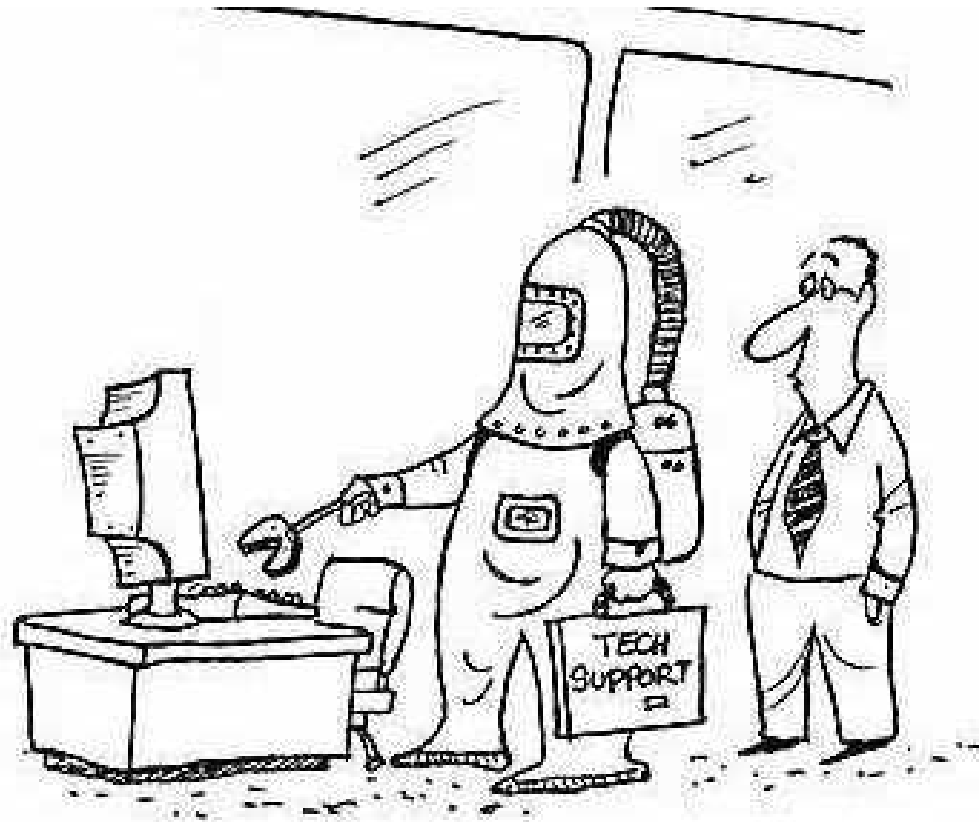


## Overview

- Risk Analysis
- Controls and Safeguards



"THE VIRUS IS THAT BAD, HUH?"

Source: <http://mashable.com>

## Risk Analysis

- ISO 27000 Series (International Standards Organization) – Security Management
- Objectives of Risk Analysis:
  - identify and categorize the risks to assets that threaten the regular operations of an organization – seems mundane, but this can make or break a company
  - provides info to managers to help them evaluate the risks and then determine how best to deal with (treat) them
  - likelihood of occurrence – and frequencies and times (depends on the type of business)
- risk likelihood can be categorized as: why do we care about rare risks?

Rating	Likelihood Description	Expanded Definition
1	<b>Rare</b>	May occur only in exceptional circumstances and may be deemed as “unlucky” or very unlikely.
2	<b>Unlikely</b>	Could occur at some time but not expected given current controls, circumstances, and recent events.
3	<b>Possible</b>	Might occur at some time, but just as likely as not. It may be difficult to control its occurrence due to external influences.
4	<b>Likely</b>	Will probably occur in some circumstance and one should not be surprised if it occurred.
5	<b>Almost Certain</b>	Is expected to occur in most circumstances and certainly sooner or later.

## Risk Analysis

- **Risk** = Probability that threat occurs x Cost to organization
- **Risk Appetite** = level of risk the organization views as acceptable
- Balance Risk Treatment --> with day to day productive functioning of a company
- The specified likelihood needs to be realistic
- In particular, a rating of **Likely** or higher suggests that this threat has occurred sometime previously.
- In contrast, the **Unlikely** and **Rare** ratings can be very hard to quantify.
  - they are an indication that the threat is of concern, but knowing whether it could potentially occur is difficult to specify.
  - typically such threats would only be considered if the **consequences** to the organization of their occurrence are so severe that they have to be considered, even if extremely improbable.

need to determine consequence

Determining Consequence

Rating	Consequence	Expanded Definition.
1	<b>Insignificant</b>	Generally a result of a minor security breach in a single area. Impact is likely to last less than several days and requires only minor expenditure to rectify.
2	<b>Minor</b>	Result of a security breach in one or two areas. Impact is likely to last less than a week, but can be dealt with at the segment or project level without management intervention. Can generally be rectified within project or team resources.
3	<b>Moderate</b>	Limited systemic (and possibly ongoing) security breaches. Impact is likely to last up to 2 weeks and generally requires management intervention. Will have ongoing compliance costs to overcome.
4	<b>Major</b>	Ongoing systemic security breach. Impact will likely last 4-8 weeks and require significant management intervention and resources to overcome, and compliance costs are expected to be substantial. Loss of business or organizational outcomes is possible, but not expected, especially if this is a once off.
5	<b>Catastrophic</b>	Major systemic security breach. Impact will last for 3 months or more and senior management will be required to intervene for the duration of the event to overcome shortcomings. Compliance costs are expected to be very substantial. Substantial public or political debate about, and loss of confidence in, the organization is likely. Possible criminal or disciplinary action is likely.
6	<b>Doomsday</b>	Multiple instances of major systemic security breaches. Impact duration cannot be determined and senior management will be required to place the company under voluntary administration or other form of major restructuring. Criminal proceedings against senior management is expected, and substantial loss of business and failure to meet organizational objectives is unavoidable.



## How CTOs/ CIO make the big bucks

- Once the likelihood and consequence of each specific threat have been identified, a final level of risk needs to be assigned.
- This is typically determined using a **table** that maps these values to a risk level
- This table details the risk level assigned to each combination.
- Such a table provides the qualitative equivalent of performing the ideal risk calculation using quantitative values.
- It also indicates the interpretation of these assigned levels.

Resultant Risk Register

	Consequences					
Likelihood	Doomsday	Catastrophic	Major	Moderate	Minor	Insignificant
Almost Certain	E	E	E	E	H	H
Likely	E	E	E	H	H	M
Possible	E	E	E	H	M	L
Unlikely	E	E	H	M	L	L
Rare	E	H	H	M	L	L

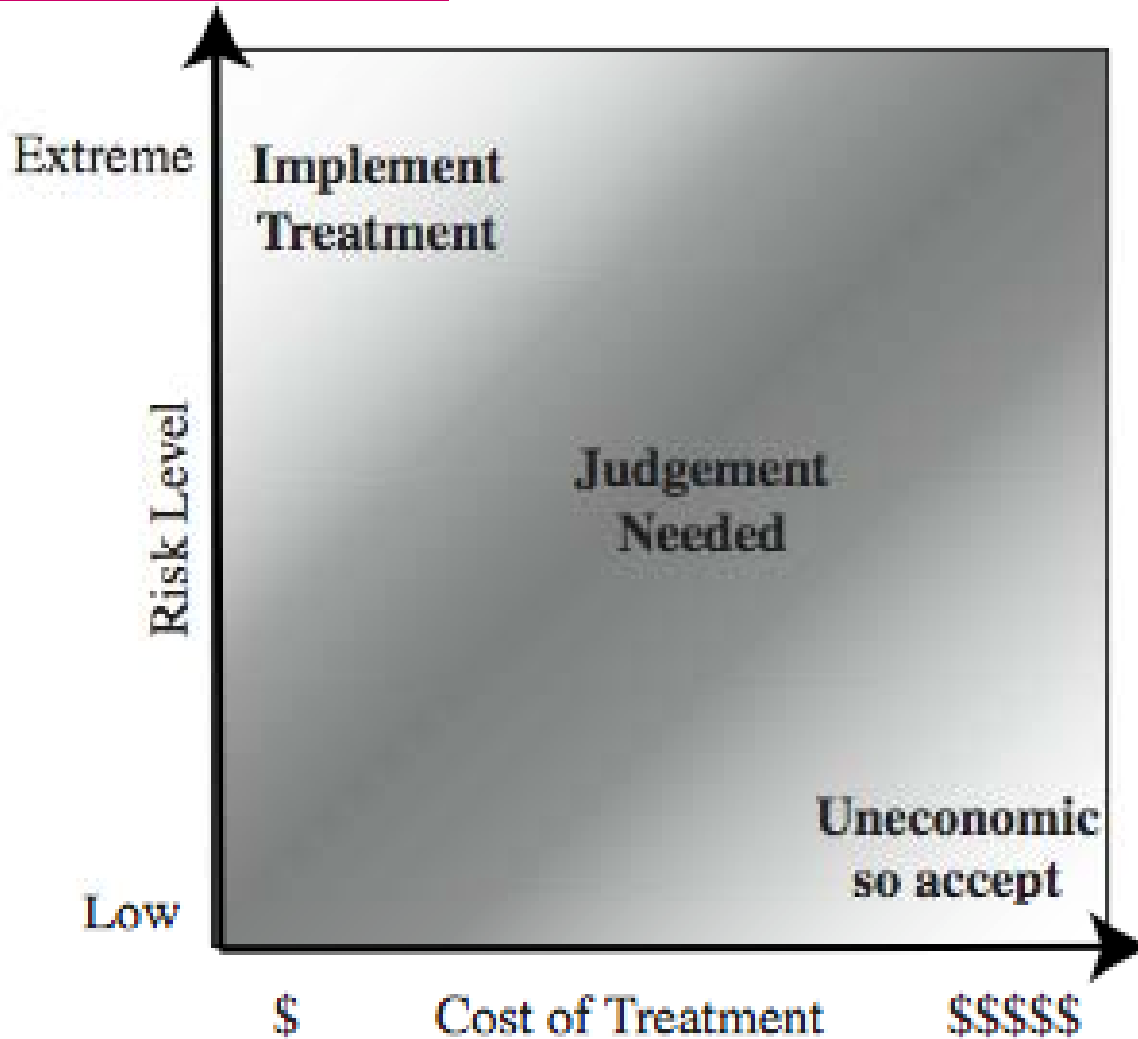
Risk Level	Description
Extreme (E)	Will require detailed research and management planning at an executive/director level. Ongoing planning and monitoring will be required with regular reviews. Substantial adjustment of controls to manage the risk are expected, with costs possibly exceeding original forecasts.
High (H)	Requires management attention, but management and planning can be left to senior project or team leaders. Ongoing planning and monitoring with regular reviews are likely, though adjustment of controls are likely to be met from within existing resources.
Medium (M)	Can be managed by existing specific monitoring and response procedures. Management by employees is suitable with appropriate monitoring and reviews.
Low (L)	Can be managed through routine procedures.

## Example Risk Register

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Internet Router	Outside Hacker attack	Admin password only	Possible	Moderate	High	1
Destruction of Data Center	Accidental Fire or Flood	None (no disaster recovery plan)	Unlikely	Major	High	2

- Asset: anything that has value to the organization
- Threat/ Vulnerability:
  - who
  - why (motivations and capabilities)
  - where
  - when (including probability of attack)
  - How (with what resources)

## Risk Treatment



- Management may decide that for business reasons, given an overall view of the organization, some risks with lower levels should be treated ahead of other risks.

## Risk Treatment Alternatives

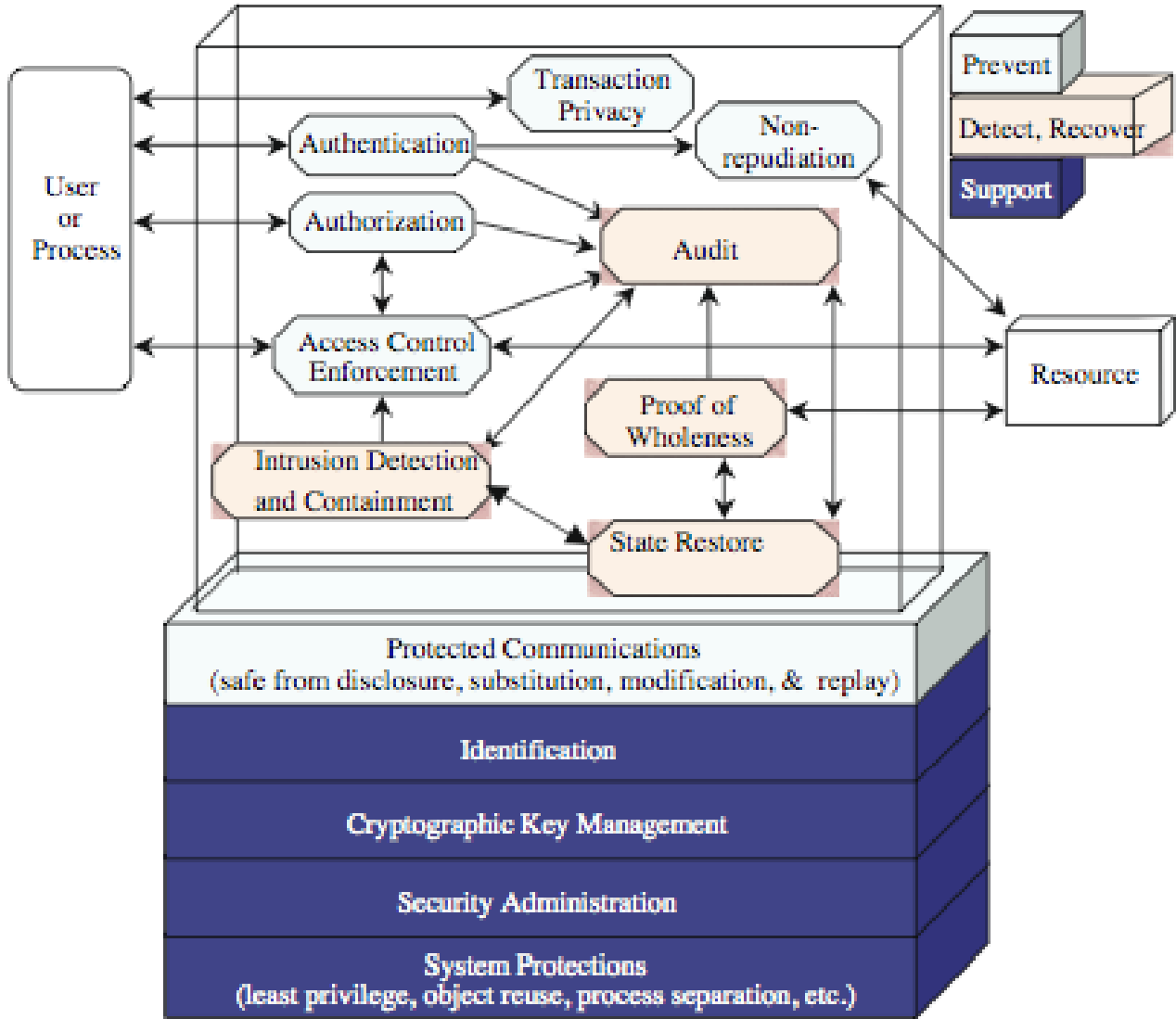
- There are five broad alternatives available to management for treating identified risks:
  - **risk acceptance:** of a risk level greater than normal for business reasons, typically due to excessive cost or time needed to treat the risk.
  - **risk avoidance:** not continuing with the activity or system which creates this risk, resulting in loss of convenience or ability to perform some function that is useful to the organization, but traded off against the reduced risk profile.
  - **risk transfer:** sharing responsibility for the risk with a third-party. This is typically achieved by taking out insurance against the risk occurring, by entering into a contract with another organization, or by using partnership or joint venture structures to share the risks and costs should it eventuate
  - **reduce the consequence:** by modifying the structure or use of the assets at risk to reduce the impact on the organization should the risk occur, e.g. implementing an offsite backup process, developing a disaster recovery plan, or arranging for data and processing to be replicated.
  - **reduce the likelihood:** by implementing suitable controls to lower the chance of the vulnerability being exploited. These could include technical or administrative controls such as deploying firewalls and access tokens, or procedures such as password complexity and change policies.

### Controls and Safeguards (to reduce consequence and likelihood)

If either of the last two options is chosen, then possible **treatment controls** need to be selected, and their cost effectiveness evaluated.

- controls or safeguards are
  - practices, procedures or mechanisms which may protect against a threat, reduce a vulnerability, limit the impact of an unwanted incident, detect unwanted incidents and facilitate recover
  
- 3 main classes of controls:
  - **management control:** focus on security policies, planning, guidelines and standards which then influence/ determine the selection of operational and technical controls.
  
  - **operational:** address the correct implementation and use of security policies and standards – how is it carried out
  
  - **technical controls:** involve the correct use of hardware and software security capabilities in systems (resources)

Technical Controls: supportive, preventive, detection & recovery



## Examples of Control

<b>CLASS</b>	<b>CONTROL FAMILY</b>
Management	Risk Assessment
Management	Planning
Management	System and Services Acquisition
Management	Certification, Accreditation, and Security Assessments
Operational	Personnel Security
Operational	Physical and Environmental Protection
Operational	Contingency Planning
Operational	Configuration Management
Operational	Maintenance
Operational	System and Information Integrity
Operational	Media Protection
Operational	Incident Response
Operational	Awareness and Training
Technical	Identification and Authentication
Technical	Access Control
Technical	Audit and Accountability
Technical	System and Communications Protection

## Cost Benefit Analysis

- conducted to determine appropriate controls
  - what are the greatest benefits, given resources available
- qualitative or quantitative
- show cost justified by reduction in risk
- contrast impact of implementing it to not implementing
- management chooses selection of controls
- considers if it reduces risk too much or not enough, is too costly or appropriate
- fundamentally a business decision
- and depends on ...?

## Implementation Plan

tables, tables, tables ...

Risk (Asset/Threat)	Level of Risk	Recommended Controls	Priority	Selected Controls	Required Resources	Responsible Persons	Start – End Date	Other Comments
Hacker attack on Internet Router	High	<ol style="list-style-type: none"> <li>1. disable external telnet access</li> <li>2. use detailed auditing of privileged command use</li> <li>3. set policy for strong admin passwords</li> <li>4. set backup strategy for router config file</li> <li>5. set change control policy for the router configuration</li> </ol>	1	<ol style="list-style-type: none"> <li>1.</li> <li>2.</li> <li>3.</li> <li>4.</li> <li>5.</li> </ol>	<ol style="list-style-type: none"> <li>1. 3 days IT net admin time to change &amp; verify router config, write policies;</li> <li>2. 1 day of training for net admin staff</li> </ol>	John Doe, Lead Network Sys Admin, Corporate IT Support Team	1-Feb-2006 to 4-Feb-2006	1. need periodic test & review of config & policy use

## Security Training and Awareness

- responsible personnel need training
  - on details of design and implementation
  - awareness of operational procedures
  
- also need general awareness for all
  - spanning all levels in organization
  - essential to meet security objectives
  - aim to convince personnel that risks exist and breaches may have significant consequences – ultimately to their own jobs – make them connect to the problem personally

### Keeping all personnel involved

- reports from users or admin staff
  - encourage such reporting (denial of access, deletion of expected items on db)
  
- detected by automated tools
  - e.g. server log analysis tools, network and host intrusion detection systems, intrusion prevention systems
  - updated to reflect new attacks or vulnerabilities
  
- sys admins must monitor vulnerability reports
  
  
- respond
  
  
- document