



TEKNILLINEN KORKEAKOULU

People and Security

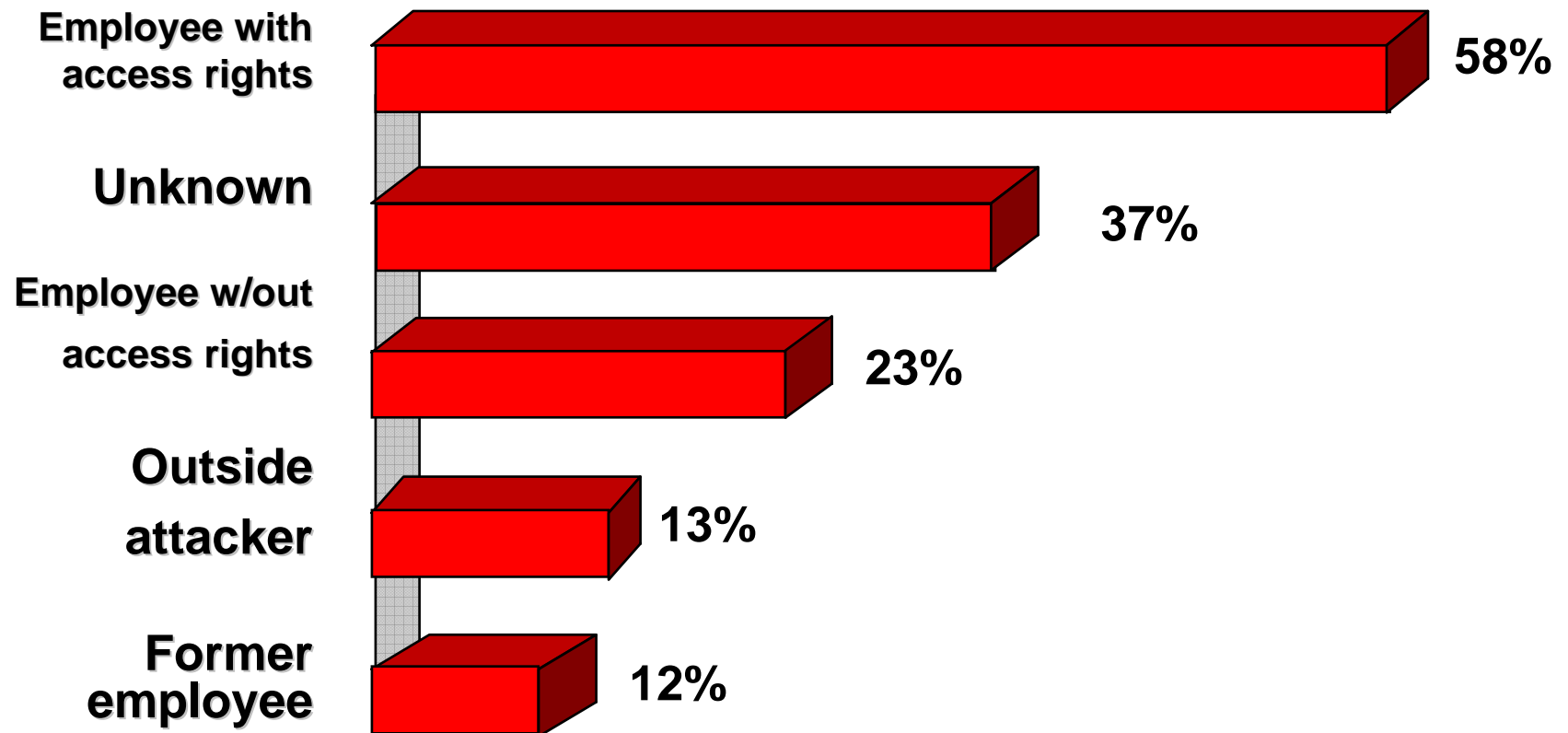


What Is the Protection Domain?

- 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



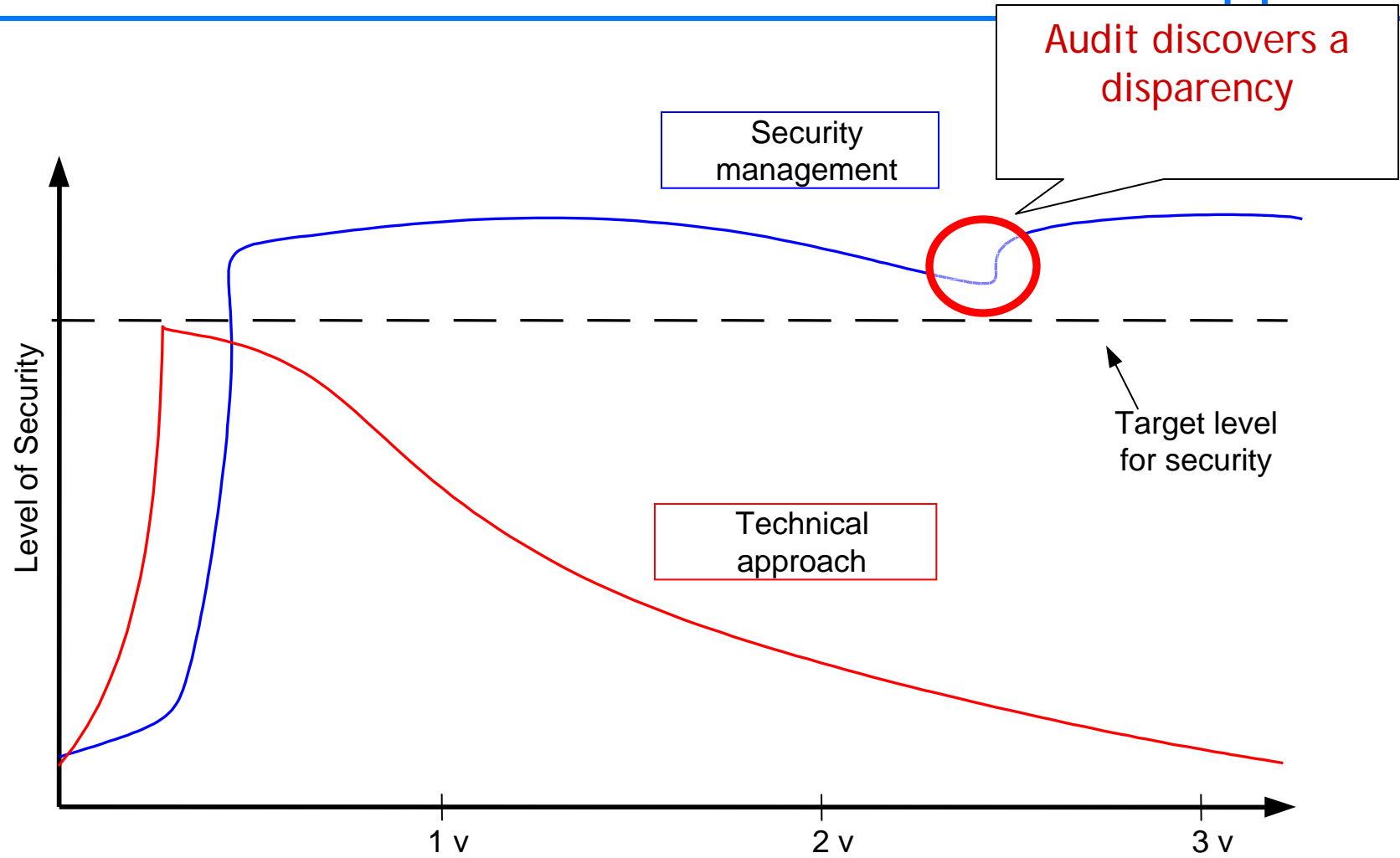
Source - Information Week/Pricewaterhouse Coopers, 1998



- The technical challenges of security are mostly conquered
 - Firewalls, encryption, virus protection
 - There is still more to do, like global PKI, SSO or federated identity and other 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

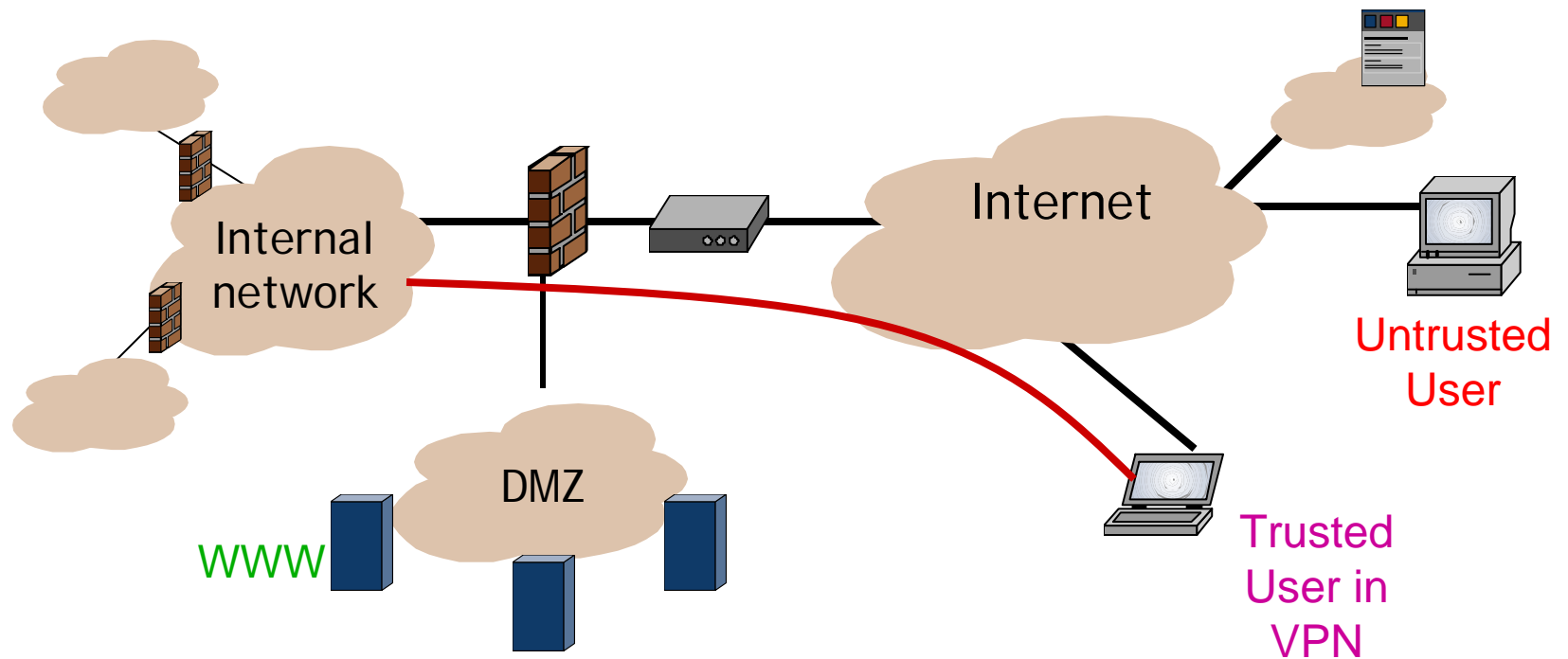


Source: Nixu Ltd.



Secure Networking

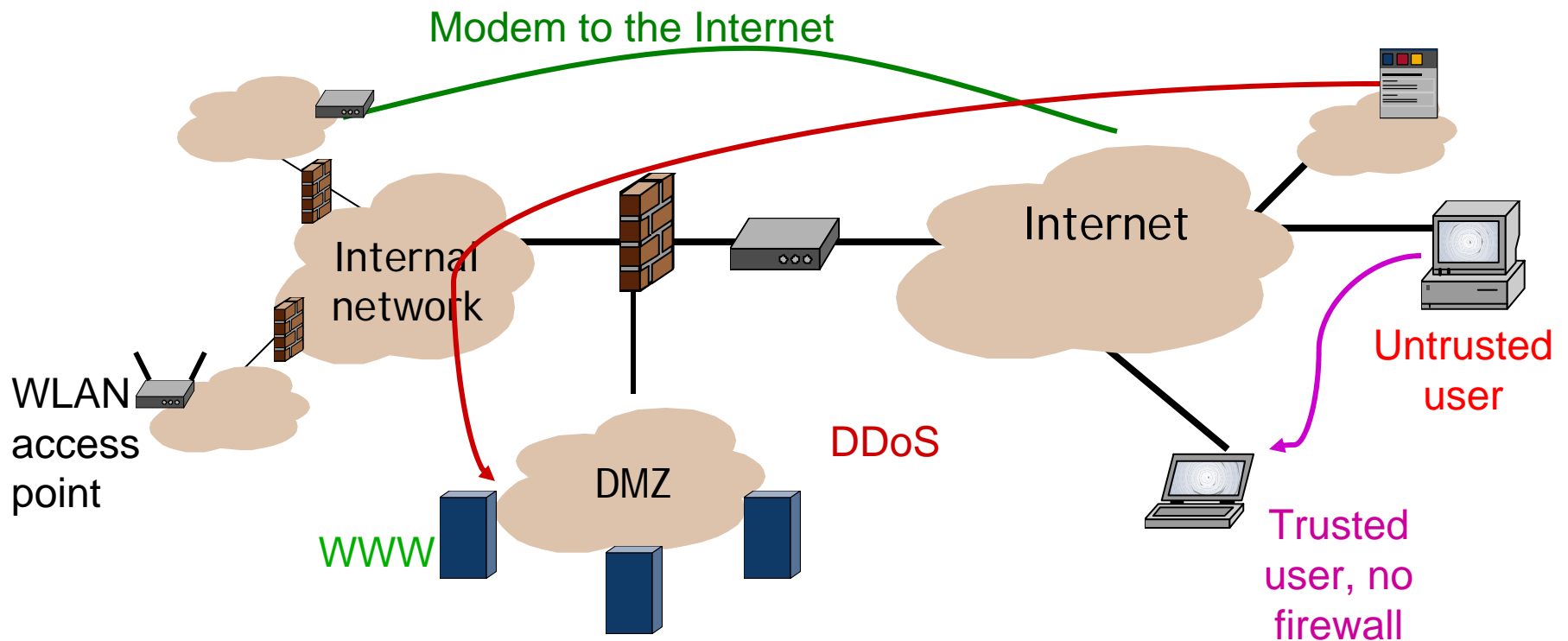
- Firewalls limit access to the network that they protect
- Encryption protects data in transit
- Cryptographic identification provides strong authentication





Networking Reality

- If left unsupervised, the security is going to be broken
- Your own users can break the security intentionally or unintentionally





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
- For example a a 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
 - Requirements must be made concrete and practical
- 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"
 - Most "exceptions" are really regular occurrences
 - Illnesses, deaths, vacations, hurry



- 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



- 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 decision making



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
- The field is known as Human Computer Interaction and Security (HCISEC)



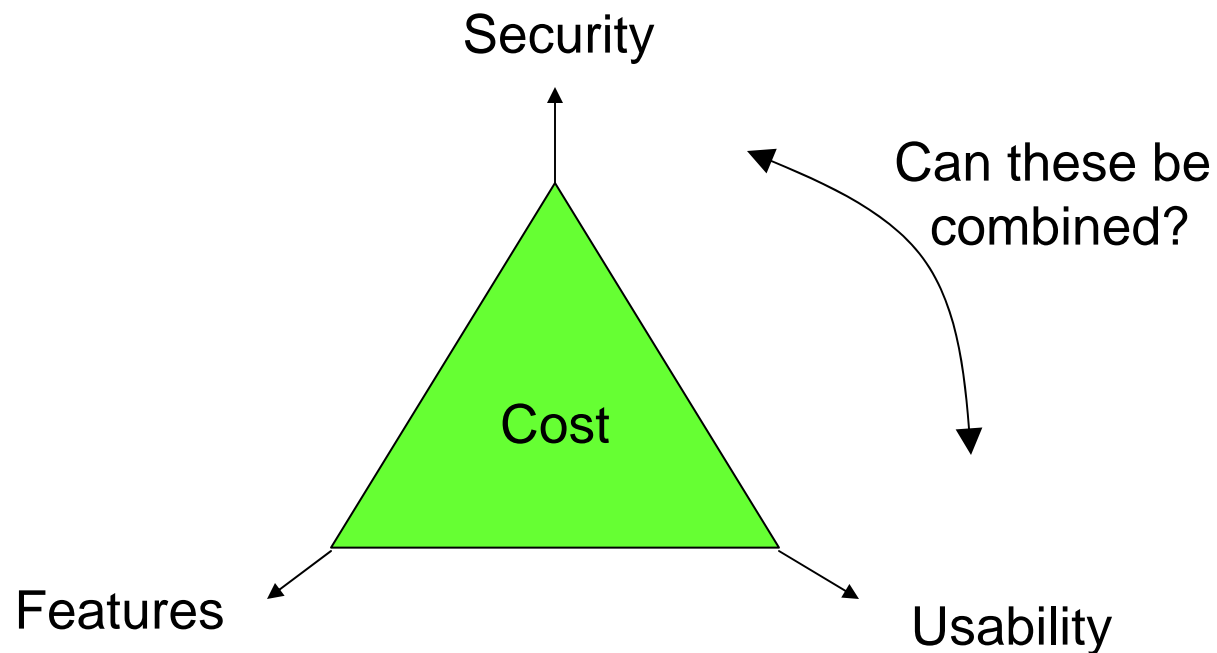
Usability Studies in Security Systems Design

- 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



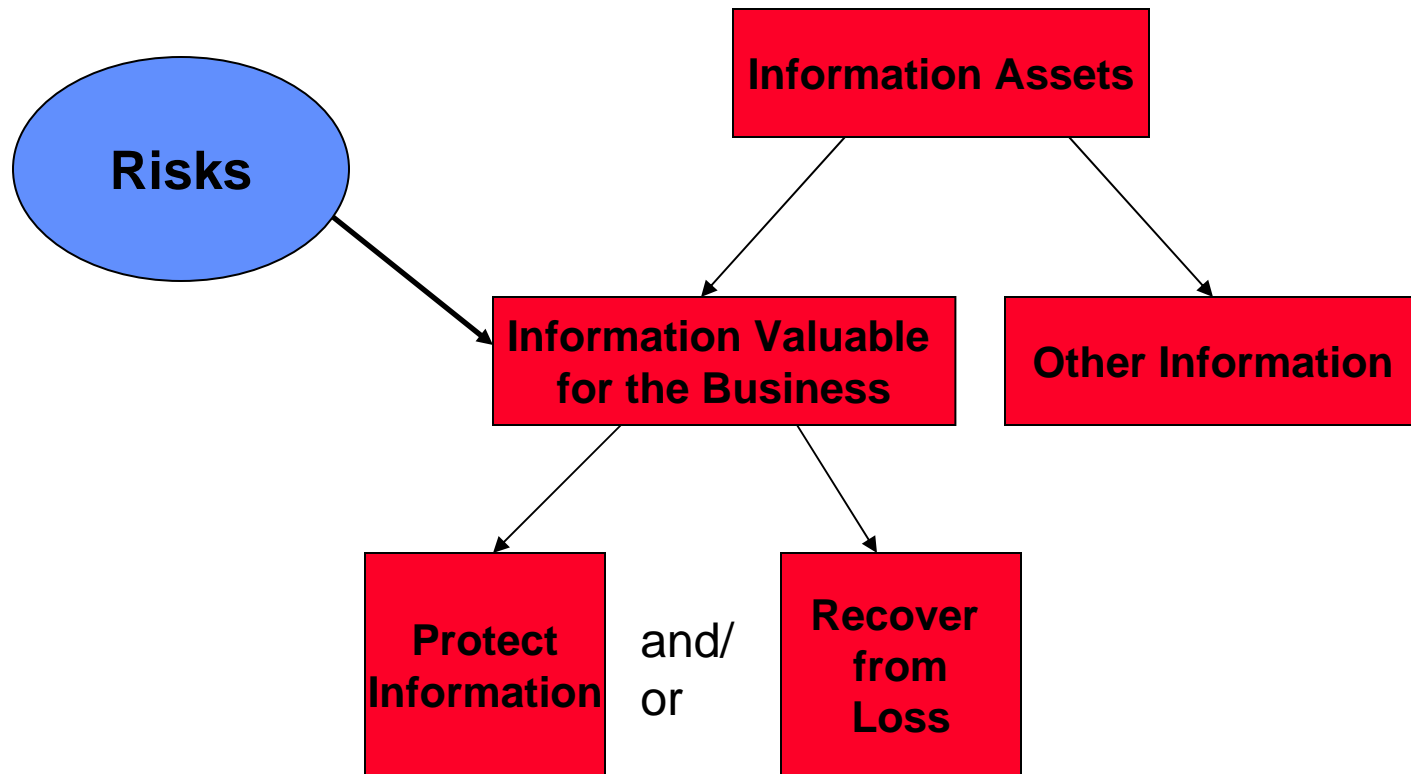


Security Is a Process

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



What to Secure?





Risk Management Is a Continuous Process

