Cyber Security

11 July 2011

From "Computer Security" to "Information Assurance": Evolving Doctrines & Consequences

Peter Sommer

London School of Economics

OECD Reviews of Risk Management Policies

Future Global Sh

IMPROVING RISK GOVERNAN

OECD

PRELIMIN

OECD 50

BETTER POLICIES FOR BETTER LIVES

MULTI-DISCIPLINARY ISSUES

INTERNATIONAL FUTURES PROGRAMME

OECD/IFP Project on

"Future Global Shocks"

"Reducing Systemic Cybersecurity Risk"

Peter Sommer, Information Systems and Innovation Group, London School of Economics

Ian Brown, Oxford Internet Institute, Oxford University

LSE

Why a Global Cyber Shock is Unlikely

- People don't immediately die
- Physical destruction of assets is rare
- Essential networks are designed for resilience
- Essential data is easily backed-up
- But localised disruption, misery and loss are all too feasible!

What Makes a Global Shock?

- **Ingredients of Triggering Event**
  - ➔ **All the ingredients to cause an event and their likelihood**
- **Potential for Overloading Affected System**
- **Potential to Cascade into other Systems**
- **Tipping Points where there is no quick return to “normal life”**

LSE

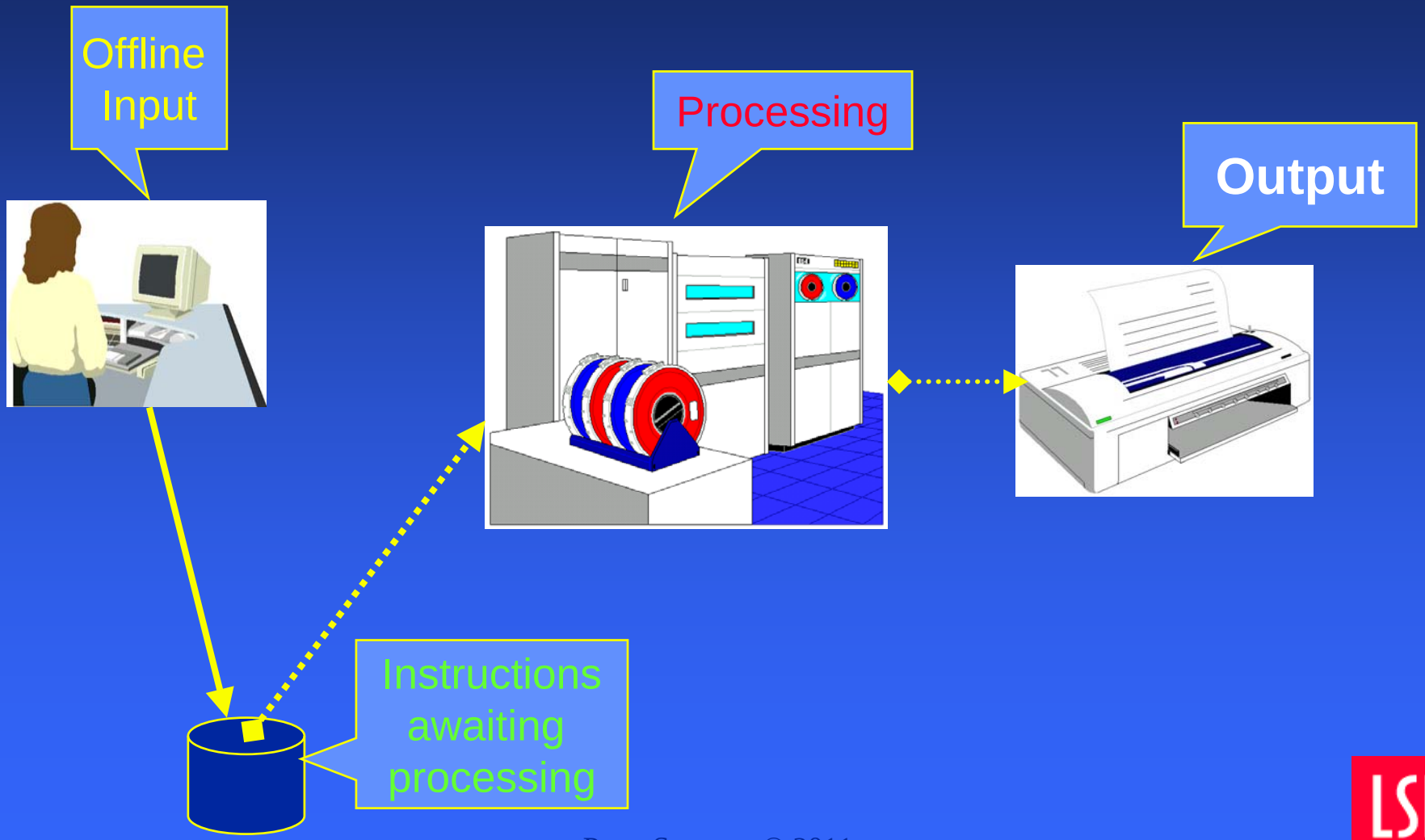
What Makes a Global Shock?

- Just because few cyber events aren't "global shocks" doesn't mean that cyber security isn't critically important to:
  - → Individuals
  - → Organisations
  - → Nation States

Cyber Security: what sort of problem is it?

- A series of individual technical problems with technical solutions
- A series of technical and managerial problems with technical and managerial solutions
- A complex set of problems with many partial solutions but with the aim of achieving “information assurance”

Batch Operations

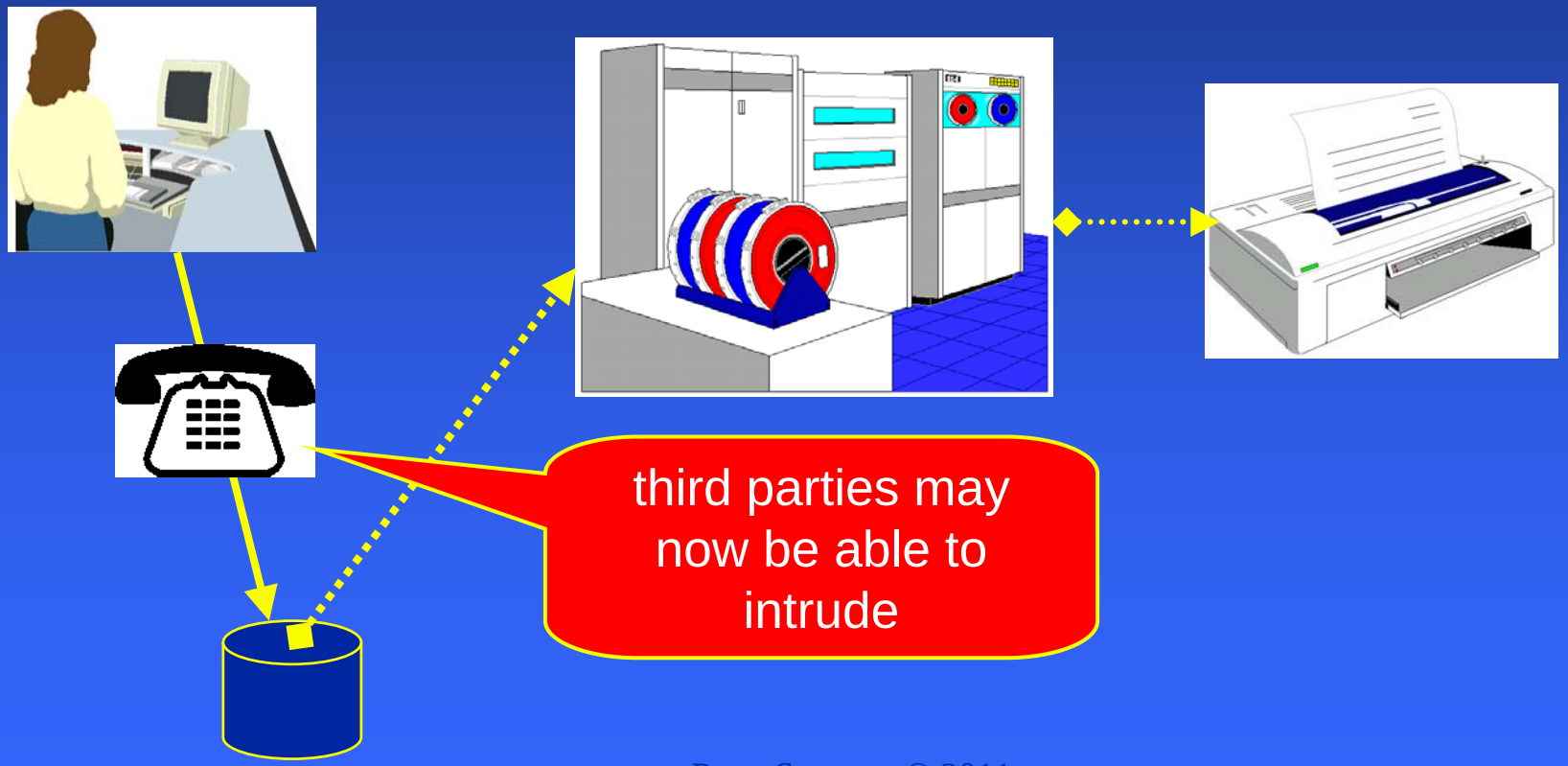


Batch Operations - Risks

- **Business Interruption**
- **Fraud**
  - ➔ **input**
  - ➔ **output**
  - ➔ **manipulative**
- **Software/hardware fails – bad design and maintenance**
- **Physical - mechanics & bombs , fire, flood**
- **insiders only**

Batch Operations

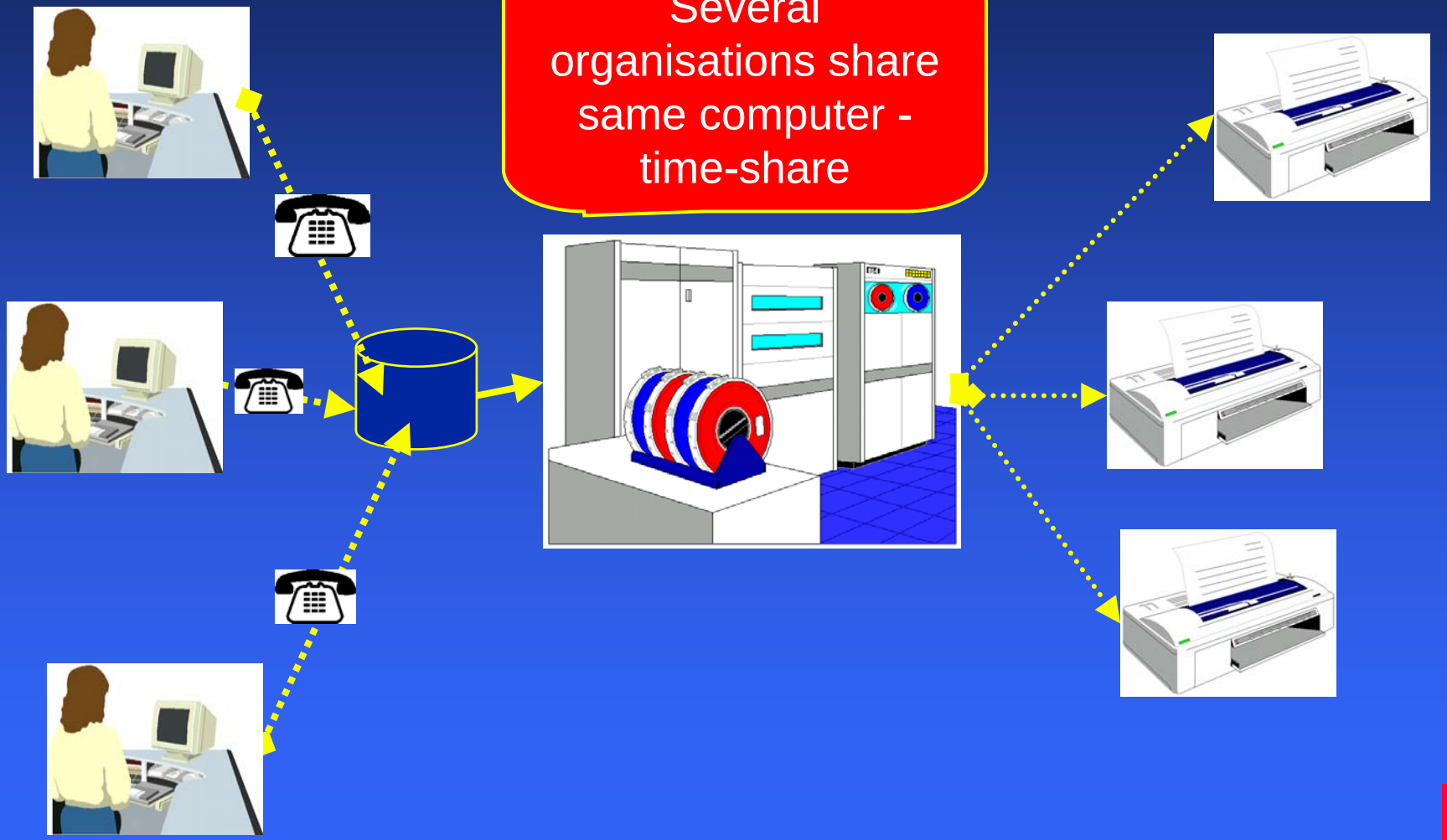
plus remote telecoms



LSE

Bureau Operations

Several organisations share same computer - time-share

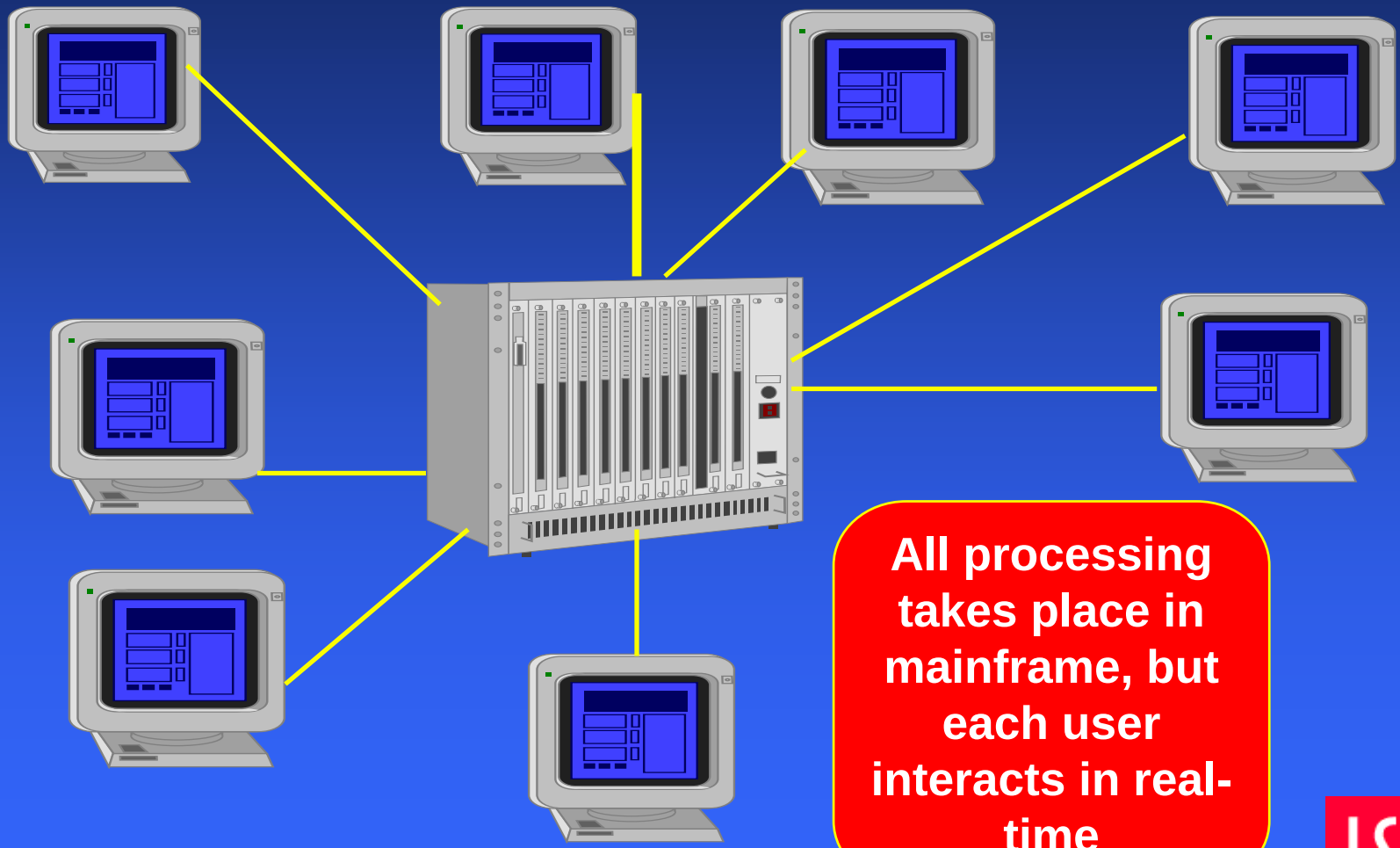


Bureau Operations - Risks

- **Business Interruption**
- **Fraud**
  - → **input**
  - → **output**
  - → **manipulative**
- **Loss of confidentiality**
- **Software/hardware fails – bad design and maintenance**
- **Physical - mechanics & bombs , fire, flood**
- **remote access means insiders and outsiders**

Interactive Computing

Central Unit + Dumb Terminals

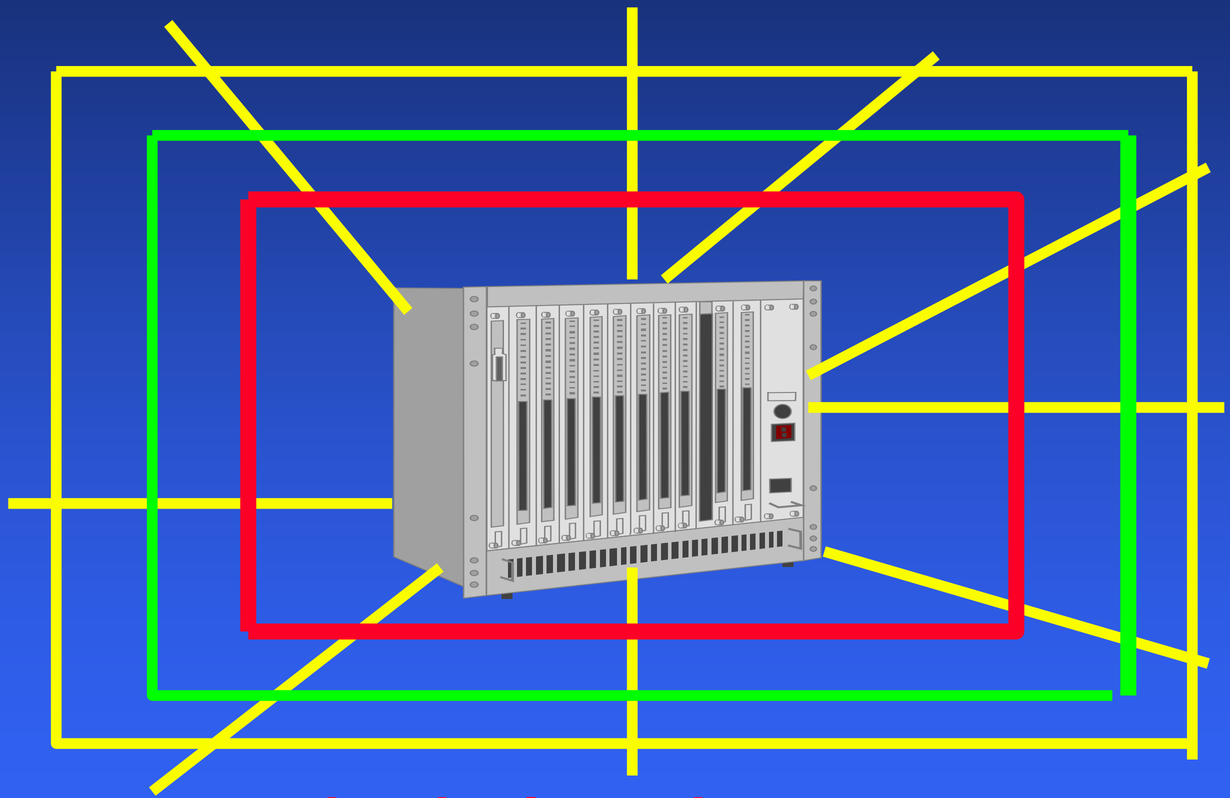


All processing takes place in mainframe, but each user interacts in real-time

LSE

Traditional Computer Security

Security by Ring-Fence.....



Physical Barriers - Computer Room

Logical Barriers - Access Control

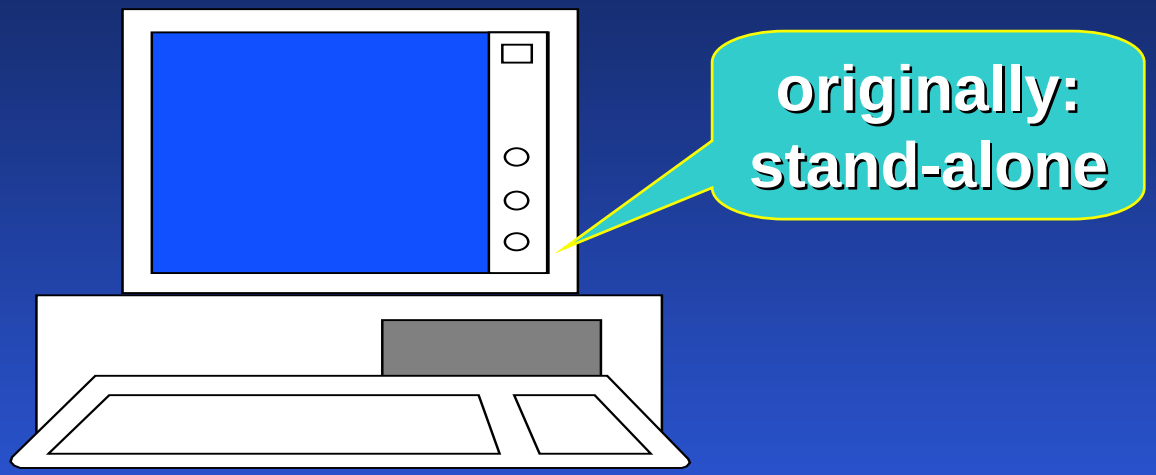
Personnel Controls

Interactive Computing - Risks

- **Business Interruption**
- **Fraud**
  - → **input**
  - → **output**
  - → **manipulative**
- **Loss of confidentiality**
- **Software/hardware fails – bad design and maintenance**
- **Physical - mechanics & bombs, fire, flood**
- **many more potential "criminals"**

LSE

The PC: Desk-top Computing



Computing Power & Data on the Desk

Democratising Computing…

the beginning of the end of "DP departmental power"

PCs (stand-alone) - Risks

- Initially: minimal, though corporate data could be accumulated and become a target for industrial espionage
- When connected (modem or via LAN): much greater opportunities for industrial espionage, unauthorized access, etc
- Viruses

New applications, GUIs and speed of response of PCs all encourage end-users to demand more of "big" computers and those who run them

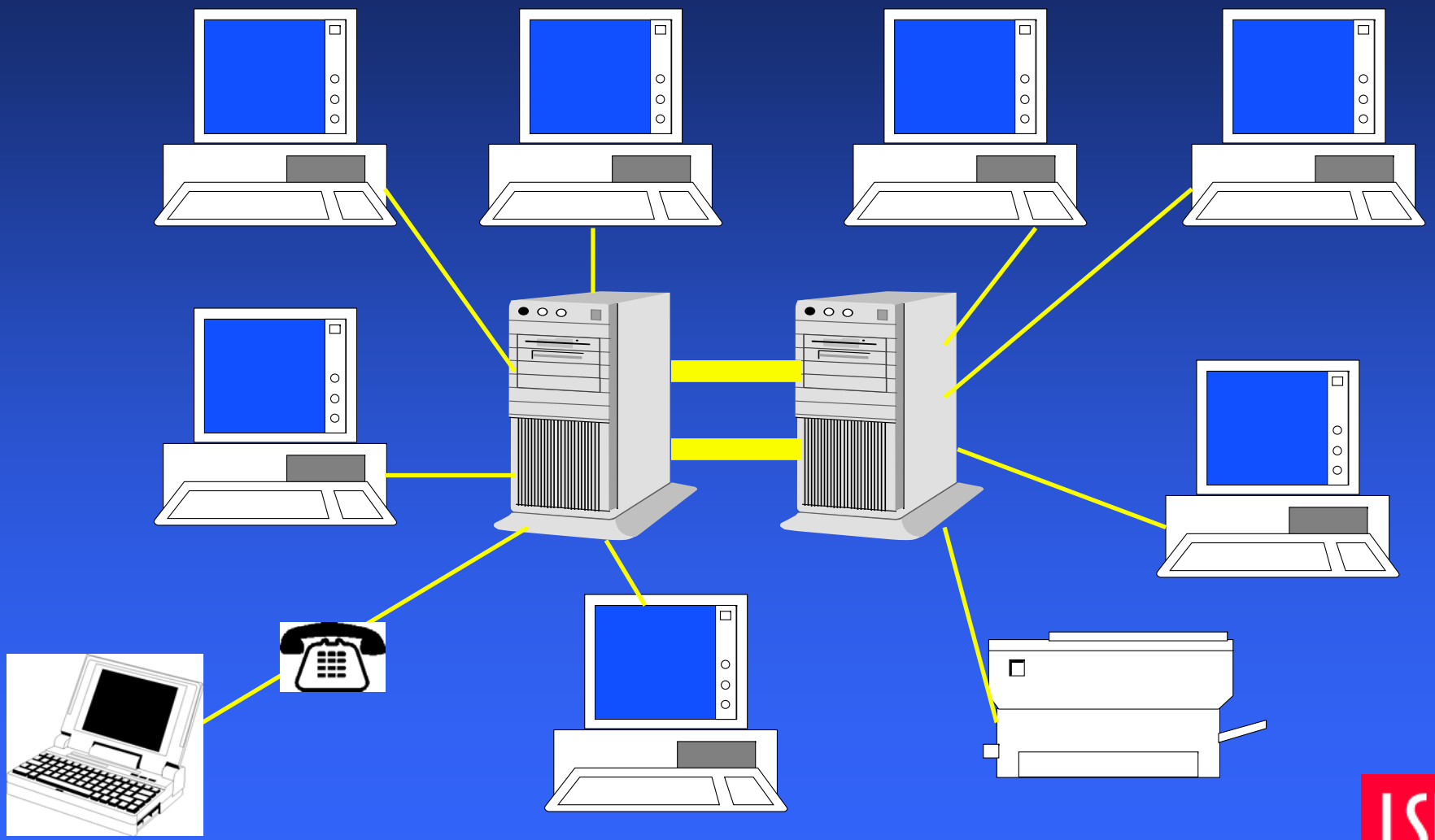
PCs (hobbyist)

About this time we get a growing number of hobbyist users:

- Recreational hackers
- Enthusiastic business folk
- Bulletin Boards etc:
  - → Provide social meeting place
  - → Means to distribute cheap software
  - → Means to distribute malware

LSE

LANs - file-server



LANs - Risks

- **Business Interruption**
- **Fraud**
  - → **input**
  - → **output**
  - → **manipulative**
- **Industrial Espionage**
- **Viruses**
- **Physical - mechanics & bombs , fire, flood**
- **insiders and outsiders**

PC OSs have poor security; low cost of LANs tends to mean small budget for security; neither PCs nor servers enjoy strong physical protection; many more people are computer-literate

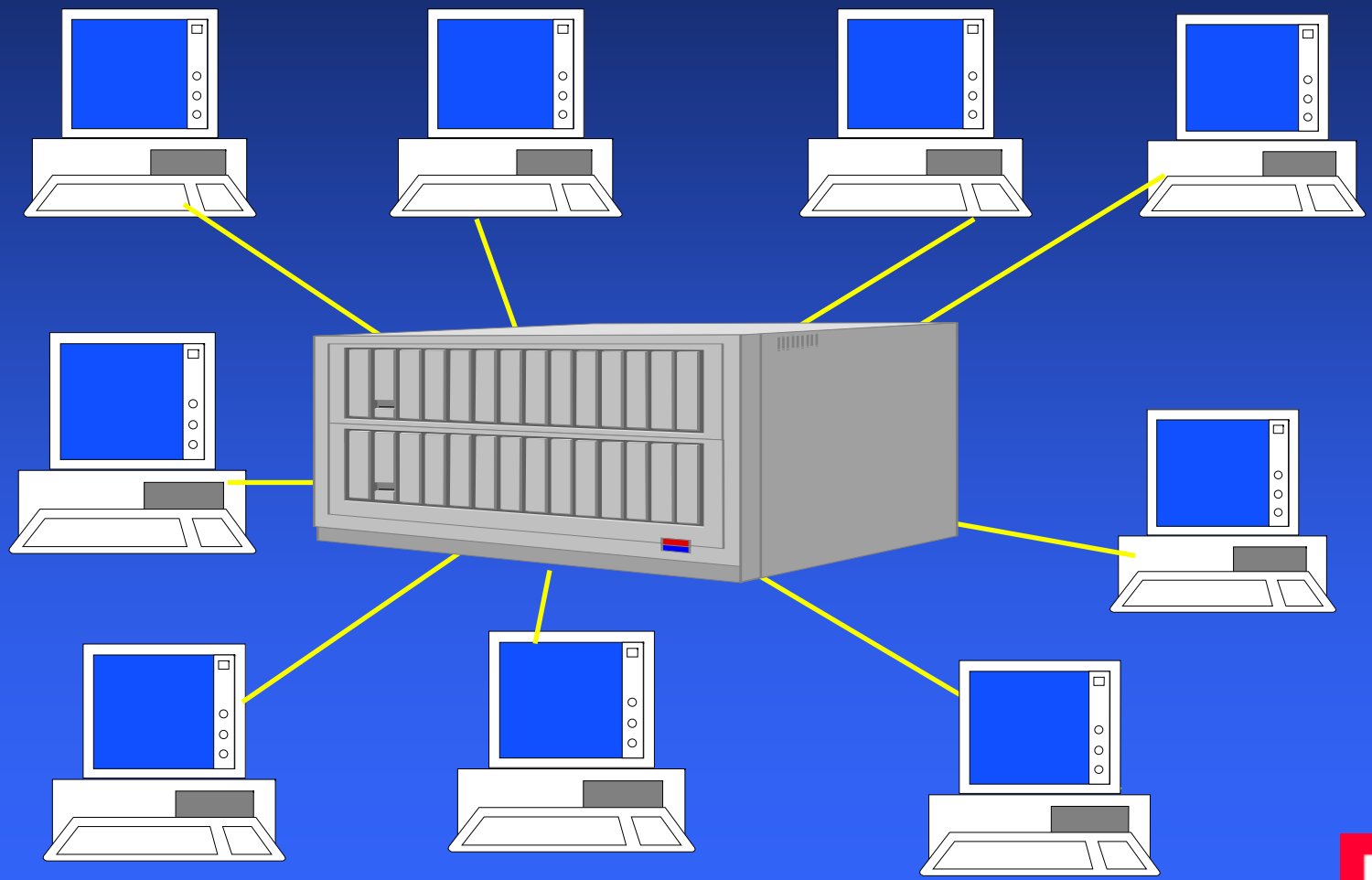
LSE

LANs - Risks

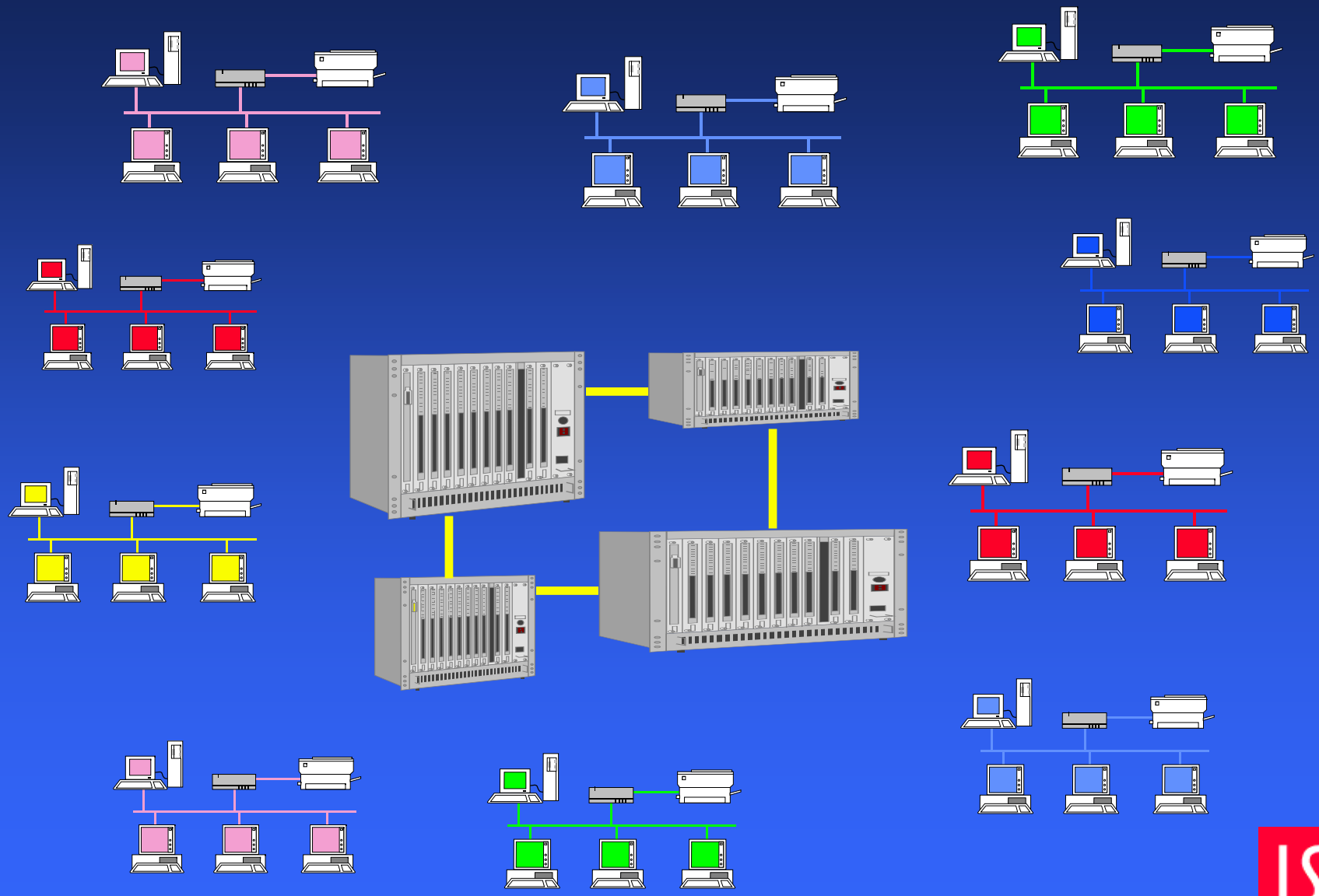
- LANs-plus-servers can be used to operate small to medium-sized businesses, as well as departments within large corporations
- Applications can include:
  - accounts
  - sales
  - marketing
  - R & D, design, presentation etc etc
- They are thus well worth “attacking”

New applications, GUIs and speed of response of LAN-connected PCs all encourage end-users to demand more of “big” computers and those who run them

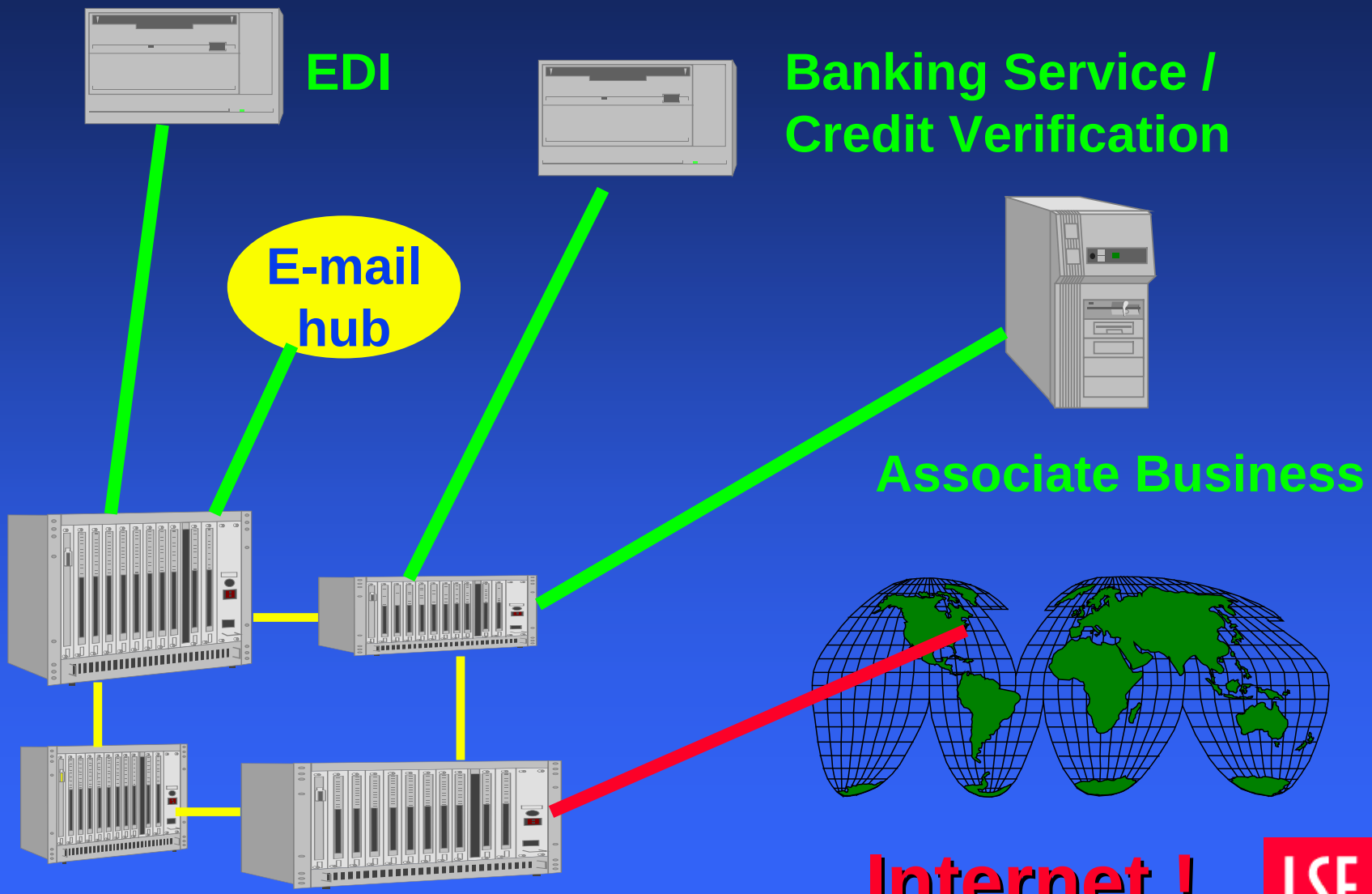
Client / Server



Open Systems - Hybrids



Internet Connections ...



Internet Connections - Risks

Risks depend on how connection is achieved:

- **to stand-alone PCs**
  - → **most risks: relatively low**
  - → **viruses**
- **via LANs**
  - → **potentially opens LAN to global visitors - TCP/IP is universal, non-proprietary**
  - → **good quality information security management plus good technology is essential**

Internet Connections - Risks

- **Business Interruption**
- **Fraud**
  - → input
  - → output
  - → manipulative
- **Loss of confidentiality**

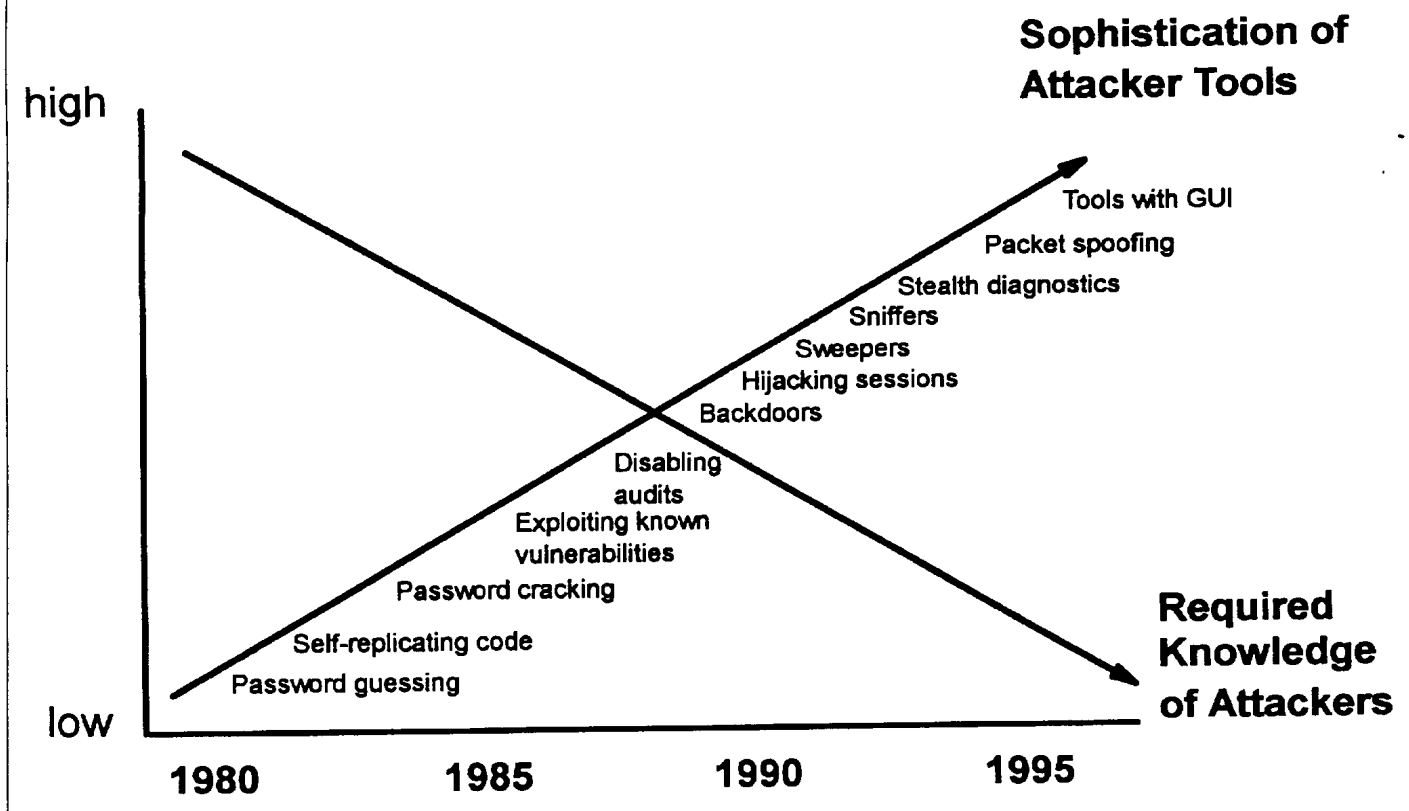
Knowledge of security weaknesses is widespread

- **Physical** - mechanics & bombs , fire, flood plus **Logical**: viruses and external cyber attacks
- insiders are still a threat but huge numbers of outsiders have potential access - plus use of sophisticated attack tools

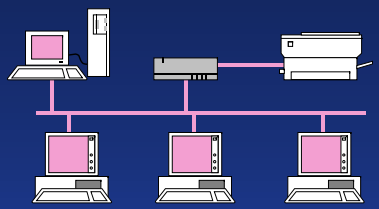
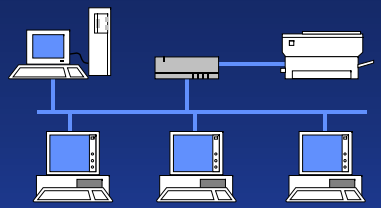
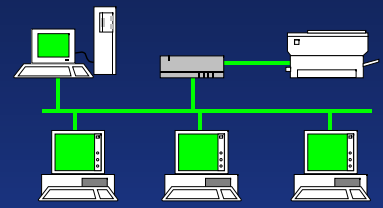
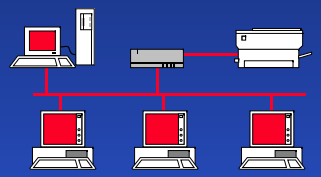
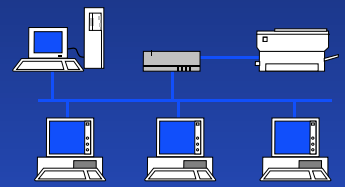
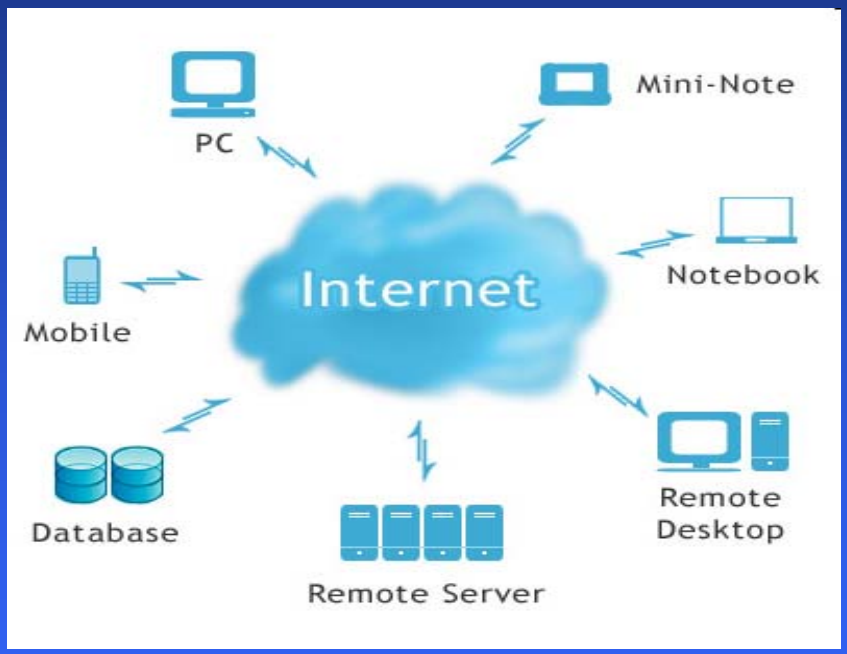
LSE

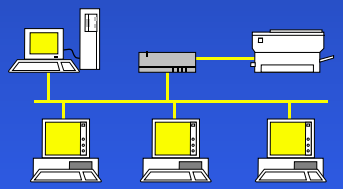
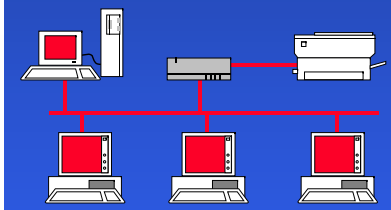
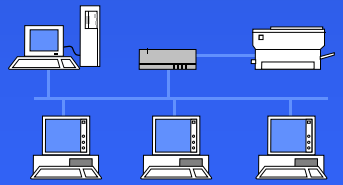
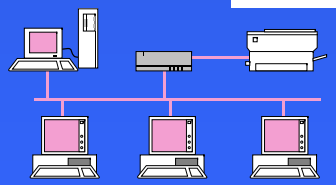
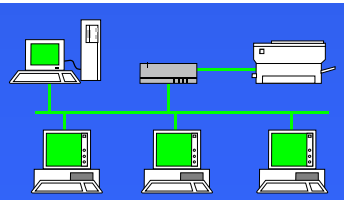
Attack methods: Spreading of Knowledge...

Figure 1.2: Attackers Require Less Knowledge as Tool Sophistication Increases



The Cloud

LSE

Cloud - Risks

- **Business Interruption**
- **Fraud**
  - input
  - output
  - manipulative
- **Loss of confidentiality**

- **Physical** - mechanics & bombs , fire, flood plus **Logical**: viruses and external cyber attacks – DDOS
- **Contractual**
- **Failure of connectivity**
- insiders are still a threat but huge numbers of outsiders have potential access - plus use of sophisticated attack tools

A history of how computer systems have been managed

- > 1970: Computer company supplies hardware & software
- 1970: "unbundling": one company supplies hardware; others supply software
  - businesses need to develop their own "EDP" management skills
  - businesses create their own development "shops"

LSE

A history of how computer systems have been managed

- 1970s: growth of specialist software houses, consultants; EDP
- 1970s: management of bureau services
- 1970s: need for telecoms and network suppliers and specialists
- late 1970s: IT strategists
- late 1970s: independent purchase of PCs
- early 1980s: independent use of modems, online services

A history of how computer systems have been managed

- Mid-1980s: EDP becomes more strategic > > Management Information Services
- Mid-1980s: attempts to bring PCs into general planning
- Late 1980s: increased use of consultancies
- Late 1980s to date : outsourcing > the Cloud

A history of how computer systems have been managed

- 1990s to date: new computer architectures lead to flatter management structures -
  - what is the role for corporate IT?
- Late 1980s to date: employees have home computers and laptops - and use them for work
- 1995 to date: Internet and Intranet development - “experimental” groups
- 1995 to date: outsourcing >>> Cloud computing: Service Level Agreements

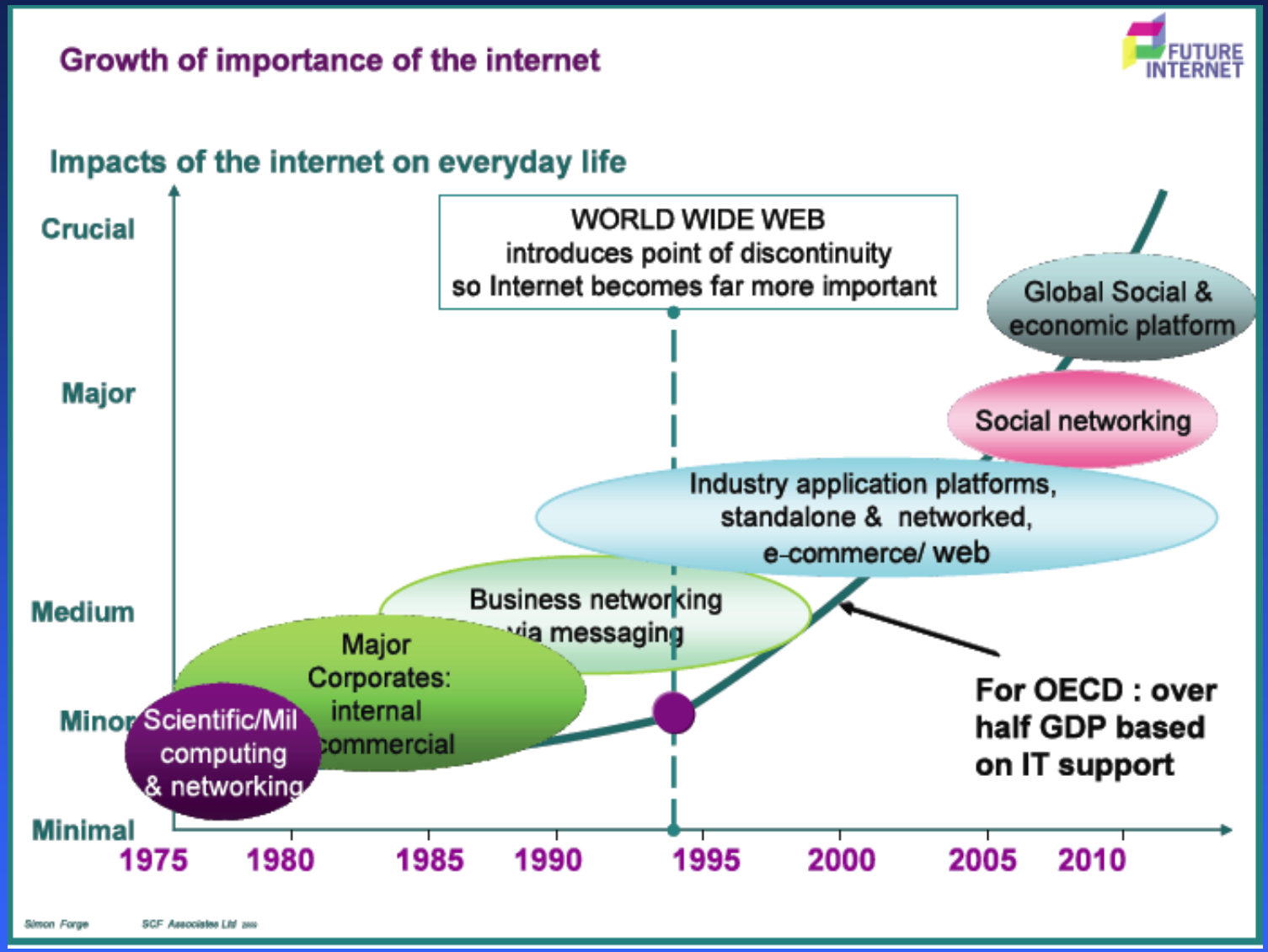
Multipliers

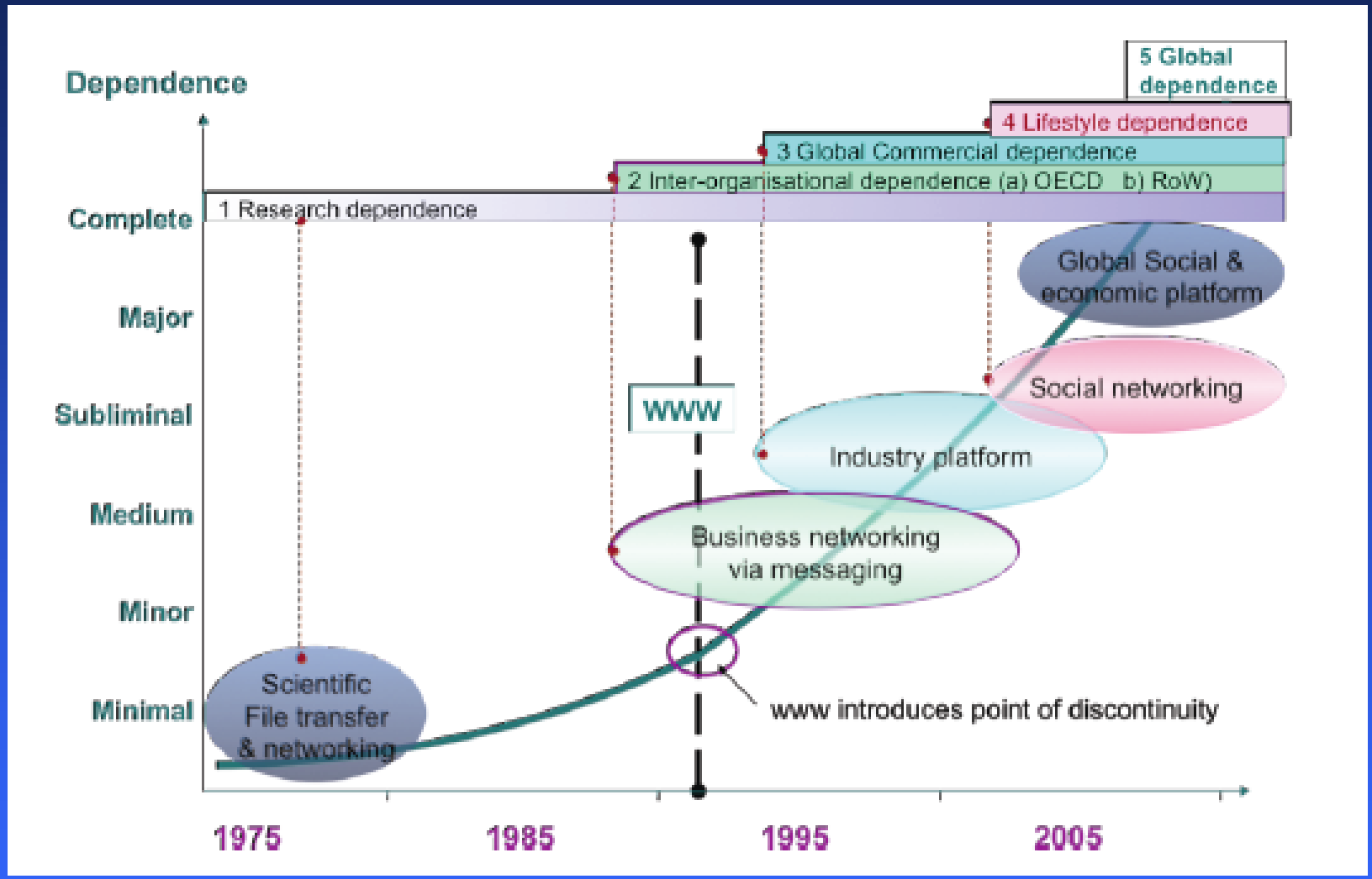
- Cheaper Computer Hardware
- Cheaper Data Storage
- Faster and Easier Communications
- More commercial applications
- More social / cultural applications
- More industrial and retail use of Just In Time
  - → Frequent re-ordering
  - → Low local stocks
  - → Semi-autonomous systems

LSE

Multipliers

- More Government to Business ICT interaction
- More Government to Citizen ICT interaction
- Abandonment of “older” facilities
  - → Local Offices
  - → Local Market places etc
  - → Older paper-based transactions
- No easy way back!





Doctrines

- What sort of problems do we need to address – and how do we do so?
- From the Tech Problem / Tech Solution to Information Assurance

LSE

Security Doctrines

- **Batch processing:**
  - ➔ Problems are very small; mostly of software and hardware failure
  - ➔ Doctrine: better testing!
- **Batch processing bureaux:**
  - ➔ Doctrine: better testing + basic authentication of users

LSE

Security Doctrines

- **Real-Time computing**
  - → Central computing resource + dumb terminals
  - → Security by ring-fence
    - Physical
    - Logical
    - Personnel
  - → Development of access control security software (tech problem/tech solution paradigm)
  - → EDP Audit to address complexity

EDP Audit

- Ideas borrowed from traditional audit
- "Standards" – checklists of features a "good" system has
- Confidentiality Integrity Availability
- Specific requirements of particular system
- Standards are still with us –ISO27000

EDP Audit

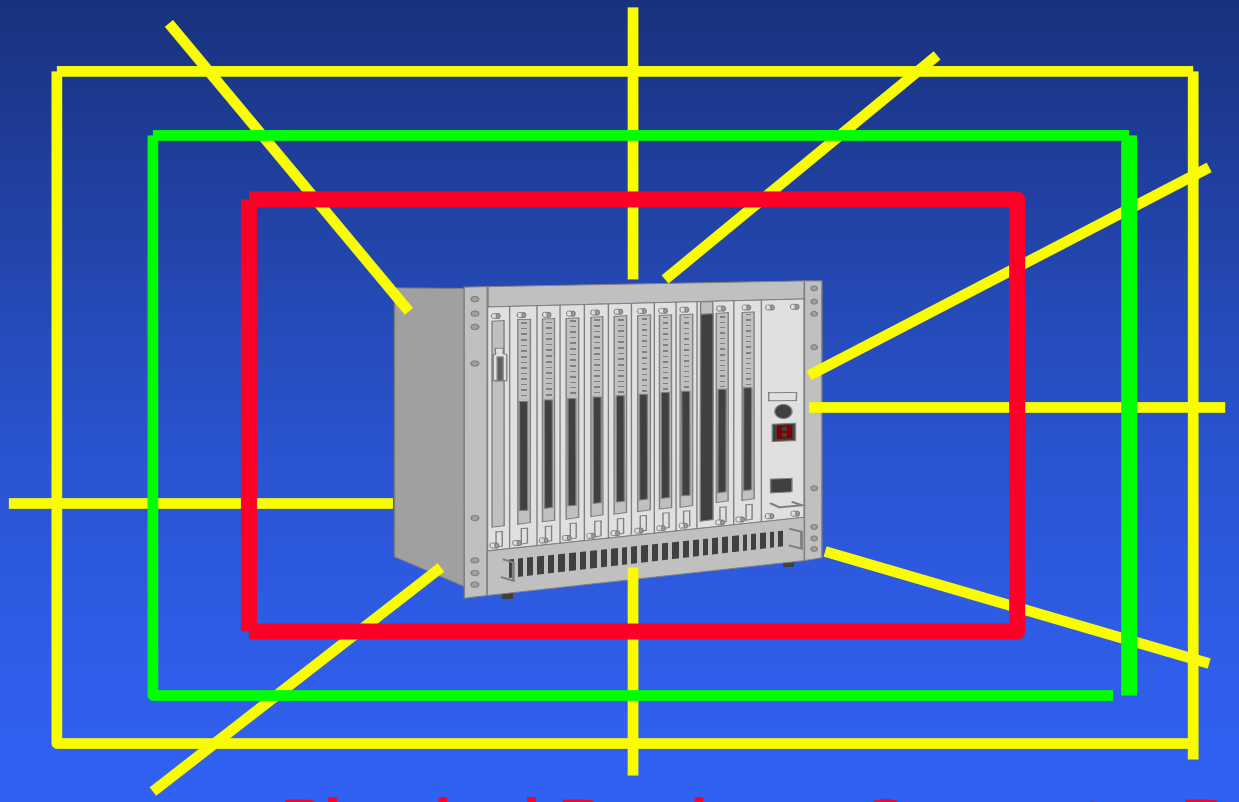
- Standards are still with us –ISO27000
- Advantages: puts an organisation and its ICT infrastructure through a testing process which may reveal defects
- Disadvantages: how and from where do you derive the checklist? Is it complete and up-to-date? What are the costs? May "compliance" lead to self-deceit that all is well?

Tech Problem / Tech Solution

- "we have a problem of unauthorised access – we need better access control"
  - ➔ Bell LaPadula models
- "we have buggy software – we need better software testing"
  - ➔ Mathematical proofs
  - ➔ Automated testing schemes
- "we are attacked by viruses – we need anti-virus software"
- "we are worried about intruders – we need firewalls, and intrusion detection systems"

LSE

The changing security paradigm



Physical Barriers - Computer Room

Logical Barriers - Access Control

Personnel Controls

De-perimeterisation

- We can no longer simply guard the perimeter of a computer system – because it no longer exists

Cloud Computing

- Data available everywhere
- Users only pay for what they need (back to bureaux and out-sourcing)
- But requires:
  - ➔ High levels of security of information (encryption)
  - ➔ High levels of access control / authentication

The changing security doctrine

- the simple “technical problems / technical solutions approach is dead
- security can’t be addressed by formula or simplistic “certification”
- centralised control of corporate security functions is no longer feasible

New doctrines

- **Information Systems**
  - → **The study of the impact of computer and telecommunications technologies on**
    - **Individuals**
    - **Businesses and Organisations**
    - **Management**
    - **Government**
    - **Society as a whole**
  - → **Using the Social Sciences**
    - **Sociology**
    - **Anthropology**
    - **Economics**
    - **Management Science**

LSE

New doctrines

- **Information Security Management**
  - → Need to ***add*** other types of discipline beyond the tech problem/tech solution paradigm
  - → The Social Sciences
    - Organisation Analysis
    - Management
    - Criminology
    - Anthropology
    - Economics
  - → Notions of Risk Management
    - Insurance disciplines

New doctrines

- **Information Assurance**
  - Security can't be perfected, but can be managed
  - The purpose now is to have ***sufficient confidence*** that a computer mediated process can be **trusted**
  - Human and organisational aspects have to be understood and engineered for
  - Re-examination of notions of **trust** and **risk management** – as well as the "**techie**" and "**standards**" approaches
  - Role of **law** as an enforcer and stimulant to better security

LSE

Information Assurance Practicalities

- **Tech measures still important**
  - ➔ Access Control / Identity Management
  - ➔ Malware Detection
  - ➔ Firewalls
  - ➔ Intrusion Detection
  - ➔ Fraud / Anomaly Detection
  - ➔ Crypto for Confidentiality and Authentication

LSE

Information Assurance Practicalities

- **Management Approaches**
  - → System Specification
  - → Threat / Risk Analysis
  - → System roll-out
  - → User training
  - → Sensitive HR, including vetting, employee monitoring
  - → User interface to tech facilities
  - → Penetration testing

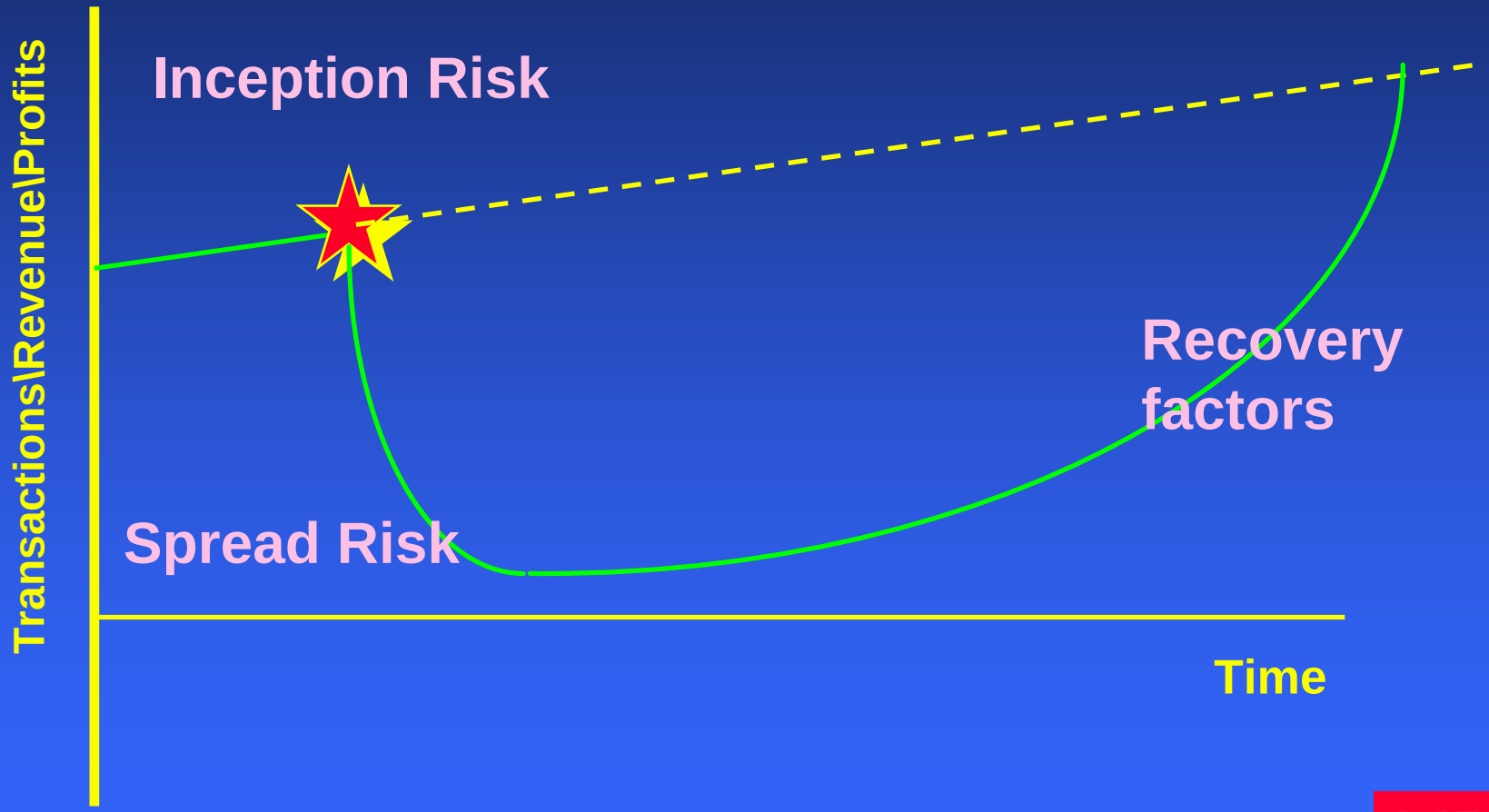
LSE

Information Assurance Practicalities

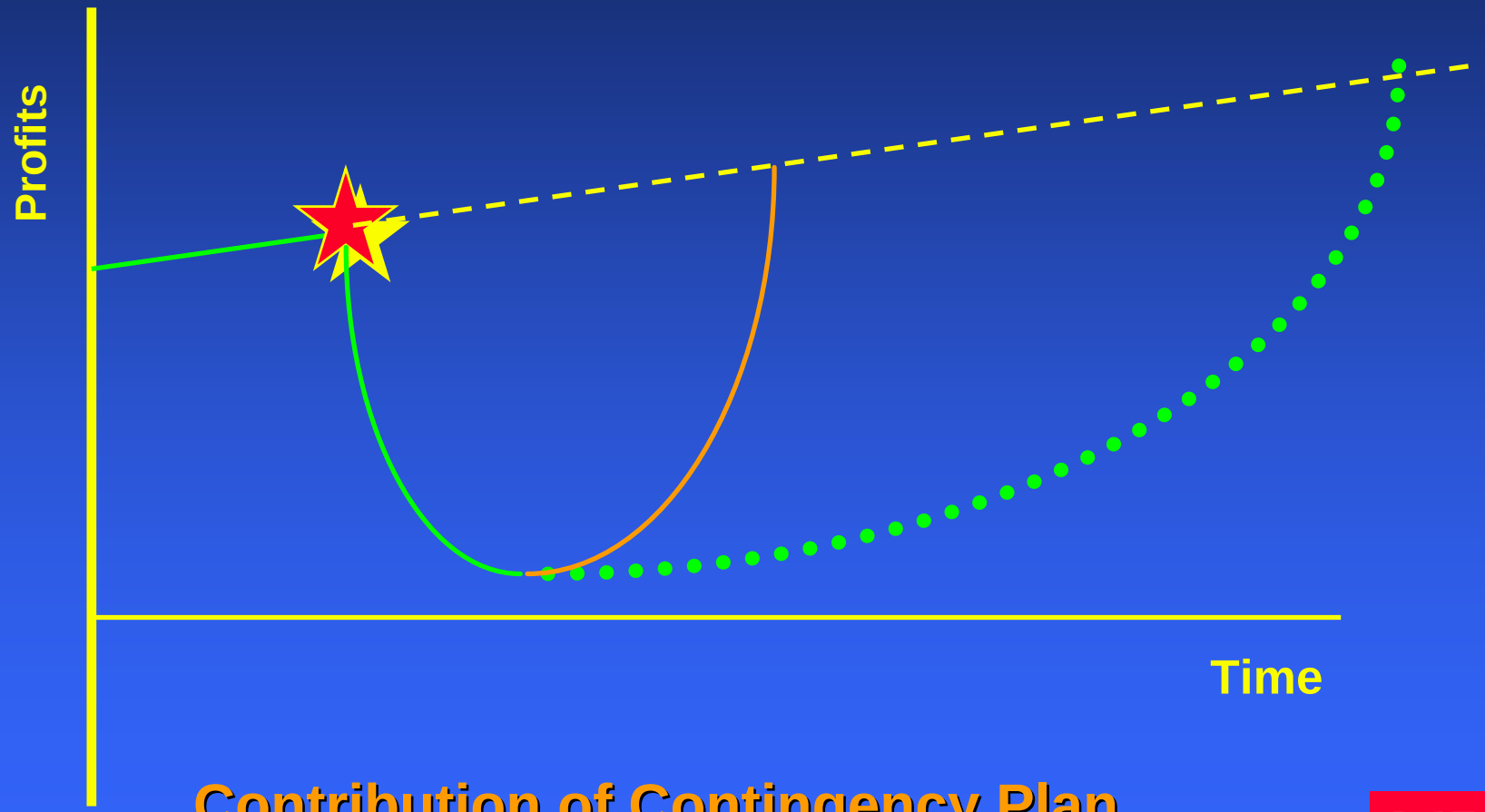
- **Management Approaches**
  - **Contingency / Recovery Plans, because:**
    - **Tech methods will sometimes fail**
    - **Zero-day threats**
    - **Modern systems are too complex to fully identify and analyse the risks**
      - **Systems, interconnections and hidden dependencies**
    - **Rate of change means systems are never static – and neither are the threats**

LSE

Shape of Disaster



Shape of Disaster

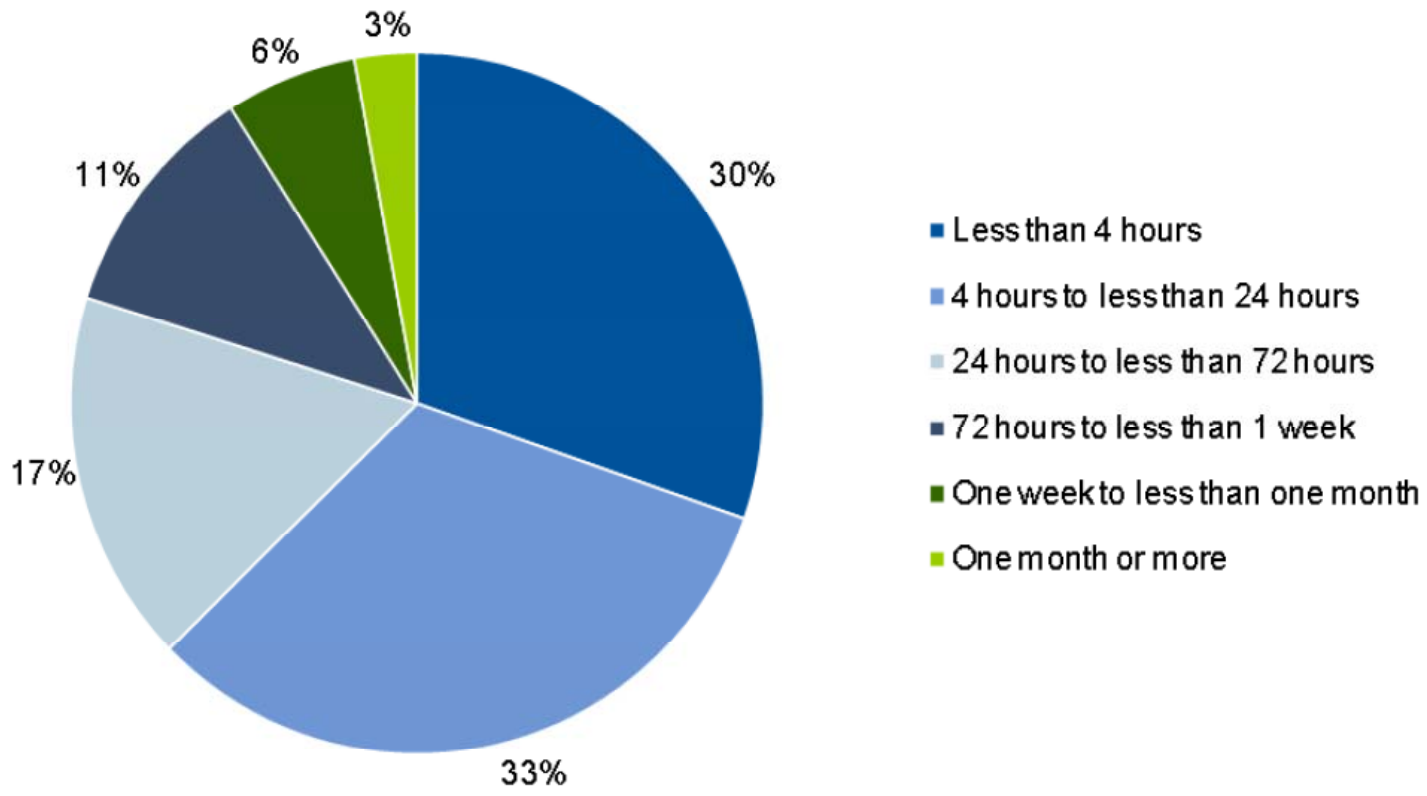


Contribution of Contingency Plan..

Recovery Factors

- You can't bring back a 100% service immediately – so what should you prioritise?
- What is already available that can be deployed?
  - ➔ Back-up data
- What do you need to acquire / prepare for?
  - ➔ Management structure
  - ➔ A Plan
- Recovery Sites
- Third Party facilities
- Load-balancing

Figure 1. Business Functions and RTOs 2010 Risk and Security Survey, n = 133



Source: Gartner (February 2010)

National Security Dimension

Two dominating features of national cyber security:

- 80-85% of CNI is in private, not government control
- Attribution of hostile attacks

National Security Dimension

Attribution of hostile attacks

- **If you can't establish, at battle speed, the source of an attack, you can't retaliate**
- **Defence based on deterrence no longer works**

National Security Dimension

80-85% of CNI is in private, not government control

- Private companies have responsibilities to produce profit for share-holders, not a greater public "good"
- Information Assurance is best applied initially at the local level
  - → By people who understand the local environment

National Security Dimension

- **"Public/Private Partnerships" won't work without an economic incentive, or licensing / regulation – neither is politically easy**
  - → **Can a government "run" a complex CNI business?**

LSE

National Security Dimension

- Role of military limited to protecting their own systems
  - ➔ Many future armed conflicts will use cyber weaponry alongside conventional kinetic weapons
    - Protection
    - Attack
  - ➔ But the military can't run complex CNI businesses

National Security Dimension

- **National "cyber shields" are very difficult to design and manage**
  - ➔ How, in practical terms, do you identify the CNI networks and systems?
  - ➔ What happens to international businesses, or businesses with key international links/partners?
  - ➔ Will the national cyber shield block important traffic?
  - ➔ Is running a cyber shield compatible with the role of an intelligence agency?

LSE

Information Assurance

Managing Risks relating to the use, processing, storage, transmission of information. includes:

- Planning, Design
- Risk Assessment
- Prevention
- Detection
- Reaction
  - → Recovery, Loss Mitigation

LSE

Information Assurance

- Protection short of Perfection
- Technical and Managerial techniques work hand-in-hand
- Ability to recover in addition to ability to prevent
- Measures best applied locally.

Costs and Information Assurance

Over time, hardware as a percentage of total spend has fallen dramatically.

Commoditised general software is also incredibly cheap.

The main costs now are in now customising these to specific individual needs.

Reliable systemic security may soon be the biggest cost centre of all

Information Assurance

Do we need to slow down the rate of change we accept?

Just because a new technology or service becomes available, do we immediately have to adopt it?

Cyber Security

11 July 2011

From "Computer Security" to "Information Assurance": Evolving Doctrines & Consequences

Peter Sommer
London School of Economics
p.m.sommer@lse.ac.uk
peter@pmsommer.com