



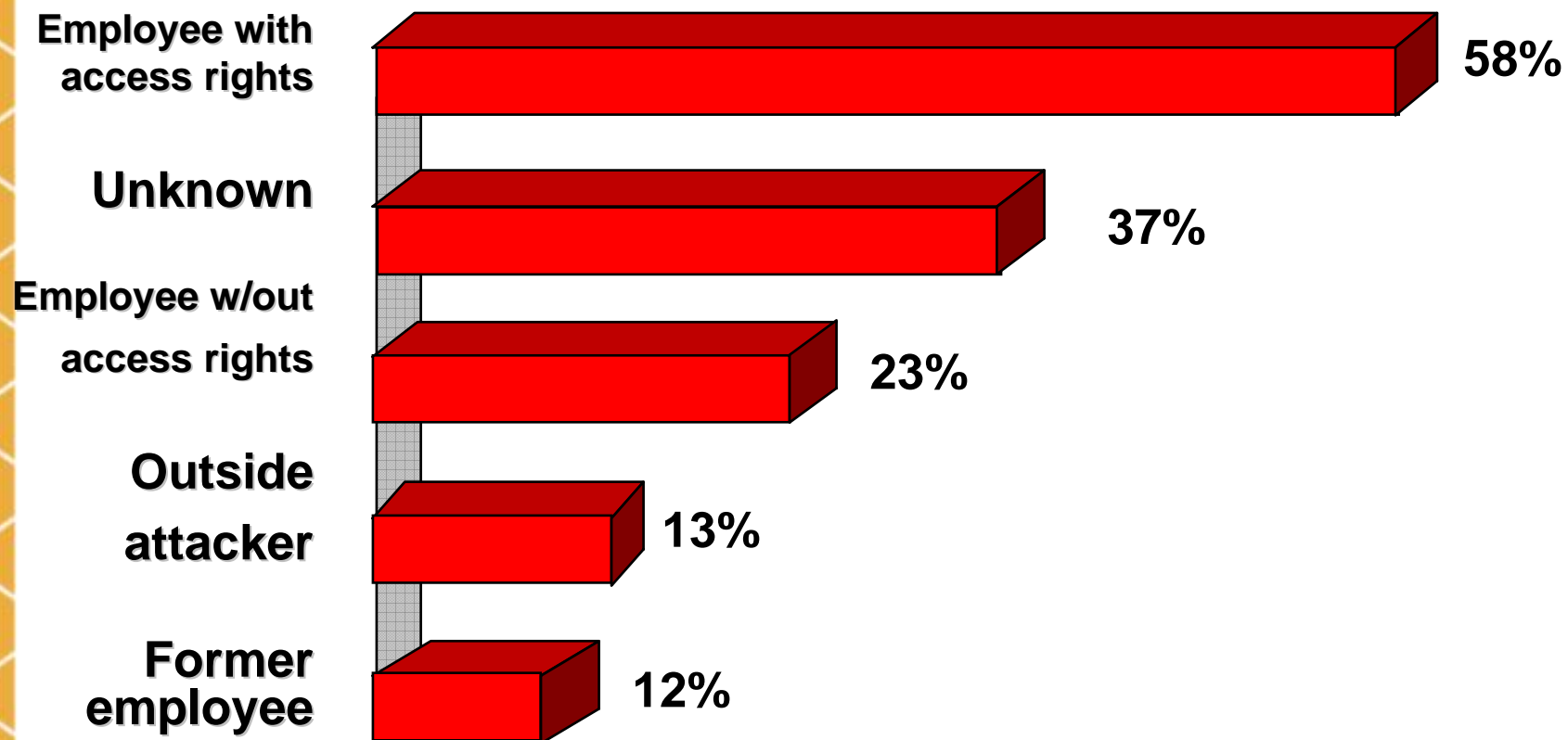
People and Security

What is the Protection Domain?

- Before you can do any meaningful security work, you have to define what you are protecting
 - Security planning
- Then you can decide what tools to use
- The plan must cover all aspects
 - Imagine that you are designing a submarine, not a ship
 - But the leaks are invisible
- You are most likely to find that the most important aspect is people
 - Usually your own employees



Likely threats to Security



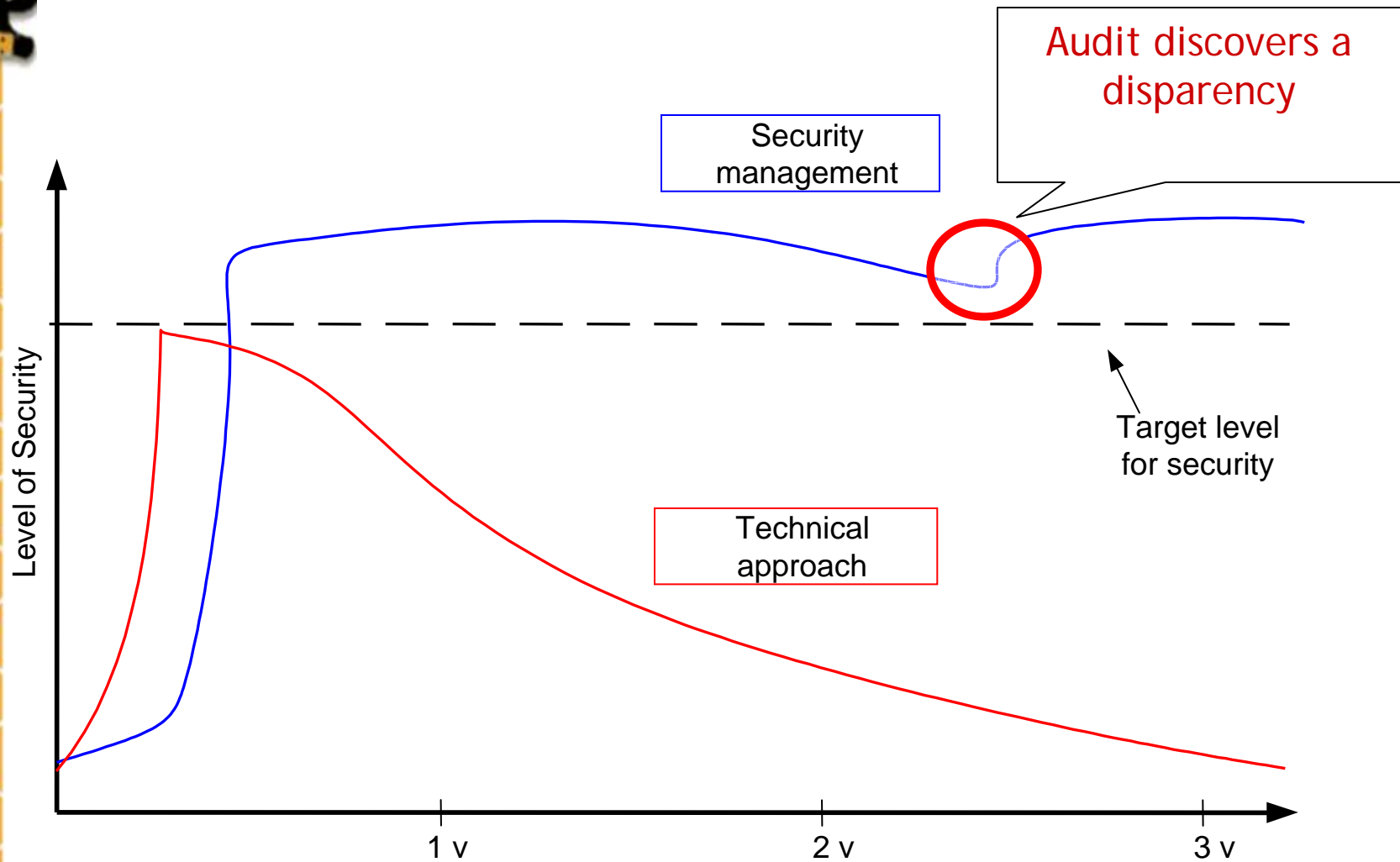
Source - Information Week/Pricewaterhouse Coopers, 1998

People Security

- The technical challenges of security are mostly conquered
 - Firewalls, encryption, virus protection
 - There is still more to do, like PKI, SSO and less obvious things
- However the largest security problem and the next challenge is the people
 - Social engineering is still the most effective attack
 - Own people are the largest threat

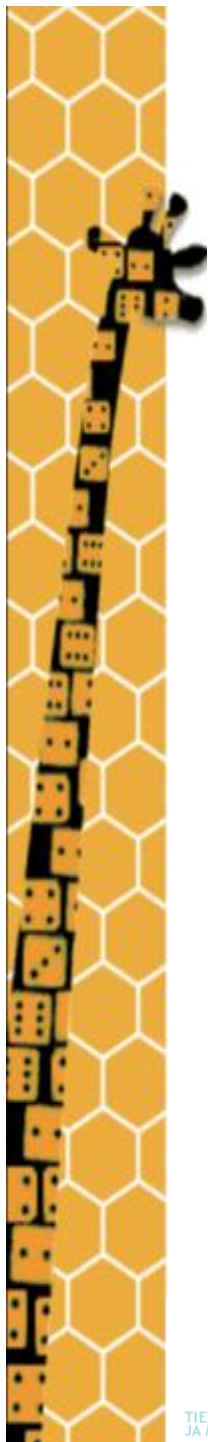


Managed Security Vs. Technical Approach



Experience From Other Fields

- Safety in manufacturing plants has a long background
 - Safety is not a separate issue, but part of the normal work processes
 - The processes are designed to allow work to be done while maintaining the required level of physical safety
- Security work can be modeled on physical safety work
 - Work processes
 - Supervisor training
- A major difference is that security threats are not visible, unlike physical threats



Security Is in the Processes

- Current focus on the security management area is in developing the processes of an organization in such a manner, that the organization works in a secure way
 - In the World War II allied powers could usually break most of the German Wehrmacht and Luftwaffe messages, but not Kriegsmarine messages because (besides better technology) they had good encryption discipline
 - No standard messages
 - No repeated session keys
 - No clear-text retransmissions
- This means that the security policy must be communicated to the people
 - The security policy that is delivered to the entire organization should be short, easy to understand and reasonable
 - Unreasonable security policies are usually not followed



Executing the Security Policy

- Safety regulations usually require that the correct procedures are taught personally to each employee
- Four step technique
 - Supervisor instructs the employee in correct procedures
 - Training reviews the instruction
 - Written guidelines are provided
 - Monitoring ensures that the set target is reached
- This method requires a lot of work
 - Likely to produce results, too
 - Everything must be made concrete
- This is also still a not completely tested theory
- Key issue:
 - How to change people's behavior?



Personal Instruction

- Instructions are made practical and adapted to daily tasks
 - From abstract principles to practice
 - "If somebody asks for a copy of a contract, verify who is asking, and find out from the responsible sales person if you can give it"
 - "Never tell your password to anybody, including the system administration people"
- Daily tasks must support the security policy
 - "There is a sealed password at the office safe which allows access to the department head's files, you may use it with his or management's permission"

Training

- Supports work instruction
- Additional learning and motivation
 - The reasons for guidelines and work practices are made clear
 - General security knowledge
 - Sample cases of real security incidents
 - Examples of how to deflect very persuasive reasoning
- A good time and place to show that the management is supporting the security work



Written Guidelines

- Written instructions
 - "Proposals, offerings, contracts etc. are confidential. Accounting is responsible for archiving them, sales controls the access."
- Who owns the instructions?
 - This matters, because the guidelines need periodic revising
 - For example the line organization owns the guidelines, but changes need to be approved by the security management
- Well defined processes are part of long lasting security

Monitoring

- Security guidelines and processes have any meaning only if they are actually followed
- Monitoring can be done like monitoring any other company policy or practice
 - Supervisors monitor daily work and give feedback on correct and incorrect procedures
 - There must exist a method for reporting conflicts between security guidelines and actual work requirements
 - An external organization can assist in monitoring how well the guidelines are followed in practice



Security Manager's Problems

- Many security managers see the lack of support from the top management as their largest problem
 - Getting the management support can make or break company's security
 - One way to show the support is that **everybody** follows the rules
- The security manager is usually not in the line of command
 - It takes people skills to lead from the sidelines
 - Especially as security is not a profit generator but loss avoidance function
- Shared responsibility is not good for security
 - There should be one person or committee responsible, a single point of focus



Usable Security

- To get the users to actually perform in a secure way it is not enough to create processes that implement security, but to also make security technology usable
- This is still a rather young branch of the security research



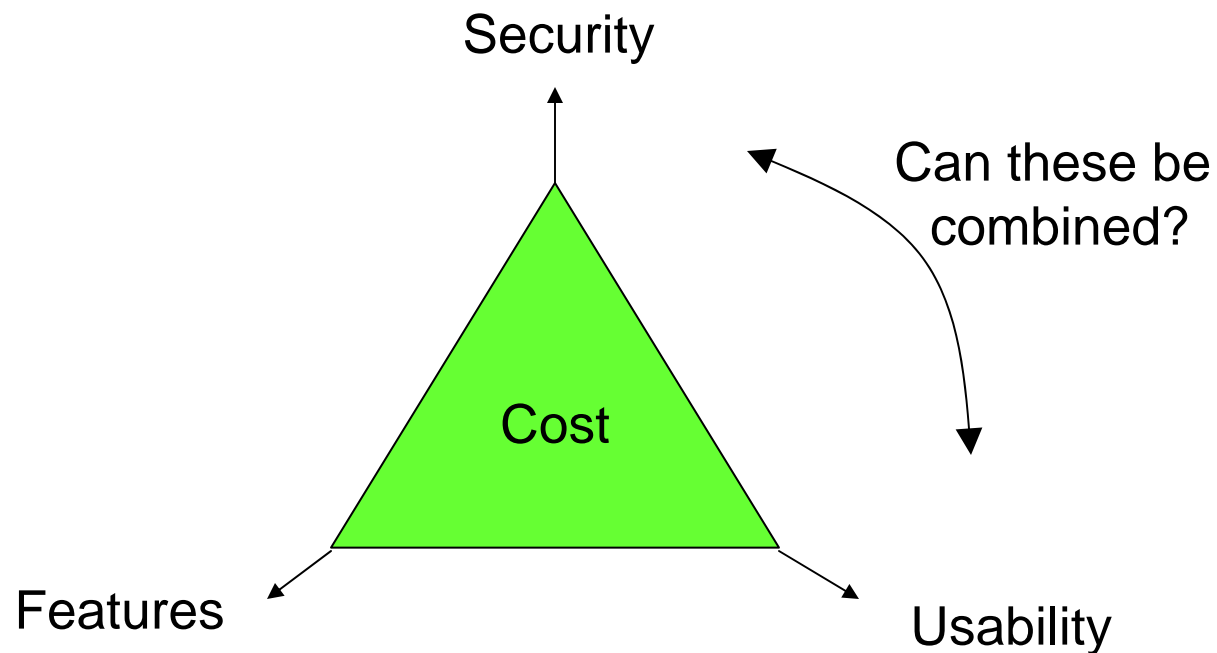
Usability Studies in Security Systems Design

- The target is to design systems that make it easy for the users to comply with various security requirements
- This requires analysis of the
 - Work processes and flow
 - User habits
 - Exception handling
 - Informal processes
- This method can be used to develop the security features of existing systems or to create new ones
- Usability testing tools can be used when developing existing or prototype systems



Balancing the Requirements

- Different system requirements are usually competing against each other to increase costs
- "Clever engineering" can overcome this



Security Is a Process

- Security is never finished
- The world changes
 - Technology changes
 - People forget working methods
- Security is a continuous loop of
 - Plan
 - Implement
 - Evaluate



Security Policy

- The main document for organization's security
- Defines
 - Assets
 - Threats
 - Solutions
- Contains
 - Aims
 - Resources
 - Responsibilities
 - Guidelines to personnel
- Technical implementation



Designing an Information Security Policy

- Evaluate your current situation
 - Information assets
 - Existing security methods
- Evaluate the risks
- Decide what to protect and how
- The value of information should be defined by the owner, generally not the writer of the policy
- Actions to be implemented should be prioritized based on risk, not on the ease of technical implementation



Risk Analysis

- Risk analysis is the assessment and evaluation of risks, to see what kind of protection is needed and where
- Risk analysis usually gives a rough estimate, which can still be used to direct security efforts
- A trivial example
 - A hard disk has information worth \$10 000
e.g.. a customer address database, which can be regenerated
 - Mean life time of a hard disk is 4 years
 - It makes sense to use up to \$2 500 yearly to protect the information

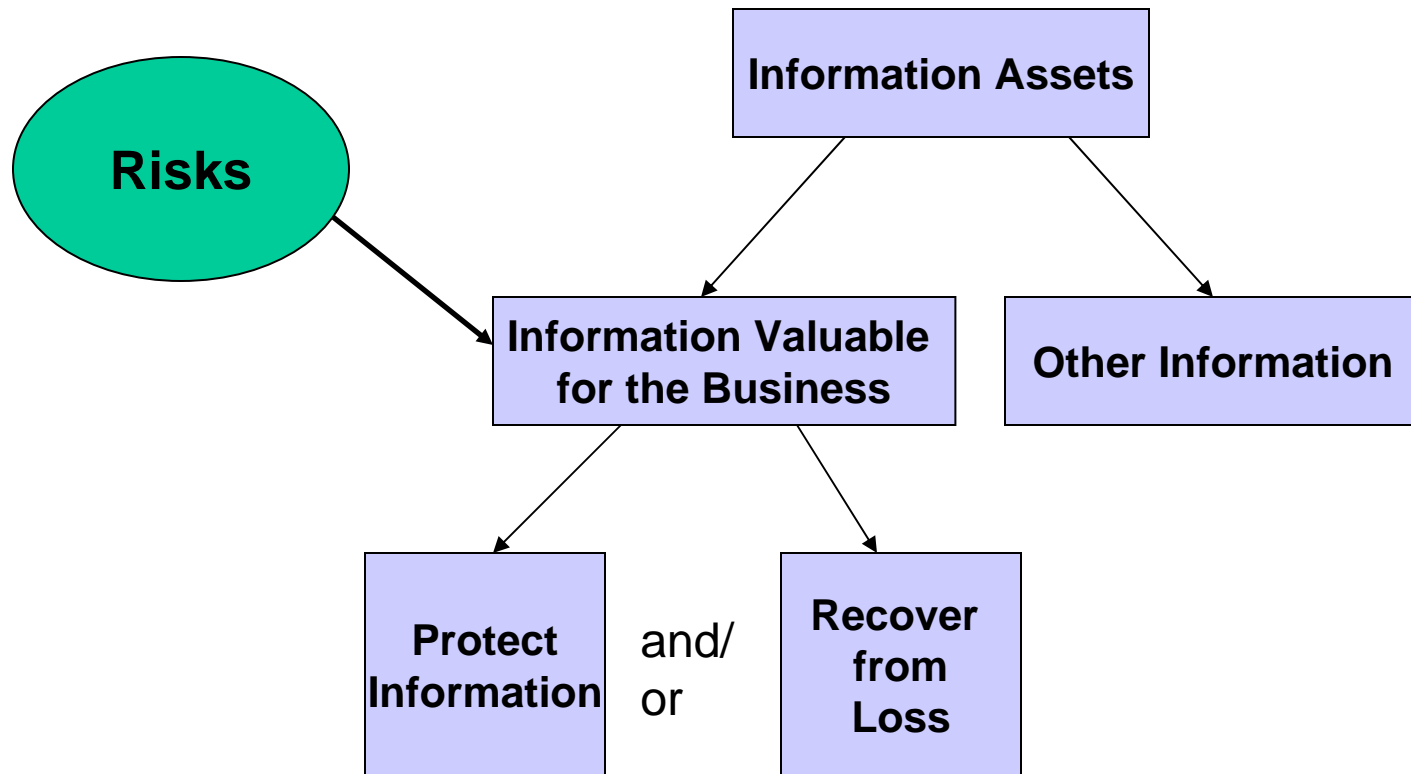


Risk Analysis

- A complete risk analysis would include evaluating every bit of information and all potential risks
 - Very expensive and hard to do
 - Usually existing but unlikely risks such as meteorites can be grouped as "other" risks
- In many cases a sufficient classification has two categories for each risk, "likely" and "serious"
 - Risks that are in both groups should get main attention
 - Serious but unlikely risks should be planned for
 - Likely but unserious risks should have an efficient process for handling them
- Or two or three levels of assets
 - Basic security level affects everything
 - Identify those assets that have higher than normal requirements



What to secure?



Risk Management Is a Continuous Process

