Security Risk Analysis

Security Risk Analysis

Guidelines

- Security risk analysis, otherwise known as risk assessment, is fundamental to the security of any organization. It is essential in ensuring that controls and expenditure are fully commensurate with the risks to which the organization is exposed.
- However, many conventional methods for performing security risk analysis are becoming more and more untenable in terms of usability, flexibility, and critically... in terms of what they produce for the user.

Risk Analysis cont.

- Security in any system should be commensurate with its risks. However, the process to determine which security controls are appropriate and cost effective, is quite often a complex and sometimes a subjective matter. One of the prime functions of security risk analysis is to put this process onto a more objective basis.
- There are a number of distinct approaches to risk analysis. However, these essentially break down into two types: quantitative and qualitative.

1. Quantitative Risk Analysis

- This approach employs two fundamental elements; the probability of an event occurring and the likely loss should it occur.
- Quantitative risk analysis makes use of a single figure produced from these elements. This is called the 'Annual Loss Expectancy (ALE)' or the 'Estimated Annual Cost (EAC)'. This is calculated for an event by simply multiplying the potential loss by the probability.
- It is thus theoretically possible to rank events in order of risk (ALE) and to make decisions based upon this.

Quantitative Risk Analysis cont.

- The problems with this type of risk analysis are usually associated with the unreliability and inaccuracy of the data. Probability can rarely be precise and can, in some cases, promote complacency. In addition, controls and countermeasures often tackle a number of potential events and the events themselves are frequently interrelated.
- Notwithstanding the drawbacks, a number of organizations have successfully adopted quantitative risk analysis.

2. Qualitative Risk Analysis

- **This is by far the most widely used approach to risk analysis. Probability data is not required and only estimated potential loss is used.**

- **Most qualitative risk analysis methodologies make use of a number of interrelated elements:**
  - **THREATS**
  - **VULNERABILITIES**
  - **CONTROLS**

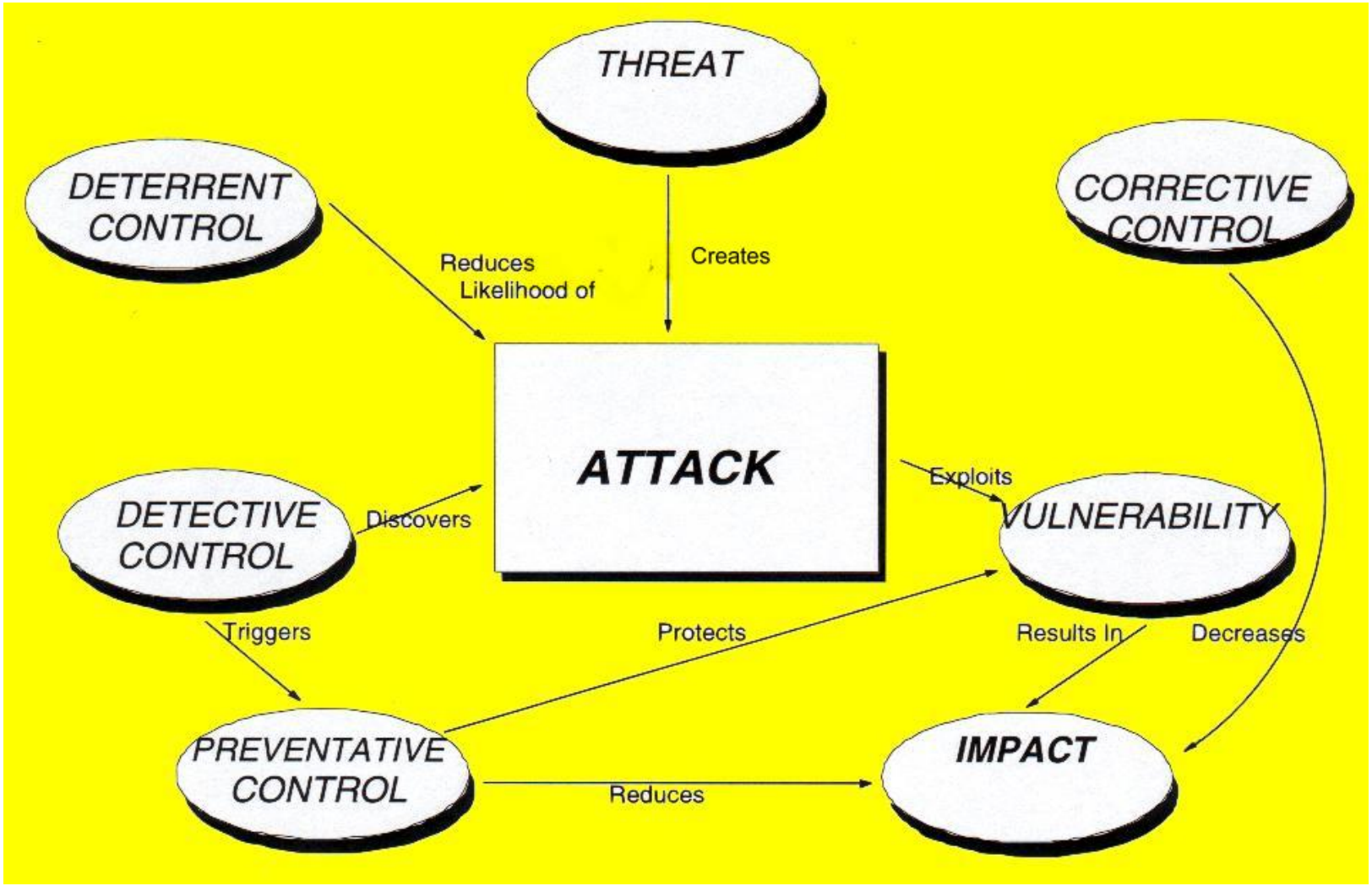
Qualitative Risk Analysis cont.

- **THREATS**
  - These are things that can go wrong or that can 'attack' the system.
  - Examples might include fire or fraud. Threats are ever present for every system.
- **VULNERABILITIES**
  - These make a system more prone to attack by a threat or make an attack more likely to have some success or impact.
  - For example, for fire a vulnerability would be the presence of inflammable materials (e.g. paper).

Qualitative Risk Analysis cont.

- **CONTROLS**
  - These are the countermeasures for vulnerabilities. There are four types:
    - **Deterrent** controls reduce the likelihood of a deliberate attack
    - **Preventative** controls protect vulnerabilities and make an attack unsuccessful or reduce its impact
    - **Corrective** controls reduce the effect of an attack
    - **Detective** controls discover attacks and trigger preventative or corrective controls.

These elements can be illustrated by a simple relational model



Risk Assessment

Business Objectives:

- **FOCUS** on key assets
- **PROTECT** against likely threats
- **PRIORITISE** future actions
- **BALANCE** cost with benefits
- **IDENTIFY / JUSTIFY**

Risk Assessment … cont.

Positive Factors

- Enables security risks to be managed
- Maximises cost effectiveness
- Safeguards information assets
- Enables IT risks to be taken more safely

Risks

- Unauthorised or accidental disclosure
- Unauthorised or accidental modification
- Unavailability of facilities / services
- Destruction of assets

Risk Impact

- Monetary losses
- Loss of personal privacy
- Loss of commercial confidentiality
- Legal actions
- Public embarrassment
- Danger to personal safety

Risk Control Strategy

- Risk prevention
- Reduction of impact
- Reduction of likelihood
- Early detection
- Recovery

Risk Assessment

Recap.

- Risk Assessment is a business requirement
- Risk Assessment is part of overall security management
- Can be complex
- Methods exist
- Approach must suit your organisation

Potential Users of Methodology

- Project Managers
- Systems Developers
- Systems Managers
- Systems Audit
- Business Managers
- Security Managers

Choosing Methodologies

- Assumed expertise of reviewer
- Complexity of environment
- When to apply Risk Analysis
- Consideration of existing controls
- Level of detail
- Scope

The Benefits of:
Security Risk Analysis

- Cost Justification
- Productivity: Audit/Review Savings
- Breaking Barriers - Business Relationships
- Self-Analysis
- Security Awareness
- Targeting Of Security
- 'Baseline' Security and Policy.
- Consistency.
- Communication.

- **Cost Justification**
  Additional security almost always involves additional expense. As this does not directly generate income, it should always be justified in financial terms. The Risk Analysis process should directly and automatically generate such justification for security recommendations in business terms.

- **Productivity: Audit/Review Savings**
  A Risk Analysis programmed should enhance the productivity of the security or audit team. By creating a review structure, formalizing a review, security knowledge in the system's "knowledge base" and utilizing "self-analysis" features, much more productive use of time is possible. The ability to 'build-in' expertise should also alleviate the need for expensive external security consultants.

Breaking Barriers - Business Relationships

- Security should be addressed at both business management and IT staff.
  - Business management are responsible for decisions relating to the security risk/level that the enterprise is willing to accept at a given time.
  - IT management are responsible for decisions relating to specific controls and application .
- Risk Analysis should relate security directly to business issues.

- **Self-Analysis**
  The Risk Assessment system should be simple enough to enable its use without necessitating particular security knowledge, or indeed, IT expertise. This approach enables security to be driven into more areas and to become more devolved. It enables security to become part of the enterprises culture, allowing business unit management to take more of the responsibility for ensuring an adequate and appropriate level of security.

- **Security Awareness**
  The widescale application of a risk assessment programmed, by actively involving a range of, and greater number of, staff, will place security on the agenda for discussion and increase security awareness within the enterprise.

- ## Targeting Of Security

  Security should be properly targeted, and directly related to potential impacts, threats, and existing vulnerabilities. Failure to achieve this could result in excessive or unnecessary expenditure. Risk Analysis promotes far better targeting and facilitates related decisions.

- ## 'Baseline' Security and Policy

  Many enterprises require adherence to certain 'baseline' standards. This could be for a variety of reasons, such as legislation (eg: Data Protection Act), enterprise policy, regulatory controls, etc. The Risk Analysis methodology should support such requirements and enable rapid identification of any failings.

- **Consistency**

  A major benefit of the application of Risk Analysis is that it brings a consistent and objective approach to all security reviews. This not only applies across different applications, but different types of business system.

- **Communication**

  By obtaining information from different parts of a business unit, a Risk Assessment aids communication and facilitates decision making.

  There are also a number of other important, but less tangible, benefits to be accrued via the application of Risk Analysis

The End