

Keele University

IS security and control

? Keele 2002. All rights reserved.

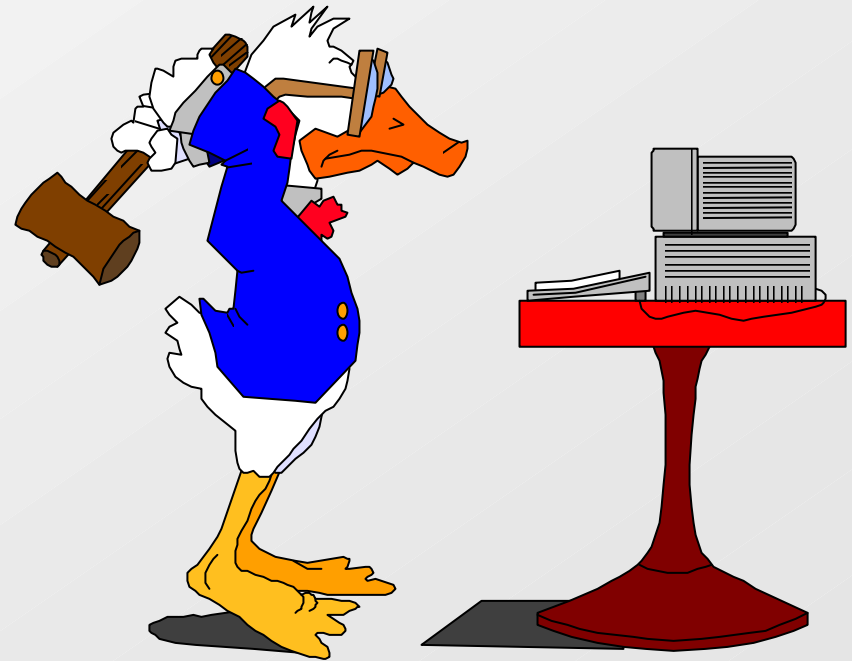
The copyright in this document is vested in Keele University. The document must not be reproduced by any means, in whole or in part, or used for manufacturing purposes, except with the prior written permission of Keele University and then only on condition that this notice is included in any such reproduction.

Information contained in this document is believed to be accurate at the time of publication, but no liability whatsoever can be accepted by Keele University arising out of any use made of this information.

Under the Copyright, Designs and Patents Act 1988, Stephen Bostock & Stephen Linkman assert the moral right to be identified as authors of this work.

Overview

- ✍ the importance of control
- ✍ sources of problems
- ✍ IS controls
- ✍ procedural controls
- ✍ facility controls
- ✍ standards and auditing



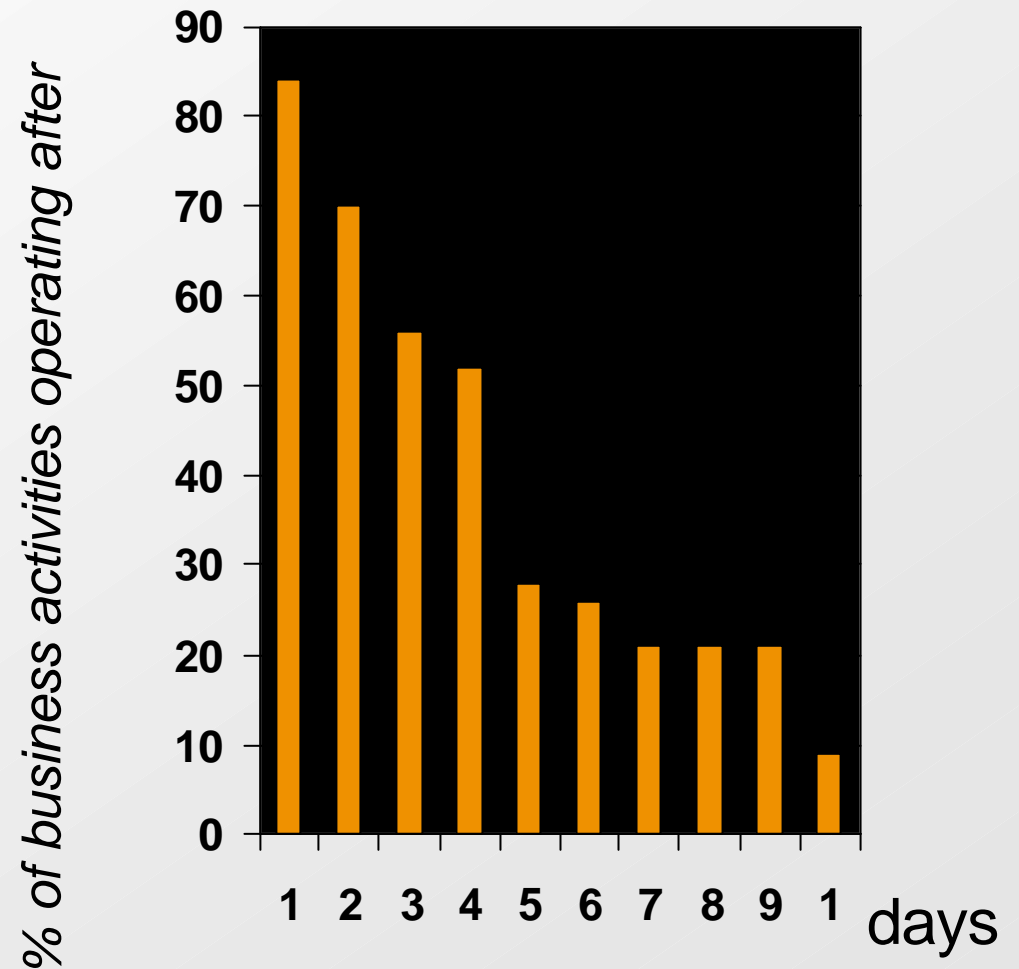
Why is security and control important?

- ✍ IS management is responsible for quality, performance and security
- ✍ errors do occur in systems
- ✍ computers are used for fraud
- ✍ systems are damaged accidentally/ maliciously
- ✍ errors are harder to detect than in manual systems, fewer people involved and much automation not checked routinely
- ✍ effective controls needed for IS security, to provide quality assurance

Dependence on IT

IS function is life or death for many businesses

it takes a few days to have effect but most businesses disappear after a major computer failure



Some possible security breaches

- ✎ fire, flood, natural disasters
- ✎ vandalism, sabotage
- ✎ theft
- ✎ unauthorized access
- ✎ invalid data entry
- ✎ breakdown, software errors
- ✎ loss of external services
- ✎ overload
- ✎ unforeseen knock-on effects
- ✎ industrial action, internal/external, loss of staff

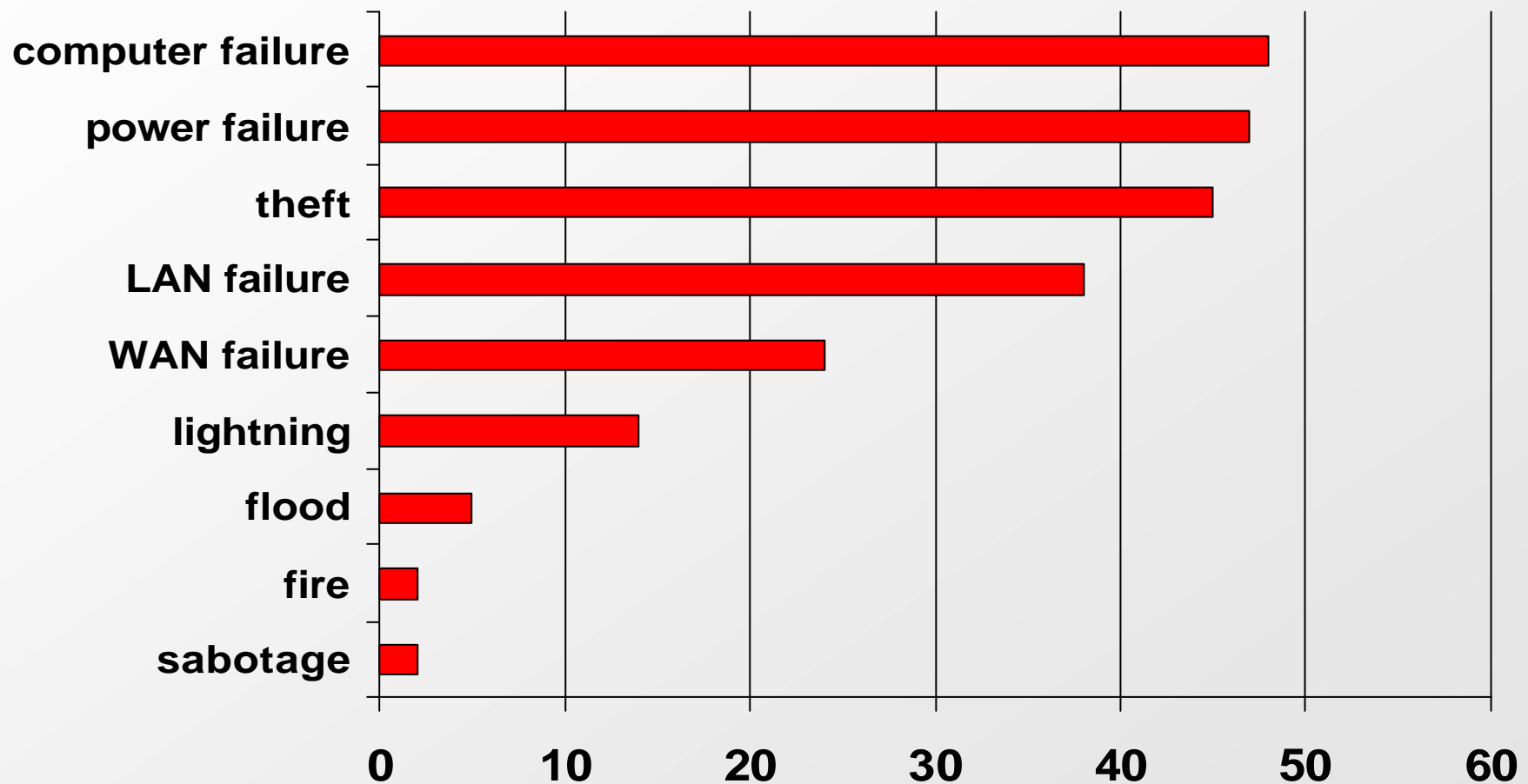
Dimensions of security

- ✍ type of problem - logical or physical
- ✍ source of problem - internal or external
- ✍ perpetrator - human or non-human
- ✍ intent (human) - accidental or deliberate
- ✍ consequences - loss of:
 - Confidentiality
 - insecure access, unauthorized disclosure
 - Integrity
 - data accuracy, completeness, reliability
 - Availability
 - loss, damage, access

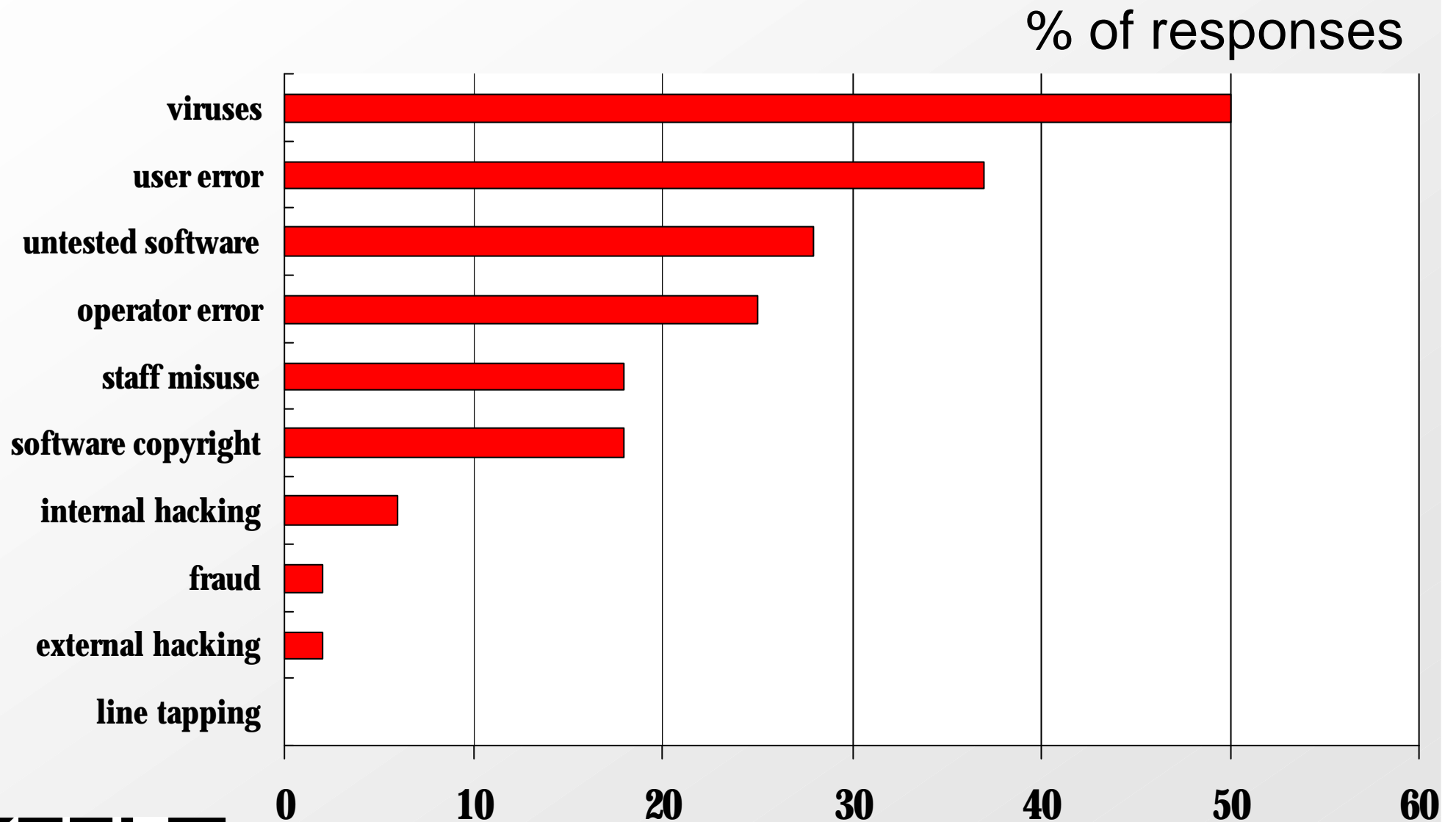
} 'CIA'

Incidences of physical breaches

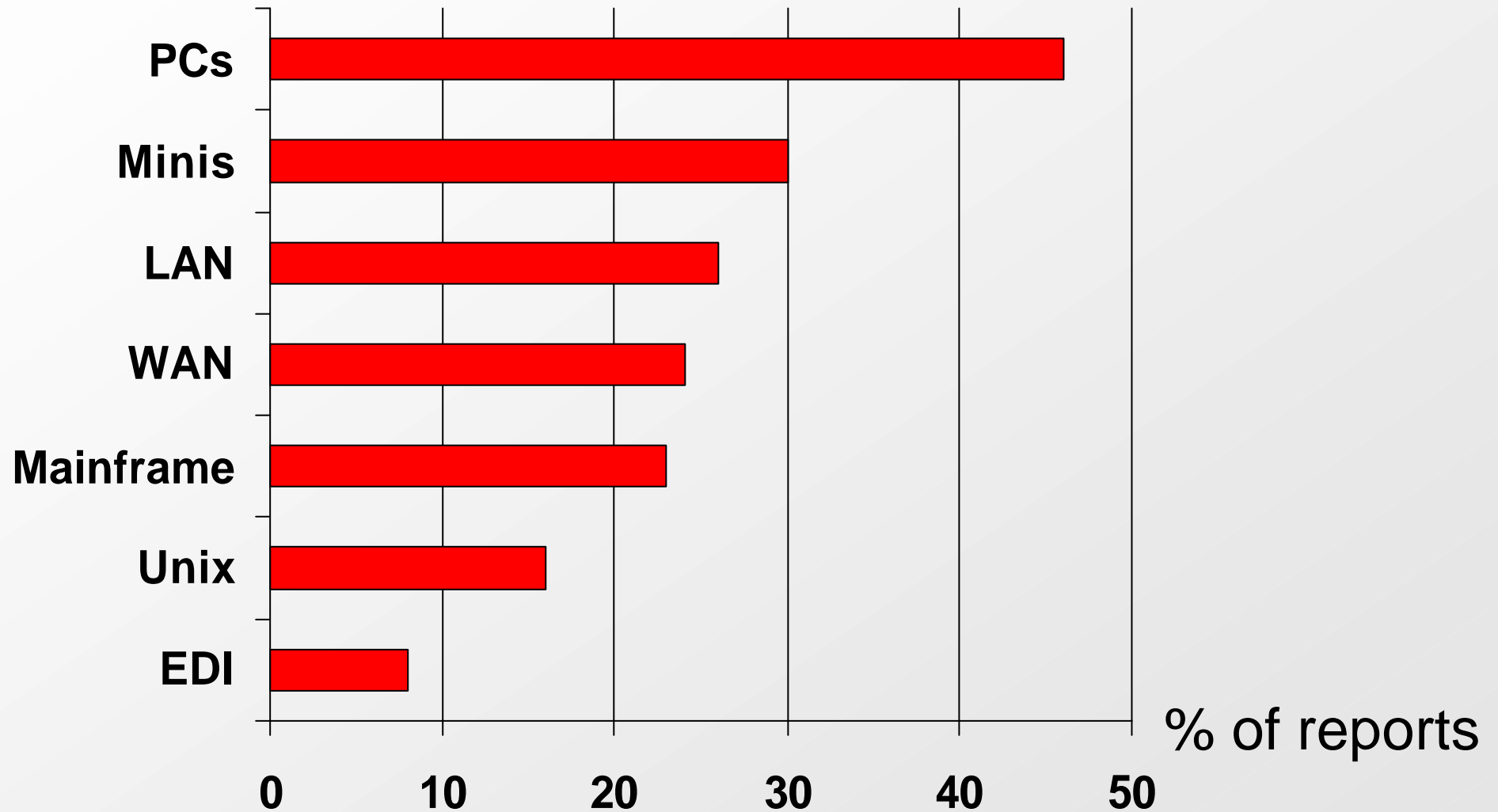
% of responses



Incidences of logical breaches



Systems most at risk



Mainframe security threats

 crime

 fire

 viruses

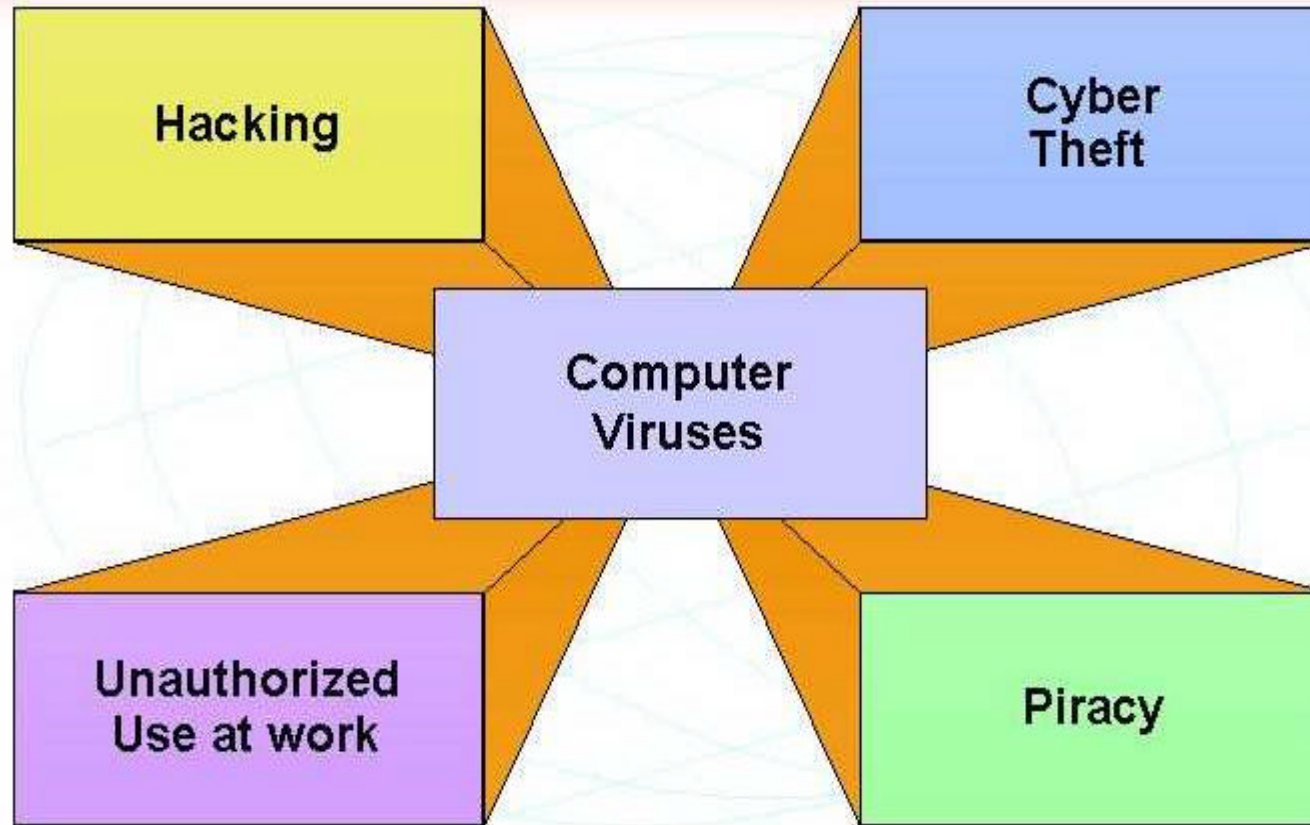
 hacking

 flood



cost of an incident

5 Computer Crime



Viruses

- ✂ programs designed to copy themselves through a computer system, possibly doing damage: sophisticated vandalism. In excess of 1,400.
- ✂ spread through executable programs, not data, except macro document viruses e.g. Word
- ✂ e.g. in 1992, 60% of UK organizations had a virus infection
- ✂ major source is unofficial software brought in by staff, but the Internet will become a problem.
- ✂ mostly nuisance and prevention is costly
- ✂ staff awareness most important

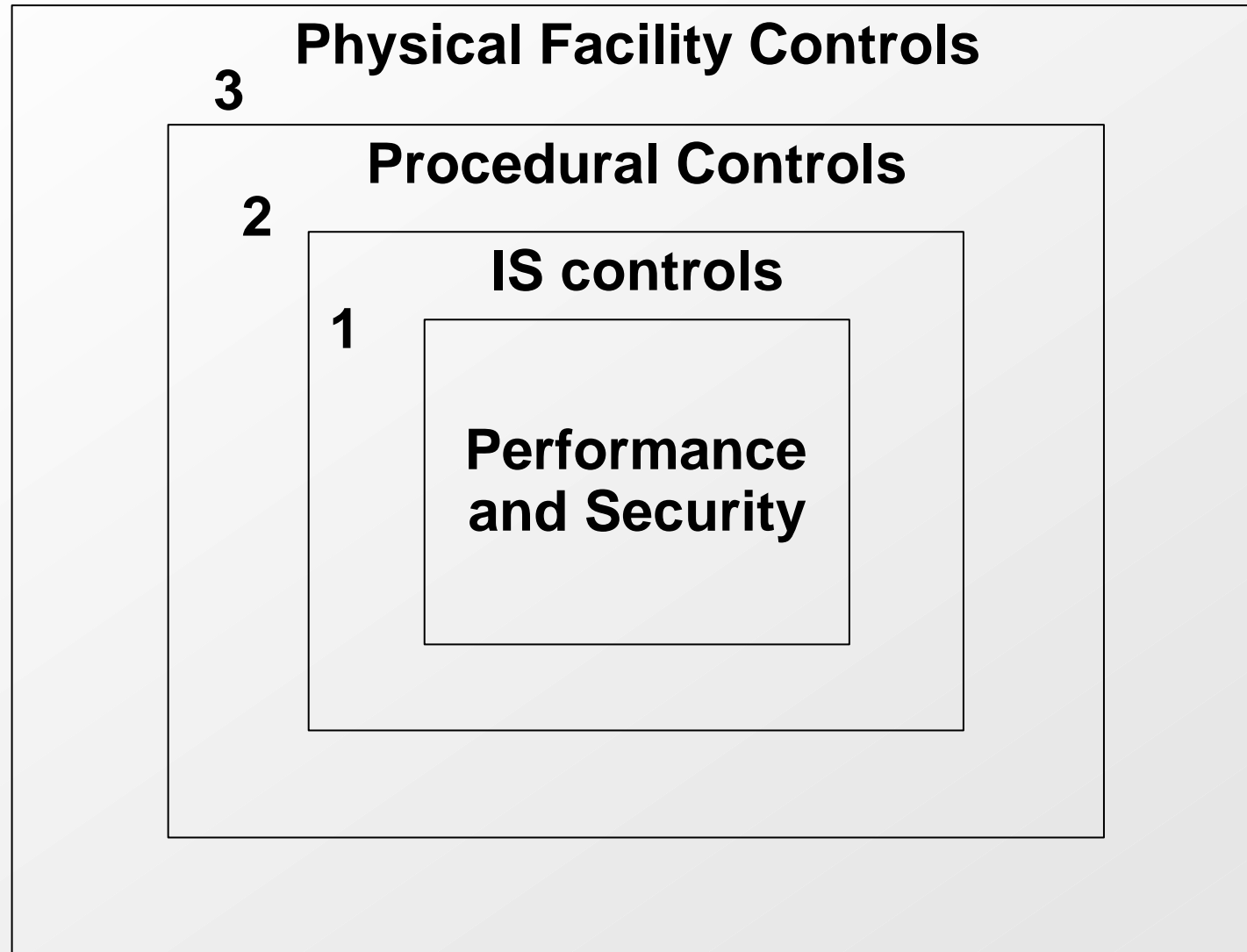
Hacking

- ✎ perception of criminal penetration, in fact mostly by staff attempting unauthorized entry
- ✎ once entry is gained, can do damage or theft or gain information
- ✎ vulnerability depends on
 - physical and logical access control
 - larger wider networks at more risk
 - value of data: higher value, more incentive to break in

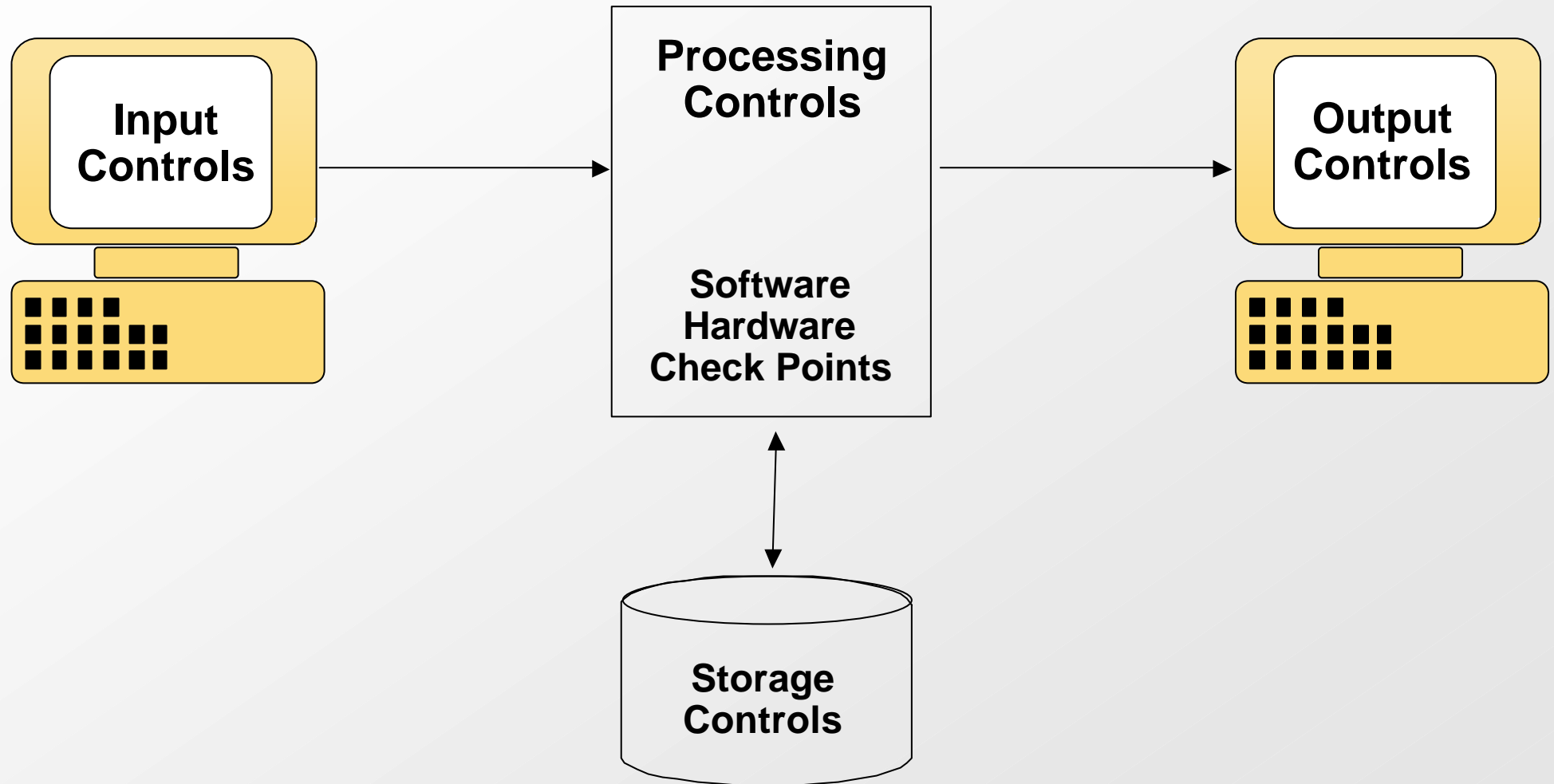
Online non-work related employee activity and corporate policies.



Major Types of Controls



1. Information System Controls



Input controls

controls on input, processing, output, storage

- ✍ GIGO - garbage in, garbage out
- ✍ data entry screens, keyboard masks, prenumbered and prerecorded forms
- ✍ logbooks of source documents, control log files of all real-time entries
- ✍ validation of data input by type, range, sequence
- ✍ control totals used for batches, hash totals

Processing controls

- ✍ checks that data is not lost, or missed from processing
- ✍ any errors in arithmetic or logic are identified
- ✍ hardware controls
 - redundant components, repeat processing
 - malfunction detection, such as parity checks
- ✍ software controls
 - operating system checks on file name and size
 - audit trail of the steps of processing
 - specialist software 'system security monitors' restrict access to resources, hardware and software

Output controls

- ✍ control the quality of information products
- ✍ similar to input controls
- ✍ output documents logged, identified, verified by staff
- ✍ control totals on output compared with those in processing
- ✍ distribution lists for output documents
- ✍ prenumbered forms for important documents
- ✍ real-time output controlled by access
- ✍ ask users on the quality of output

Storage controls

- ✍ database administrators responsible for organizing and securing files
- ✍ access controls limit access to parts of the filestore: username, password
- ✍ passwords can be chosen by user but forced changes regularly, minimum length (6 chars)
- ✍ different passwords for read and write access
- ✍ passwords can be encrypted, or call-back used for remote access
- ✍ limited login tries, then delay to prevent hacking

Example: Unix security

- ✍ login created by administrator
- ✍ password (3 to 8 characters), can be aged to force change
- ✍ user categories:
owner, group, other
- ✍ access to files and directories:
read, write, execute
- ✍ accounting logs (*accton*) record users' activity
- ✍ `ls -l` lists files and permissions
- ✍ `chmod [u,g,o,a] [+,-] [rwx] filename`

Back-up - 1

dual recording

- maintain two live copies - then one may be undamaged

dumping

- regular, frequent copies made
master copies and interim transactions
log of interim, log of master back-ups
copies on site and off site, each updated

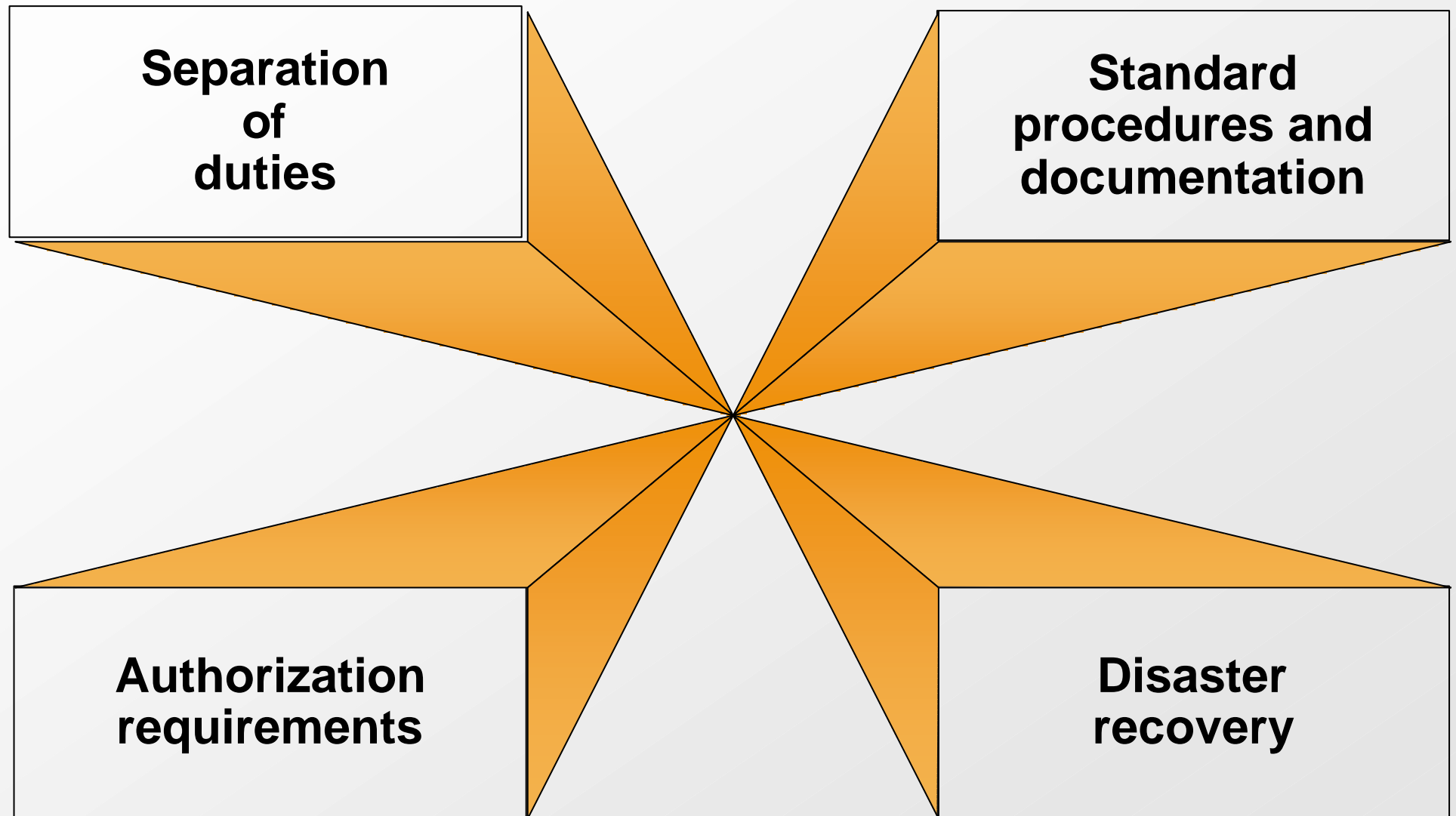
audit trail

- log of all inputs and updates as before-looks or after-looks
- before-looks + transaction tapes restore current data

Back-up - 2

- ✍ a weakness in all backups is that errors can occur during recording of back-ups and logs
- ✍ therefore two or more generations of back-ups are needed
 - for example, 1 day old copy on site, 2 day old copy off site, each replaced daily
- ✍ there is no foolproof back-up protection!

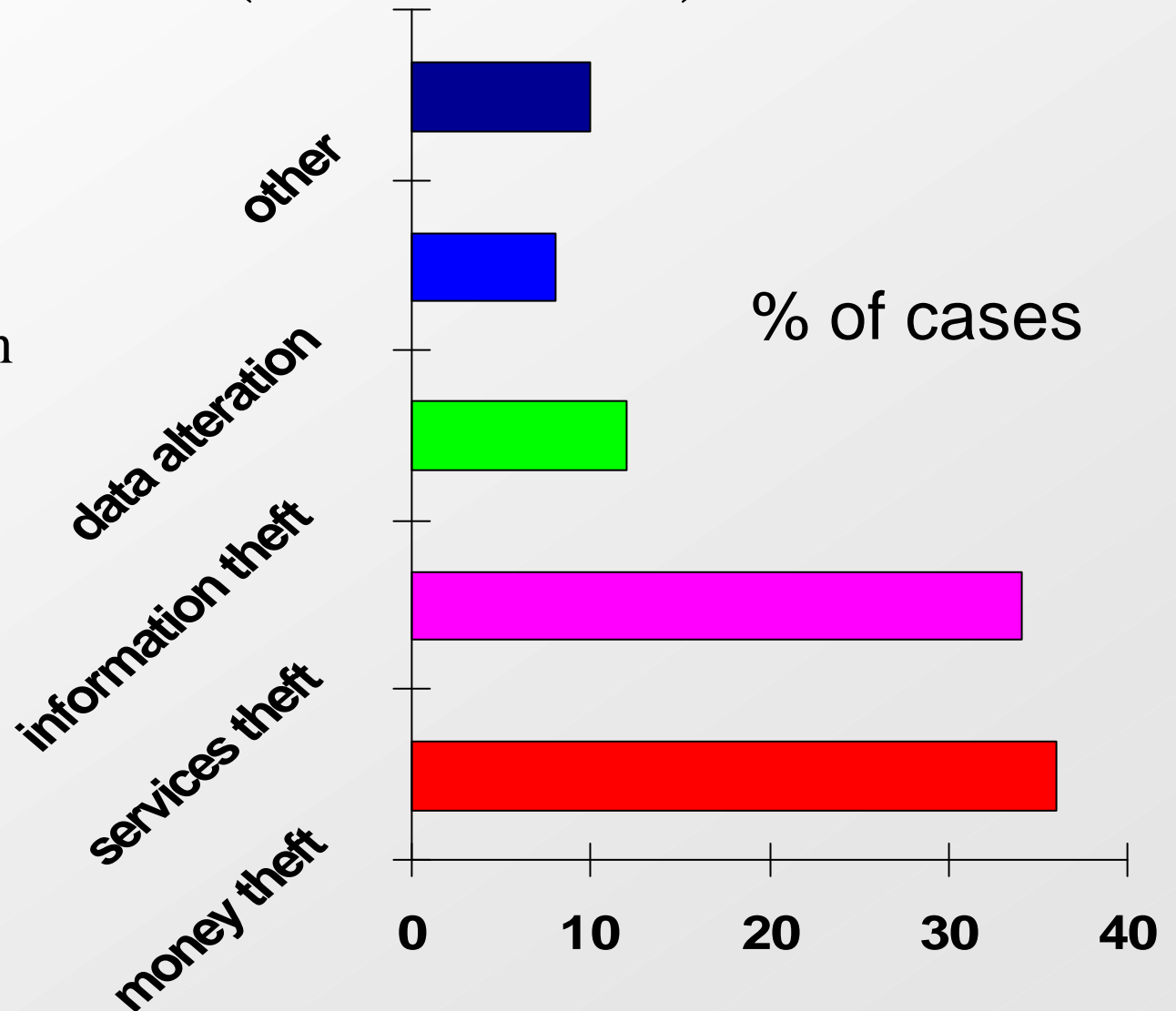
2. Procedural Controls



Staff involvement in security problems (NCC data)

✂ staff are vital to security

✂ training needed in procedures, and awareness



Procedural controls

- separation of duties

- ✍ separation (segregation) of duties is a basic principle
- ✍ should be no instances where one person is responsible for using the system AND setting, implementing and its policing controls
- ✍ different groups must be responsible for
 - development, input media, operating, documentation and archives, output
- ✍ each group, with different access rights, must check on each others' work

Procedural controls

- procedures and documentation

- ✍ standard procedures and documentation must be available and maintained
- ✍ to minimize both error and fraud
- ✍ for both normal running and emergencies

Procedural controls

- authorization requirements

before requests for changes to system

-  have a formal review to minimize detrimental effects on the integrity of the IS service

Procedural controls

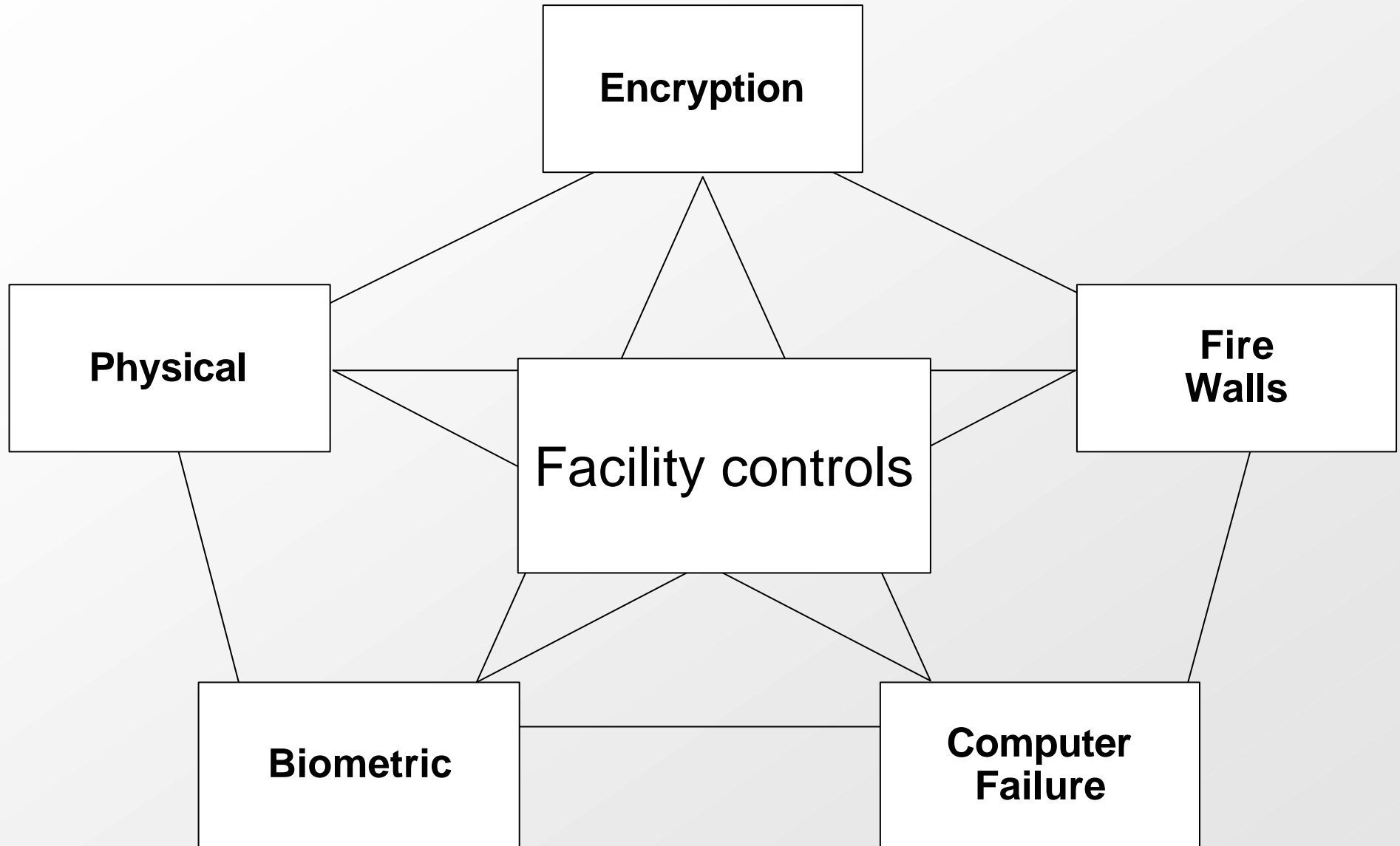
- disaster recovery

- ✎ disasters do happen: man-made and natural
- ✎ for a business to survive disaster it must have a written recovery (contingency) plan, specifying
 - who does what,
 - what facilities to be used, and
 - the priority of applications to be processed.
- ✎ a manual fall-back system is possible for short periods to maintain cash flow, management information and customer support

Disaster recovery

- ✍ a 'hot' standby scheme is use of an existing, similar system for temporary use
- ✍ a 'cold' standby scheme
 - is an in-house emergency computer room, or
 - subscribe to use of a fixed, or portable, emergency computer centre
- ✍ the backup files must survive
- ✍ tests, drills and exercises are needed

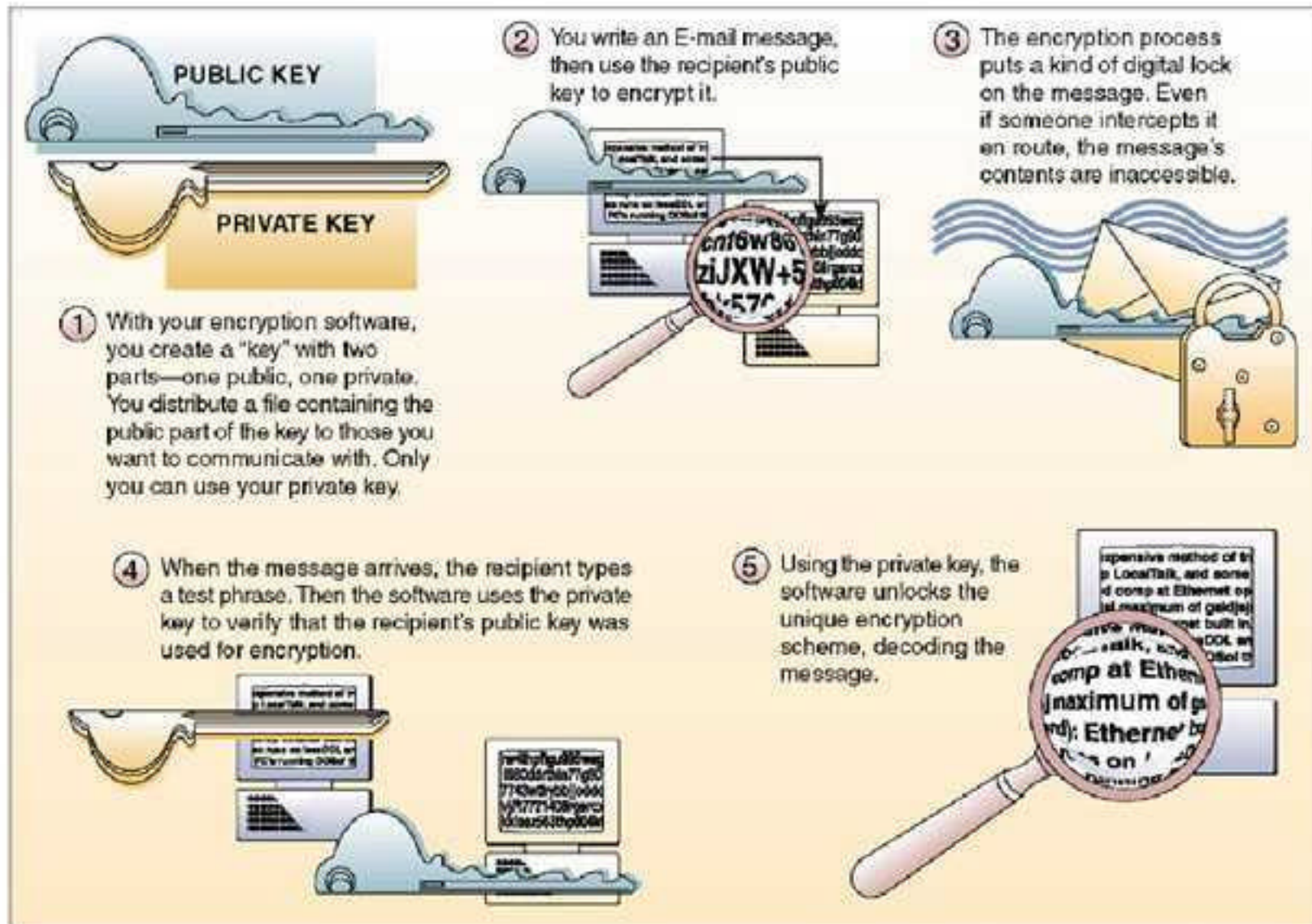
3. Facility Controls



Facility controls- encryption

- ✍ 'scrambling' data before communicating it
- ✍ an algorithm or numerical 'key' is used to scramble it, and is needed to de-scramble it
- ✍ several algorithms used: DES, RSA, PGP
- ✍ scrambled data can be hidden e.g. in pictures
- ✍ US etc. government surveillance is against strong encryption, business wants it
- ✍ clipper chip and 'trusted third party' (TTP) systems allow governments/police to hold all keys

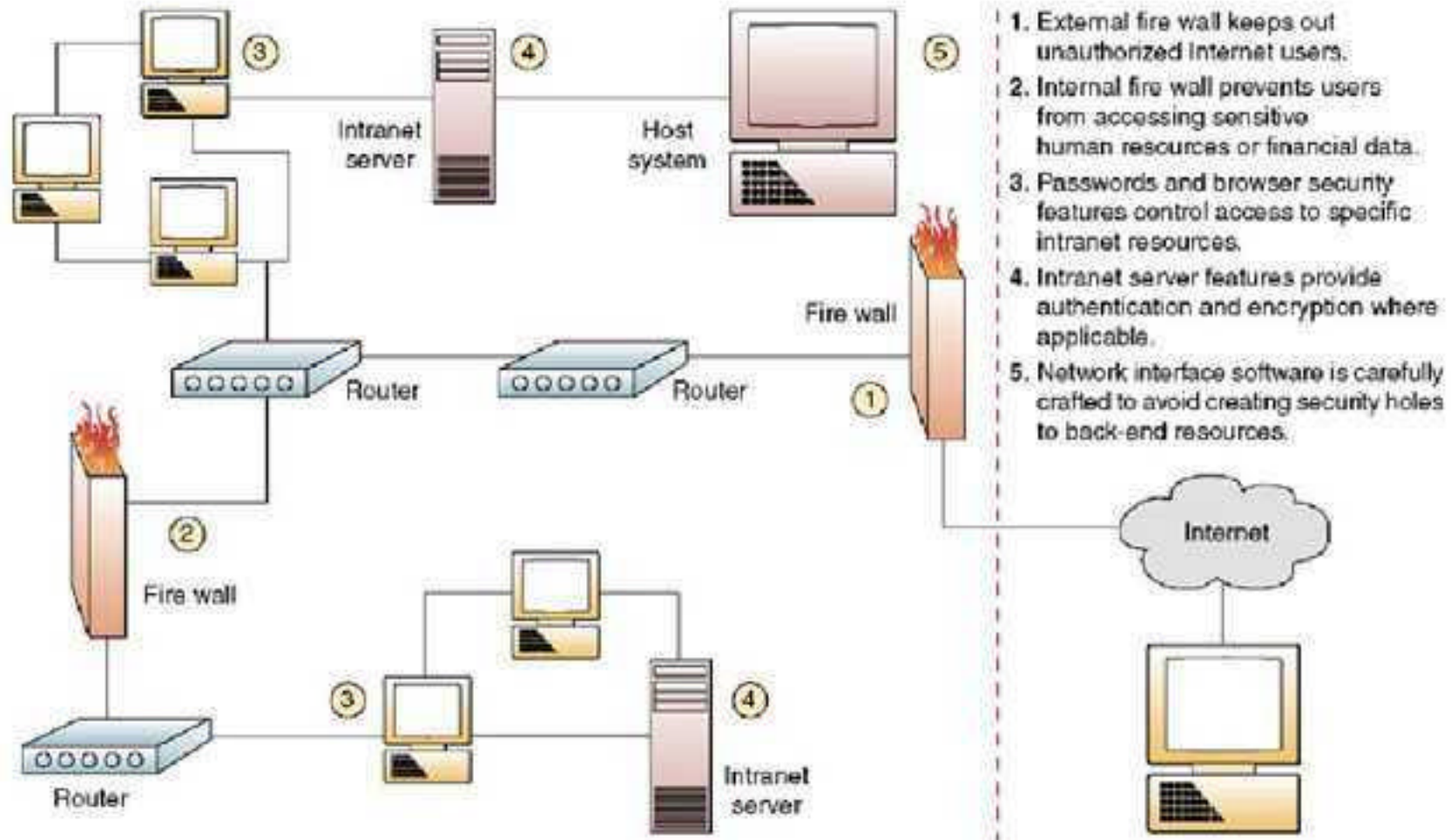
How public key/private key encryption works.



Facility controls - firewalls

- ✍ (communication controls - could be considered under processing controls)
- ✍ networks give remote access to IS: to whom?
- ✍ a network firewall is a computer that protects a network from intrusion by screening all traffic, allowing only authorized access in and out.
- ✍ different access for different services
 - e.g. get email but not run programs or write to files
- ✍ access only from specific locations
- ✍ necessary on an Internet server

An example of the Internet and intranet fire walls in a company's networks.



Facility controls

- physical threats

- ✍ include sabotage, vandalism, accident
- ✍ access protection/control: general security
- ✍ electricity supplies: Uninterrupted Power Supply
- ✍ fire extinguishers: halon gas is expensive, carbon dioxide is cheaper and good for small electrical fires, powder and water damage equipment - only to prevent spread
- ✍ weather - cables are at risk of flood, mainframes need air conditioning
- ✍ hardware failure - especially moving parts, maintenance is cheaper if <15% of total costs

Facility controls

- biometric & identification

✍ biometric controls

- special sensors to identify voice, fingerprint, signature, retina patterns, or face patterns

✍ identification badges, electronic door locks, cards, tokens

- punch cards are cheap and disposable
- infra-red readable ones are more secure
- stripe cards, or magnetic cards with wire pattern
- proximity cards or tokens emit a radio signal
- smart cards disclose data when prompted

Facility controls

- computer failure

- ✍ what percentage is down-time?
- ✍ prevention of down-time - maintenance is needed to minimize it
- ✍ preventative measures are taken, with contingency plans using a backup facility
- ✍ fault tolerant systems have multiple processors and peripherals, used as necessary
 - fail-safe continues the full service
 - fail-soft continues at reduced service

Summary of security measures

- ✍ staff training and awareness
- ✍ physical isolation against damage, accident
- ✍ regulation of access by various means
- ✍ encryption is expensive, only for sensitive data
- ✍ back-ups essential
- ✍ risk assessment and contingency plans
- ✍ cost/benefits assessed

BS7799 - British Standard on Information Security Management -1

10 key security controls

1. A written policy document should be available to all employees responsible for information security.
2. Responsibilities for the protection of individual assets and for carrying out specific security processes should be explicitly defined.
3. Users should be given adequate security education and technical training.
4. Security incidents should be reported through management channels as quickly as possible.

BS7799 - British Standard on Information Security Management - 2

5. Virus detection and prevention measures and appropriate user awareness procedures should be implemented.
6. There should be a managed process in place for developing and maintaining business continuity plans across the organization.
7. Attention is drawn to the legal restrictions on the use of copyright material.
8. Important records of an organization should be protected from loss, destruction & falsification.

BS7799 - British Standard on Information Security Management - 3

9. Applications handling personal data on individuals should comply with data protection legislation and principles.
10. All areas within the organization should be considered for regular review to ensure compliance with security policies and standards.

Auditing IS

- ✍ periodic examinations of the system either by internal or external staff
- ✍ auditing ‘around’ the computer verifies the correctness of input and output
- ✍ auditing ‘through’ the computer verifies processing as well, using computer records
- ✍ an audit trail records all stages of a transaction's progress. Harder than for manual systems. Auditing personnel should be part of project teams, and consulted about changes.

Summary

- ✍ the importance of control
- ✍ sources of problems
- ✍ IS controls
- ✍ procedural controls
- ✍ facility controls
- ✍ standards and auditing