disaster management teams must be defined;
  - included here should also be the organizational structure of all recovery teams, presented to an appropriate level of detail and outlining all respective team actions.

SECURITY RISKS AND HAZARDS

vii) Logistics:

- Logistical planning will include sections on transport, staffing, supplies such as media, communications, access and security arrangements, services, etc. Without adequate logistical planning, there is a high degree of risk that the disaster recovery plan will fail.

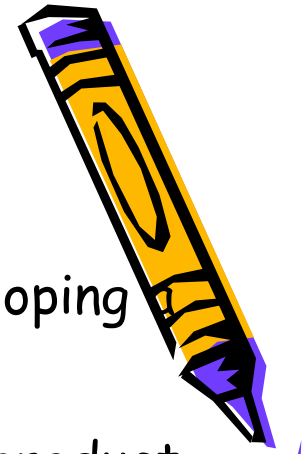
viii)Maintenance and testing:

- This section defines how the recovery plan will be tested and maintained.

ix) Appendices:

- This is the area in which to file the following:
  - Insurance policies
  - Any third-party standby service agreements
  - Vendor agreements
  - Important or useful correspondence
  - Results from risk analysis
  - Business impact reviews, etc.

Risk Analysis (In details)



1. Introduction:

What is a formal process of determining risks and developing plan to deal with them?

Risks do not arise all by themselves. A risk is normally a product of two factors:

a. threats (something could go wrong) and
b. vulnerabilities (the information system/s used by the business will allow things to do wrong).

a) Threats include:

- Deliberate manipulation of information prior to input/processing
- Impersonation of a legitimate user
- Untrained or poorly trained staff

Risk Analysis (In details) Cont….

b) Vulnerabilities include:

- Poor website or network design (e.g. which can allow "hackers" into a system or web site)
- Poor recruitment procedures

The first and key stage risk analysis in addressing risks

- is to do a risk analysis:

A risk analysis process has three main stages:

1) Understanding risks to the business and how they can occur
2) Understanding the potential cost to the business if they do occur (a business should focus its attention with the risks that have the greatest potential cost)
3) Identifying suitable and effective measures and policies to:
   - Minimise the likelihood of the threats happening
   - Prevent or detect the threat
   - Enable appropriate recovery action to be taken

Risk Analysis (In details) Cont…

- Good, effective security planning includes a careful 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:

i. 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.

ii. 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.

iii. 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 (In details) Cont….

- 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 Ksh.100,000., then the risk exposure is Ksh.30,000. So we can use a calculation like this one to decide that a virus checker is worth an investment of Ksh.10,000., since it will prevent a much larger potential loss.*
    - Clearly,
      - risk probabilities can change over time, so it is important to track them and plan for events accordingly.

Risk Analysis (In details) Cont….

- Risk is inevitable in life:
  - Crossing the street is risky but that does not keep us from doing it. We can identify, limit, avoid, or transfer risk but we can seldom eliminate it.
- In general, we have three strategies for dealing with risk:
  i. Avoiding the risk,
     - *by changing requirements for security or other system characteristics*
  ii. Transferring 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*
  iii. Assuming the risk,
     - *by accepting it, controlling it with available resources, and preparing to deal with the loss if it occurs*

Risk Analysis (In details) Cont….

- Thus, 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. In other words, risk leverage is
- 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 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.
    - Then, 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?

Risk Analysis (In details) Cont….

2. The Nature of Risk

In building and using computing systems, we must take a more organized and careful approach to assessing our risks.

Many of the systems we build and use can have a dramatic impact on life and health if they fail. For this reason, risk analysis is an essential part of security planning.

We cannot guarantee that our systems will be risk free; that is why our security plans must address actions needed should an unexpected risk become a problem. And some risks are simply part of doing business;

for example, as we have seen, we must plan for disaster recovery, even though we take many steps to avoid disasters in the first place.

When we acknowledge that a significant problem cannot be prevented, we can use controls to reduce the seriousness of a threat.

For example,

- you can back up files on your computer as a defense against the possible failure of a file storage device. But as our computing systems become more complex and more distributed, complete risk analysis becomes more difficult and time consuming and more essential.

Risk Analysis (In details) Cont….

3. Steps of a Risk Analysis

- Risk analysis is performed in many different contexts;
- for example,
  - *environmental and health risks are analyzed for activities such as building dams, disposing of nuclear waste, or changing a manufacturing process.*
  - 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:
  i. Identify valuable assets.
  ii. Determine vulnerabilities.
  iii. Estimate likelihood of exploitation.
  iv. Compute expected annual loss.
  v. Survey applicable controls and their costs.
  vi. Project annual savings of control.

Risk Analysis (In details) Cont….

4. Arguments For and Against Risk Analysis

- Risk analysis is a well-known planning tool, used often by auditors, accountants, and managers. In many situations, such as obtaining approval for new drugs, new power plants, and new medical devices, a risk analysis is required by law in many countries. There are many good reasons to perform a risk analysis in preparation for creating a security plan.

a. Improve awareness.

- Discussing issues of security can raise the general level of interest and concern among developers and users.
  - Especially when the user population has little expertise in computing,
  - the risk analysis can educate users about the role security plays in protecting functions and data that are essential to user operations and products.

Risk Analysis (In details) Cont…

4. Arguments For and Against Risk Analysis cont

b. Relate security mission to management objectives.

- Security is often perceived as a financial drain for no gain. Management does not always see that security helps balance harm and control costs.

c. Identify assets, vulnerabilities, and controls.

- Some organizations are unaware of their computing assets, their value to the organization, and the vulnerabilities associated with those assets. A systematic analysis produces a comprehensive list of assets, valuations, and risks.

d. Improve basis for decisions.

- A security manager can present an argument such as "I think we need a firewall here" or "I think we should use token-based authentication instead of passwords." Risk analysis augments the manager's judgment as a basis for the decision.

e. Justify expenditures for security.

- Some security mechanisms appear to be very expensive and without obvious benefit. A risk analysis can help identify instances where it is worth the expense to implement a major security mechanism. Justification is often derived from examining the much larger risks of not spending for security.

Risk Analysis (In details) Cont….

i. However, despite the advantages of risk analysis, there are several arguments against using it to support decision making.

   i. **False sense of precision and confidence.**

      - The heart of risk analysis is the use of empirical data to generate estimates of risk impact, risk probability, and risk exposure. The danger is that these numbers will give us a false sense of precision, thereby giving rise to an undeserved confidence in the numbers. However, in many cases the numbers themselves are much less important than their relative sizes. Whether an expected loss is ksh.10,000,000 or ksh.15,000,000 is relatively unimportant. It is much more significant that the expected loss is far above the Ksh1,000,000 or ksh. 2,000,000 budget allocated for implementing a particular control. Moreover, anytime a risk analysis generates a large potential loss, the system deserves further scrutiny to see if the root cause of the risk can be addressed.

Risk Analysis (In details) Cont….

ii) Hard to perform.

- Enumerating assets, vulnerabilities, and controls requires creative thinking. Assessing loss frequencies and impact can be difficult and subjective. A large risk analysis will have many things to consider. Risk analysis can be restricted to certain assets or vulnerabilities, however.

iii) **Immutability.**

- It is typical on many software projects to view processes like risk analysis as an irritating fact of life a step to be taken in a hurry so that the developers can get on with the more interesting jobs related to designing, building, and testing the system. For this reason, *risk analyses, like contingency plans and five-year plans, have a tendency to be filed and promptly forgotten.* But if an organization takes security seriously, it will view the risk analysis as a living document, updating it at least annually or in conjunction with major system upgrades.

Risk Analysis (In details) Cont….

iv) Lack of accuracy.

- Risk analysis is not always accurate, for many reasons.
  - First, we may not be able to calculate the risk probability with any accuracy, especially when we have no past history of similar situations.
  - Second, even if we know the likelihood, we cannot always estimate the risk impact very well. The risk management literature is replete with papers about describing the scenario, showing that presenting the same situation in two different ways to two equivalent groups of people can yield two radically different estimates of impact.

Risk Analysis (In details) Cont….

iv) Lack of accuracy.

- Risk analysis is not always accurate, for many reasons.
  - we may not be able to anticipate all the possible risks.
  - For example,
  - we may not know enough about software, security, or the context in which the system is to be used, so there may be gaps in our risk analysis that cause it to be inaccurate.

- This lack of accuracy is often cited as a deficiency of risk analysis.
  - Risk analysis is useful as a planning tool, to compare and contrast options.

Risk Analysis (In details) Cont….

- We may not be able to predict events accurately, but we can use risk analysis to weigh the tradeoffs between one action and another.
- When risk analysis is used in security planning,
  - it highlights which security expenditures are likely to be most cost effective.
- This investigative basis is important for choosing among controls when money available for security is limited.
  - And our risk analysis should improve as we build more systems, evaluate their security, and have a larger experience base from which to draw our estimates.

Risk Analysis (In details) Cont….

- A risk analysis has many advantages as part of security plan or as a tool for less formal security decision making.
  - It ranges from very subjective and imprecise to highly quantitative.
- It is useful for generating and documenting thoughts about likely threats and possible countermeasures.
  - Finally, it supports rational decision making about security controls.

The End

Question

&

Answers

THANKS