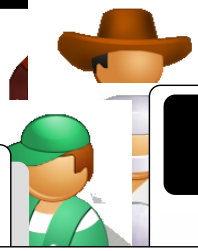
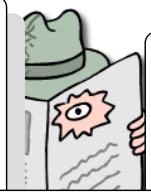
Fundamentals

Trap-door

Mis-representation

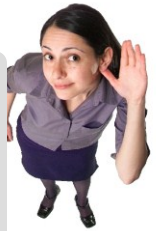


Visual spying



Logical scavenging

Eavesdropping

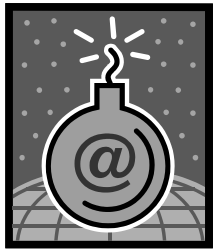


Interference

Physical removal

Spoofing

Logic bombs



Trojan horse

Authorizati attack

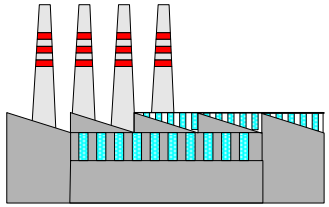
Introduction

Industrial Age

Postal system
Paper voting
Telephone
Physical shopping

Information Age

Email
E-voting
Voice-over-IP
E-shopping

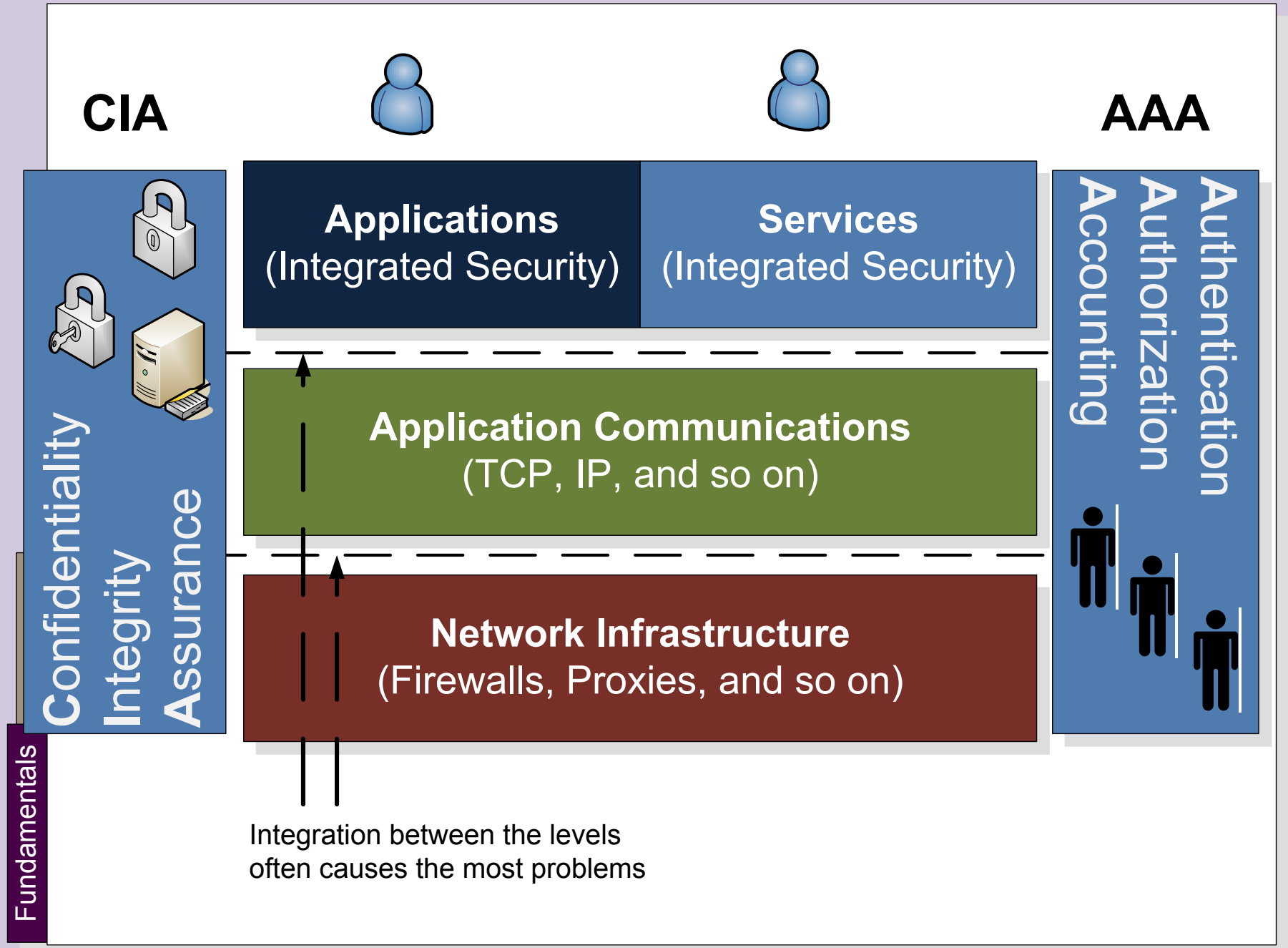


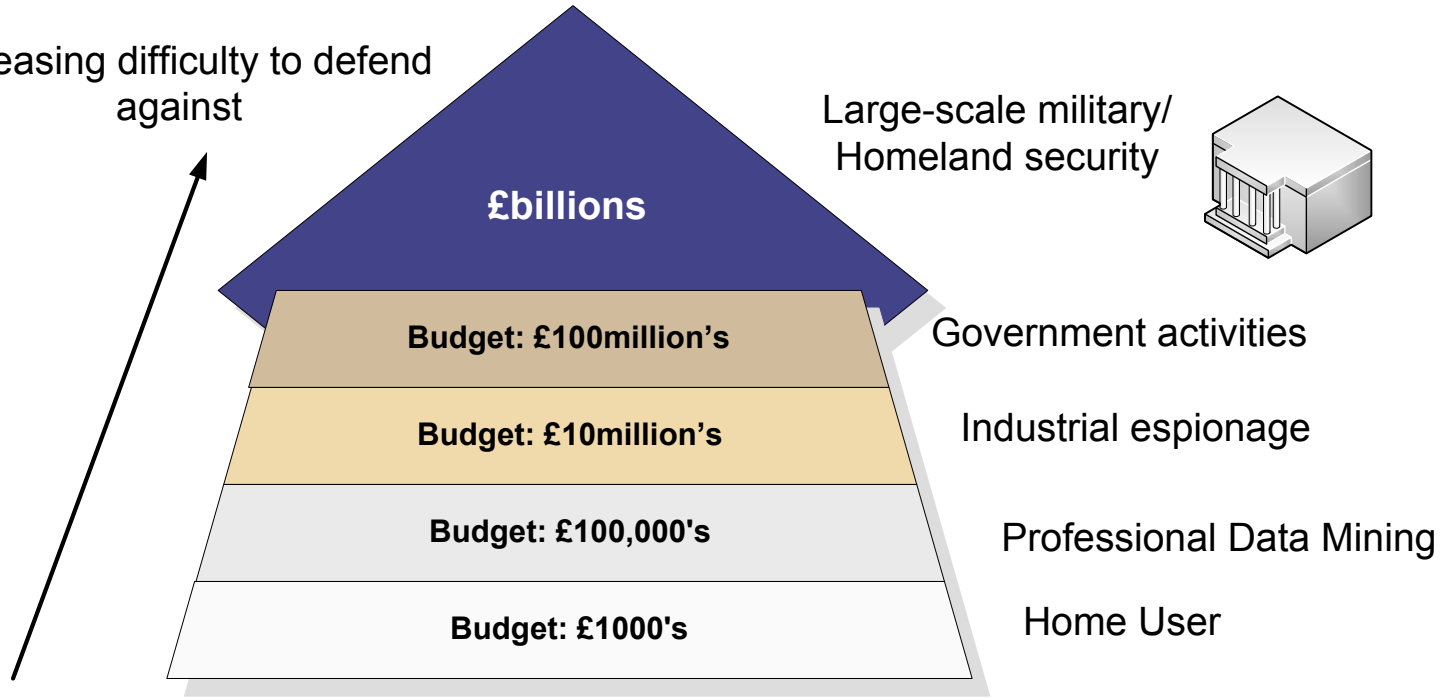
Fundamentals:
Security
Assurance
Authentication

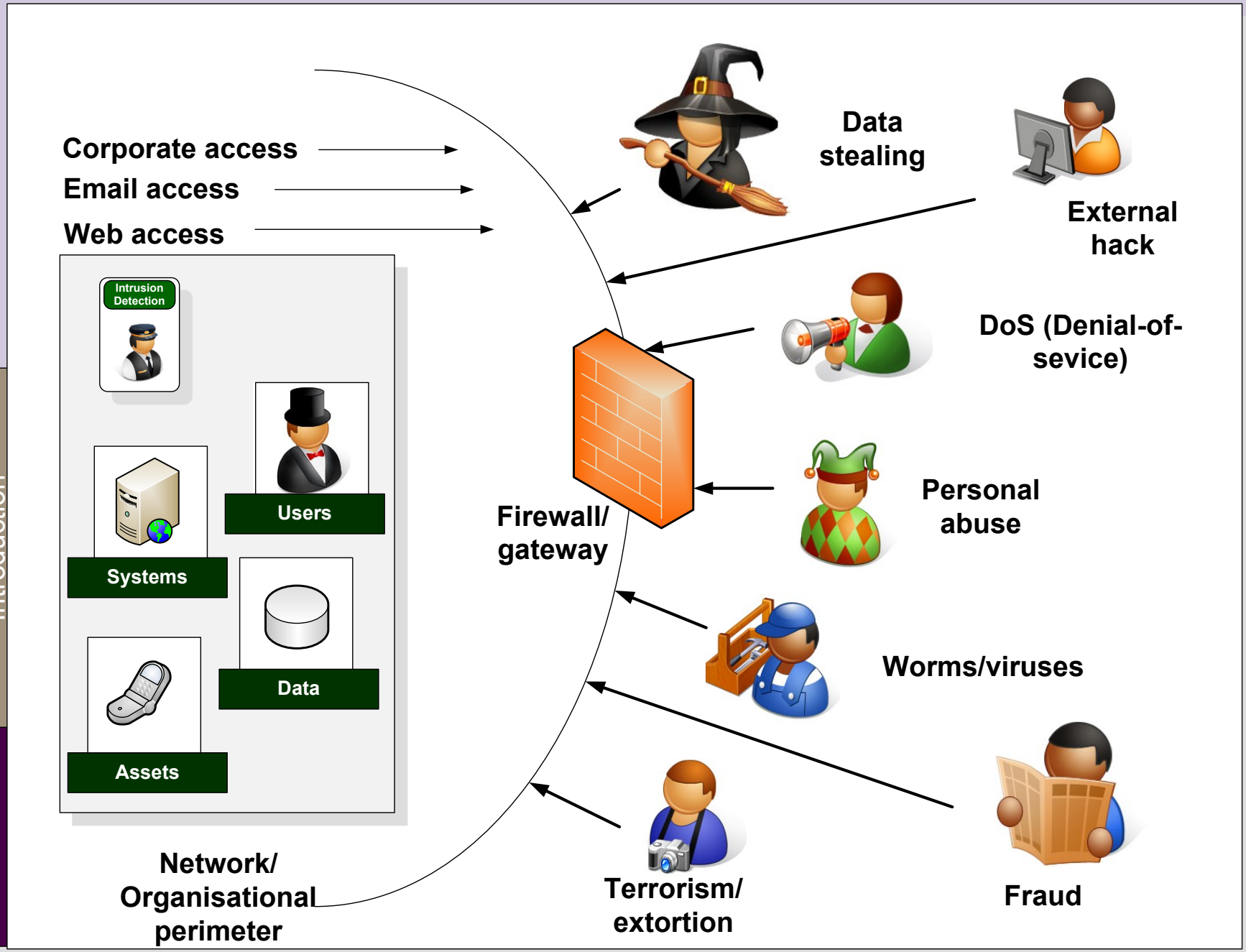
Authentication
(Device,
User, Servers,
Connections, etc)

Confidentiality
(Encryption)

Assurance
(Integrity)


CIA
AAA
Applications
(Integrated Security)
Services
(Integrated Security)
Application Communications
(TCP, IP, and so on)
Network Infrastructure
(Firewalls, Proxies, and so on)
Confidentiality
Integrity
Assurance
Authentication
Authorization
Accounting
Integration between the levels
often causes the most problems
Fundamentals


Increasing difficulty to defend against
£billions
Budget: £100million's
Budget: £10million's
Budget: £100,000's
Budget: £1000's
Large-scale military/ Homeland security
Government activities
Industrial espionage
Professional Data Mining
Home User

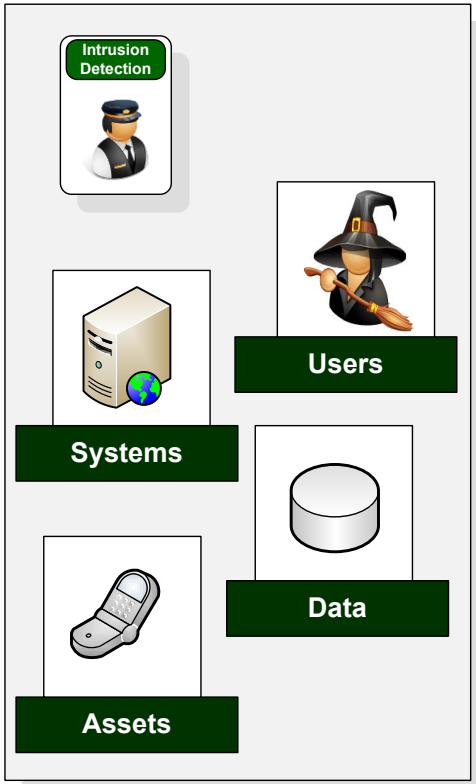

Corporate access
Email access
Web access
Intrusion Detection
Users
Systems
Data
Assets
Network/
Organisational
perimeter
Firewall/
gateway
Data
stealing
External
hack
DoS (Denial-of-
sevice)
Personal
abuse
Worms/viruses
Terrorism/
extortion
Fraud

CSI (Computer Security Institute) found:
- 70% of organisation had breaches
- 60% of all breaches came from inside their own systems

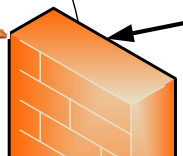
Data stealing

External hack

Corporate access



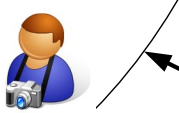
DoS (Denial-of-sevice)



Firewall/ Gateway (cannot deal with internal threats)

Personal abuse

Worms/viruses

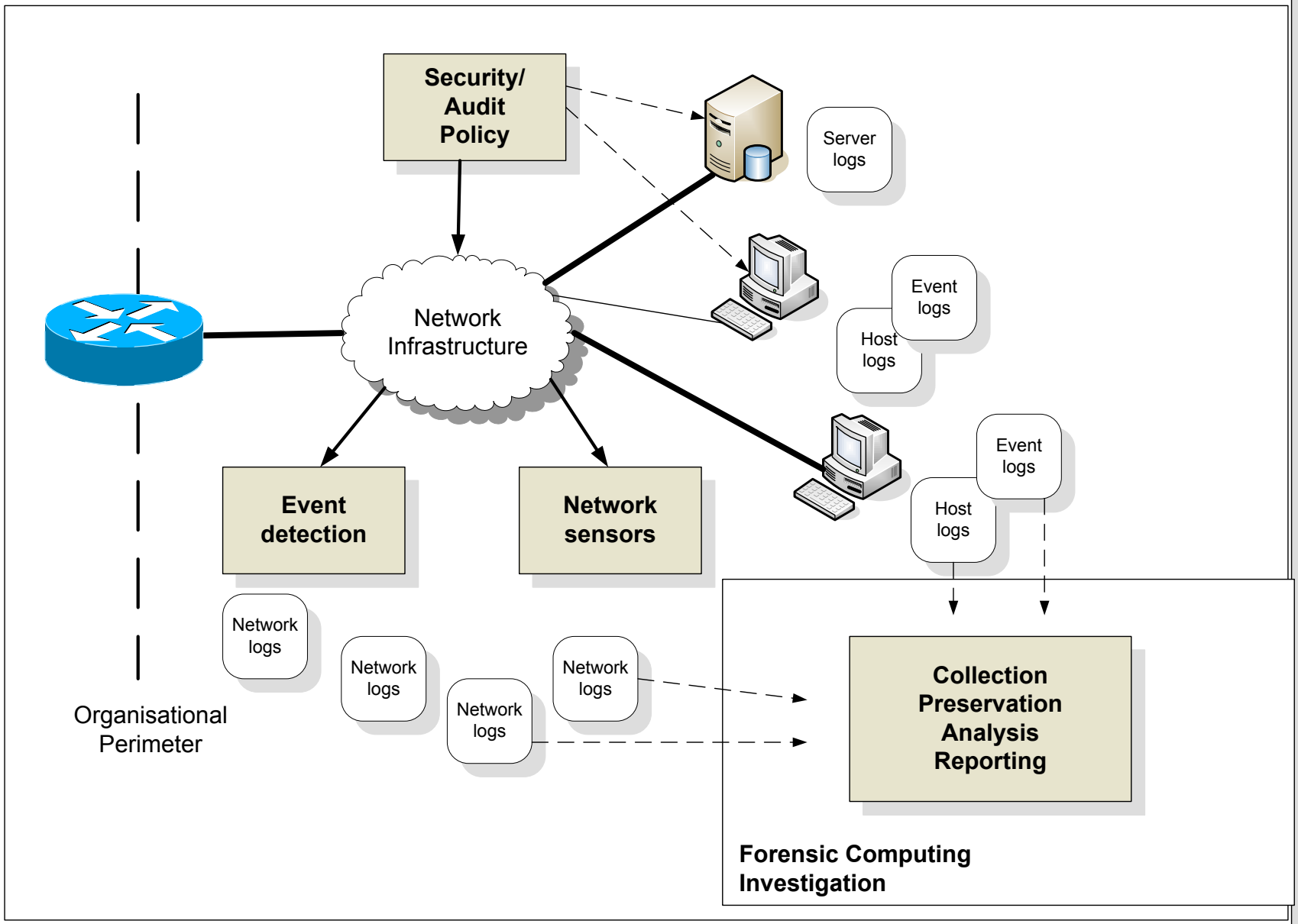


Terrorism/ extortion

Fraud

Network/ Organisational perimeter

Outside and inside threats

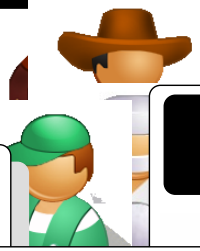


Network/host infrastructure context

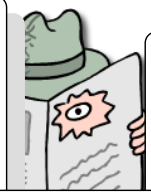
Fundamentals

Trap-door

Mis-representation

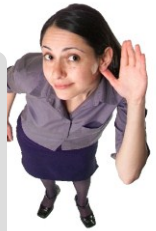


Visual spying



Logical scavenging

Eavesdropping

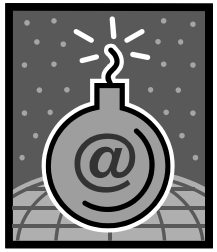


Interference

Physical removal

Spoofing

Logic bombs



Trojan horse

Authorizati attack

Threats

Fundamentals

Threats

Networksims.com Home Page: The Best Cisco Simulator (Emulator) in the World with router, switch, PIX, and wireless simulation for CCNA, CCNP, CCSP, ONT, ISCW, ...

File Edit View History Bookmarks Tools Help

file:///F:/networksims/new/emulators111.htm

add ads to page

My Click Site

HOME | DEMO | EXAMPLE | TESTS | PURCHASE | CONTACT | TESTIMONIALS | VIDEOS

TESCO direct

YOUR M&S > View now

amazon.co.uk

John Lewis

Which? - Reviews

Advertise here ...

MENU

- Home
- Versions
- Test resources
- Purchase
- Site Licenses
- Challenge Demos
- Contact us

CERTIFICATIONS

- CCNA
- CCSP
- CCNP

About the Software

This sdf asd fas dfa sdfa sdf asdf asdf asdf asdf asdf asdf asdf asdf asdf asdf asdf asdf asdfasd sdf asd fas dfa sdfa sdf asdf asdf asdf asdf asdf asdf asdf asdf asdf asdf asdf asdf asdfasd sdf asd fas dfa sdfa sdf asdf asdf asdf asdf asdf asdf asdf asdf asdf asdf asdf asdf asdfasd sdf asd fas dfa sdfa sdf asdf asdf asdf asdf asdf asdf asdf asdf asdf asdf asdf asdf asdfasd

* 12,960 exam questions *16 hours of video lectures *290 router labs

Find: affil Next Previous Highlight all Match case

Done

Amazon.co.uk: low prices in E

File Edit View History B

This contains a wide range c

amazon.co.uk

Shop All Departments

- Books
- Music, DVD & Games
- Electronics
- Computers & Office
- Home & Garden
- Toys, Children & Baby
- Clothes, Shoes & Watches
- Sports & Leisure
- Health & Beauty
- DIY & Tools

Check This Out

Designer Clothing
Save up to 70% on Evisu tops, t-shirts and jeans.

Microsoft Windows 7 Home Premium... for Windows
~~£149.99~~ **£125.33**
(Why is this recommended for you?)

Mac OS X Snow Leopard (Mac DVD) for Mac OS X 10.5 Leopard
£22.99
(Why is this recommended for you?)

CCNA Security Lab Manual: The Only... Paperback by Cisco Networking Academy
£20.89
(Why is this recommended for you?)

› See more new releases

Recommended for You

LOOK INSIDE!

Done

Stolen credit card details used to purchase

Fake Purchaser

Can I sell your site through mines? 15% commission?

Affiliate scammer

15% commission for every sale

Author: Prof Bill Buchanan

Threats: Affiliate Scam

Control by proxy

Botnet access

Botnet

Botnet command

Bot Master

Author: Prof Bill Buchanan

Visual spying

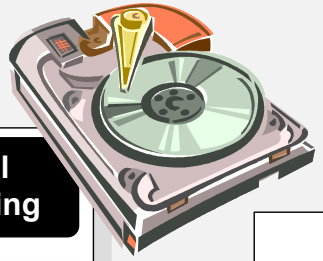
Visual spying. This actual physical viewing a user's activities, such as their keystrokes or mouse clicks.

Mis-representation

Misrepresentation. This involves the actual deception of users and system operators.

Eavesdropping

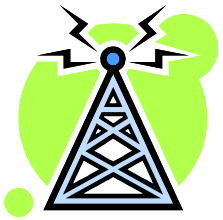
Eavesdropping. This involves intercepting communications.



Logical scavenging

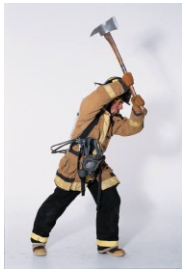
Logical scavenging. This involves scavenging through discarded media.

Interference



Interference. This involves the actual interference of communications, such as jamming communications, or modifying it in some way.

Physical attacks



Physical removal

Physical attacks. This involves an ...al physical attack ...he hardware. **...sical removal**. ... involves the ...al physical ...oval of hardware.

Spoofing. This involves the spoofing of devices.

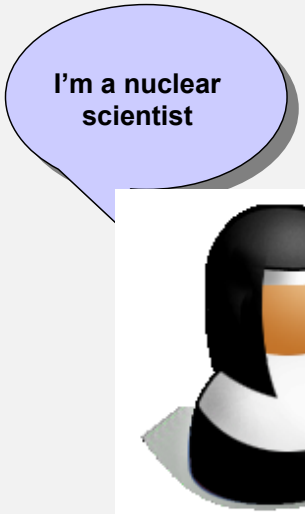
Spoofing

Bob

Eve

Im-personation

Impersonation. This involves the impersonation of a user/device.



Piggy back attacks. This involves adding data onto valid data packets.

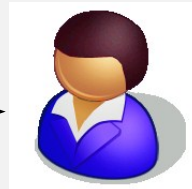
Piggy back

Network weaving

Network weaving. This involves confusing the system onto the whereabouts of a device, or confusing the routing.

Hello…

Hello… Goodbye

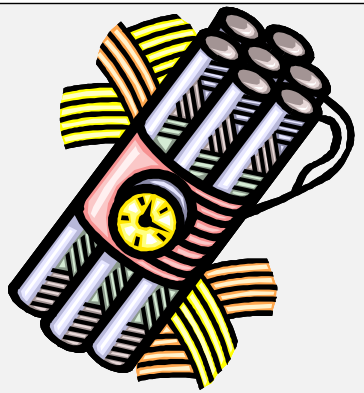


A virus has piggybacked onto an email

Trojan horses. This involves users running programs which look valid, but install an illicit program which will typically do damage to the host.

Best project ever!
Click here

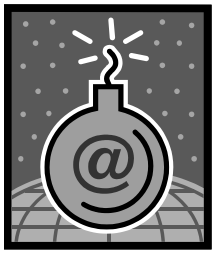
The email contains a Trojan virus



Logic bombs. This involves the installation of a program which will trigger some time in the future based on time or an event.

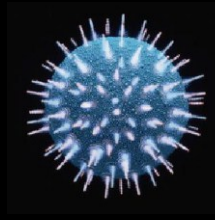
Trojan horse

Logic bombs



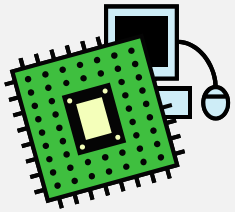
Malevolent worms. This involves a worm program which mutates in a given way which will eventually reduce the quality of service on the network, such as using up CPU resources or network bandwidth.

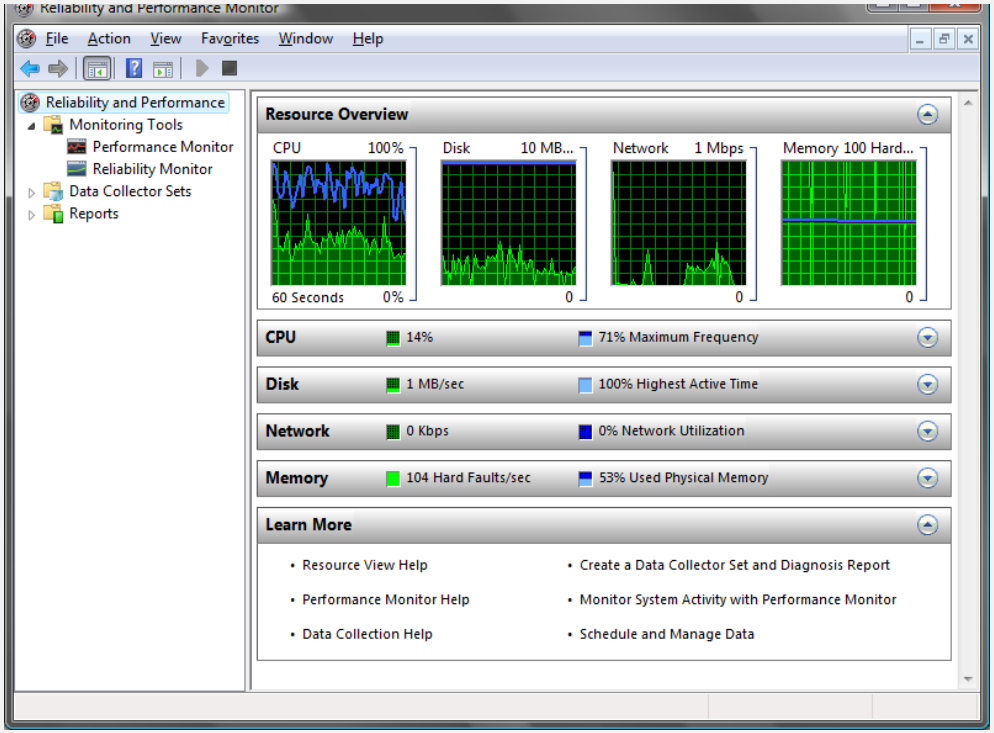
Viruses



Viruses. This involves attaching program which self replicate themselves.

Worms





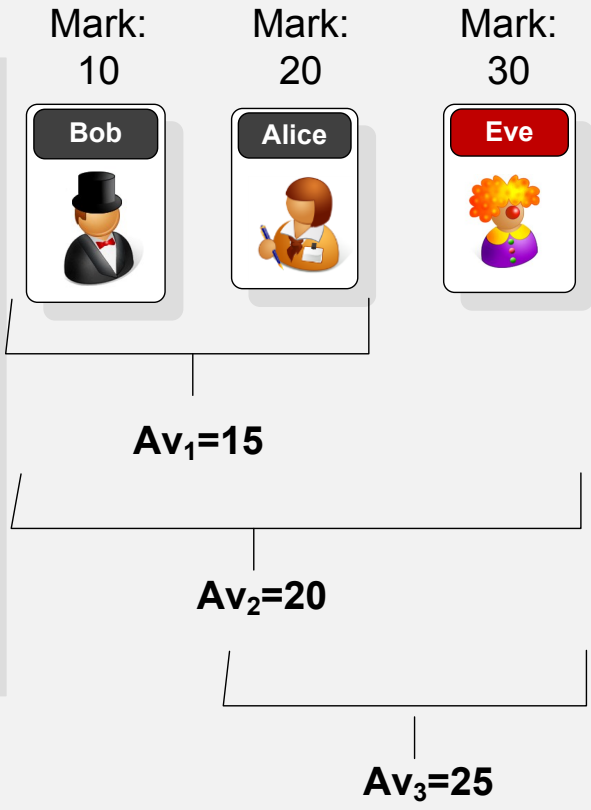

DoS

Bob
Eve
Firewall
Eve
Eve
Continual requests for the service, such as requesting large files from a Web server
End-source DoS. Exhaust the services on a server.
Network bandwidth DoS. Exhaust the network bandwidth.
Web Server
FTP Server

Inference

Inference. This involves exploiting database weaknesses using inferences.

For example … the marks for any student is not allowed, but the average a number of students is allowed.



Query: Average(Bob,Alice) -> Av_1= (B+A)/2
Query: Average(Bob,Eve) -> Av_2= (B+E)/2
Query: Average(Alice,Eve) -> Av_3= (A+E)/2

Av_1-Av_2=(A-E)/2

Av_1-Av_2+Av_3 = (A-E)/2+(A+E)/2=A

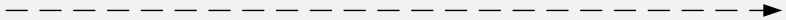
Alice's mark is Av_1-Av_2+Av_3

Alice's mark=Av_1-Av_2+Av_3=15-20+25=20

Covert channel

Covert channels. This involves hiding data in valid network traffic.

Timing channel. Transmit with relative timing of events.
Storage channel. Modify an object (such as adding to network packet headers).



Goodbye!

```
IP Src: 10.0.0.1
IP Dest:192.168.0.1
TTL: 'o'
```

hello

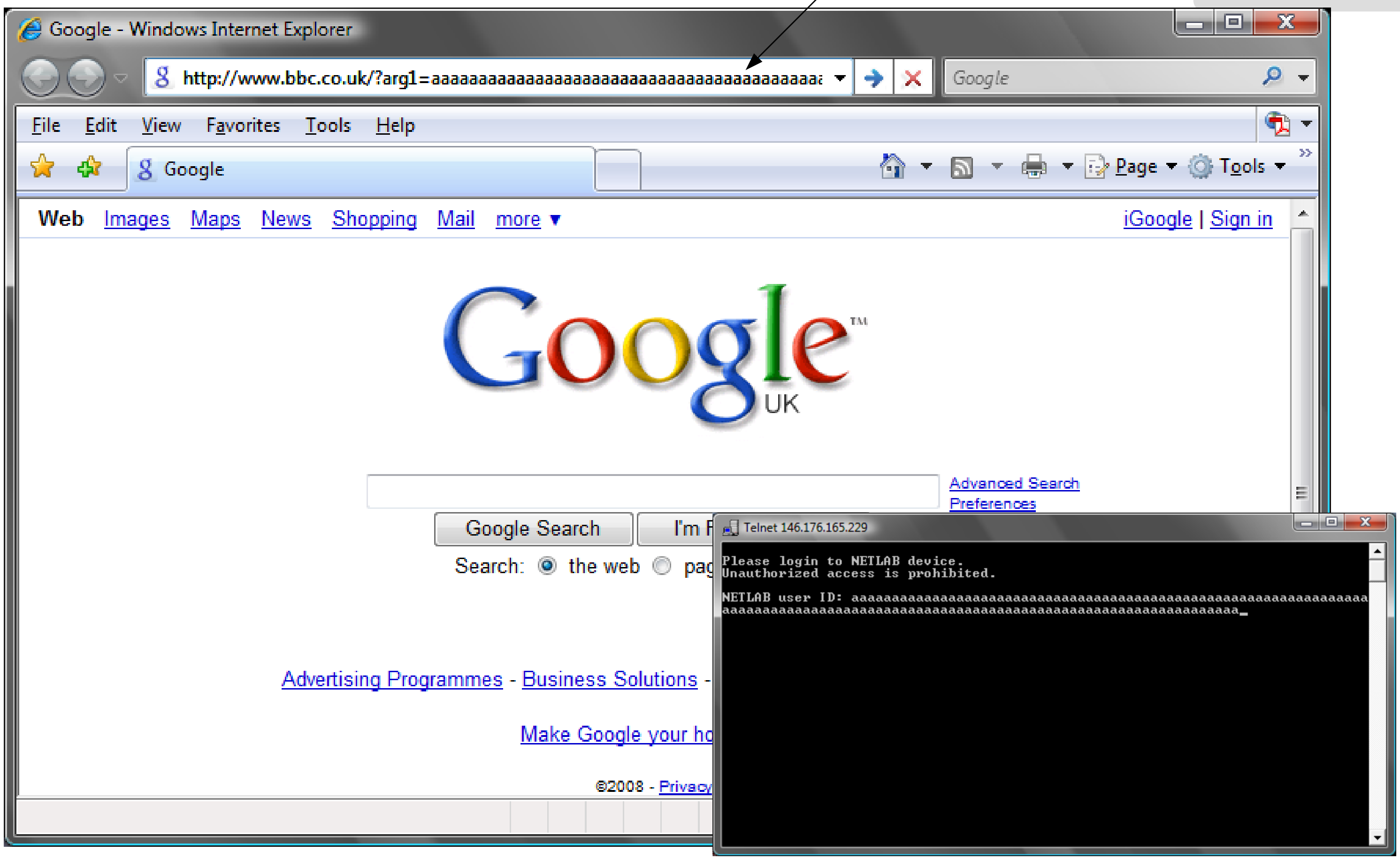
```
IP Src: 10.0.0.1
IP Dest: 192.168.0.1
TTL: 'G'
```

Eve reads the data packets, and the message seems valid, but the message "Go" is hidden in the packet headers.

Active attack

Active attack. This entering incorrect data with the intention to do damage to the system.

Possible buffer overflow attack where the intruder tries to put incorrect information into the page



Threats

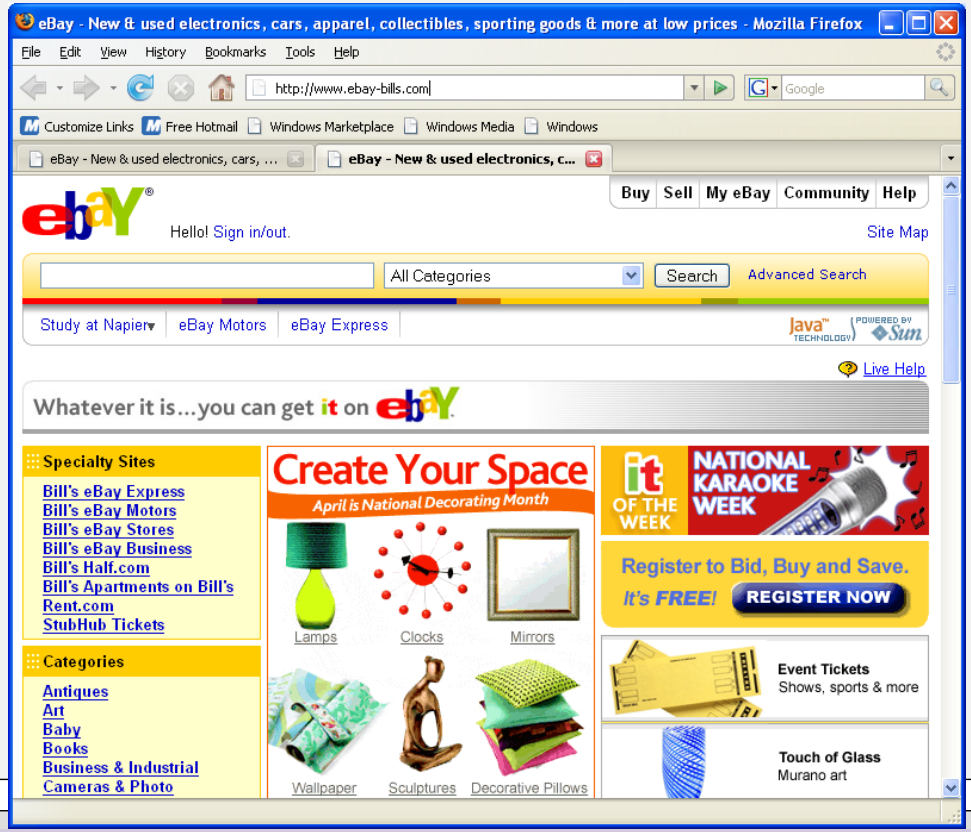
Fundamentals

Authorization attacks. This involves trying to gain access to a higher level of authorization than is valid for the user, such as with password attacks.

Authorization attack

Trap-door

Trap door impersonation. This involves the creation of pages or login screens which look valid, but are used to gain information from a user, such as their bank details, or login password.



Trap-door

eBay: Urgent Security Notice - Message (HTML)

File Edit View Insert Format Tools Actions Help

Reply | Reply to All | Forward

From: eBay [support_ref_5581@ebay.com] Sent: Sun 23/10/2005 11:30

To: School of Computing

Cc:

Subject: eBay: Urgent Security Notice

Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be blocked::http://218.38.30.15:680/rock/Isa/urs, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us.

Trap-door

Valid looking email address (spoofed!)

eBay: Urgent

File Edit View

Reply | Reply to All | Forward

From: eBay [support_ref_5581@ebay.com]
To: School of Computing
Cc:
Subject: eBay: Urgent Security Notice

Valid looking URL (but links to different Site)

Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

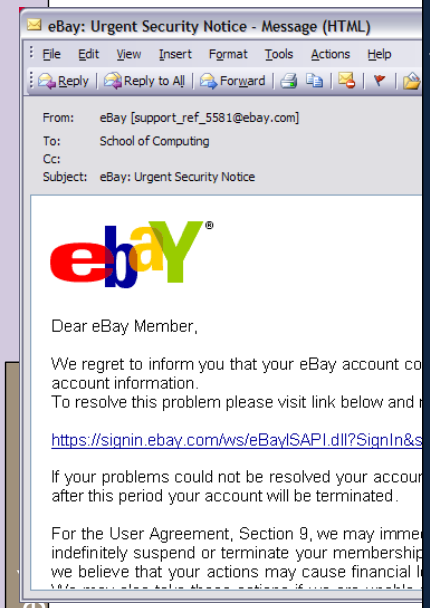
https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be blocked::http://218.38.30.15:680/rock/Isa/urs, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, se to provide our services to you if gal liability for you, our users or us.

```
C:\>nslookup 218.38.30.15

Name:     ns.thundernet.co.kr
Address:  218.38.30.15
```




```
Microsoft Mail Internet Headers Version 2.0
Received: from mer-w2003-6.napier-mail.napier.ac.uk ([146.176.223.1]) by
EVS1.napier-mail.napier.ac.uk with Microsoft SMTPSVC(6.0.3790.1830);
     Wed, 18 Jan 2006 00:17:45 +0000
Received: from pcp0011634462pcs.ivylnd01.pa.comcast.net (Not
Verified[68.38.82.127]) by mer-w2003-6.napier-mail.napier.ac.uk with
NetIQ MailMarshal (v6,1,3,15)
    id <B43cd89280000>; Wed, 18 Jan 2006 00:17:44 +0000
FCC: mailbox://support_id_1779124147875@ebay.com/Sent
X-Identity-Key: id1
Date: Tue, 17 Jan 2006 17:10:39 -0700
From: eBay <support_id_1779124147875@ebay.com>
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: W.Buchanan@napier.ac.uk
Subject: Important Notification
Content-Type: multipart/related;
 boundary="------------020707050401080303030003"
Return-Path: support_id_1779124147875@ebay.com
Message-ID: <MER-W2003-3AM4wEzpE0000ac5c@EVS1.napier-mail.napier.ac.uk>
X-OriginalArrivalTime: 18 Jan 2006 00:17:45.0579 (UTC)
FILETIME=[9B1173B0:01C61BC4]

--------------020707050401080303030003
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit

--------------020707050401080303030003
Content-Type: image/gif;
 name="arcade.GIF"
Content-Transfer-Encoding: base64
Content-ID: <part1.06020402.07040401@support_ref_32@ebay.com>
Content-Disposition: inline;
 filename="arcade.GIF"
```

Fundamentals

Question from eBay Member -- Respond Now - Message (HTML)

File Edit View Insert Format Tools Actions Help

Reply | Reply to All | Forward

From: eBay member: redsticksales [member@ebay.co.uk]

To:

Cc:

Subject: Question from eBay Member -- Respond Now

Mon 02/06/2008 08:15

Example of pressure phishing

Question from eBay Member -- Respond Now

eBay sent this message on behalf of an eBay member via My Messages. Responses sent using email will go to the eBay member directly and will include your email address. Click the **Respond Now** button below to send your response via My Messages (your email address will not be included).

Question from redsticksales

Item: (220206808277)
redsticksales is a **potential buyer**.

Hello, So , you send me the item ???, when I will have my item ??? please respond me right now !!! or i will contact the ebay right now !!!

Thank you!

Respond to this question in My Messages.

Respond Now

Marketplace Safety Tip

Always remember to complete your transactions on eBay - it's the safer way to trade.

Is this message an offer to buy your item directly through email without winning the item on eBay? If so, please help make the eBay marketplace safer by

Item Details

Item number: **220206808277**

End date: **Mar-01-08 20:44:23 PST**

View item description:
https://cgi.ebay.com/ws/eBayISAPI.dll?ViewItem&item=7713864284&sspagename=ADME:B:AAQ:U

Thank you for using eBay
www.ebay.com/

http://202.102.73.112/icons/small/x/signin.ebay.ie/SignIn/index.html

Trap-door

eBay Change Email Notice - Message (HTML)

File Edit View Insert Format Tools Actions Help

Reply | Reply to All | Forward

From: eBay [mem.celine@ebay.co.uk]

To: Buchanan, Bill

Cc:

Subject: eBay Change Email Notice

Example of worry of security problems

eBay sent this message to (w.buchanan@napier.ac.uk).
Your registered name is included to show this message originated from eBay. Learn more.

eBay Change Email Notice

Dear w.buchanan@napier.ac.uk,

Thank you for submitting your change of email address request. Instructions on completing the change have been sent to your new email address. Once the process is completed, your eBay-related email will no longer be routed to this email address.

If you did not make this change, check with family members and others who may have access to your account first. If you still feel that an unauthorized person has changed your email, get help here:
http://pages.ebay.com/help/confidence/isqw-account-theft-reporting.html

Change of email address request was made from:
IP Address: 195.224.154.232
ISP Host: mail.alkane.co.uk

http://www.suryasamudra.com/red

Thank you,
eBay

Learn how you can protect yourself from spoof (fake) emails at:
http://pages.ebay.com/education/spooftutorial

If you would like to receive this email in text format, change your notification preferences.

See our Privacy Policy and User Agreement if you have questions about eBay's communication policies.
Privacy Policy: http://pages.ebay.com/help/policies/privacy-policy.html
User Agreement: http://pages.ebay.com/help/policies/user-agreement.html

Fundamentals

Threats: Authorization attack/trap door

Trap-door

Question from eBay Member -- Respond Now - Message (HTML)

File Edit View Insert Format Tools Actions Help

Reply | Reply to All | Forward

This message was sent with High importance.

From: eBay [service@eBay.com] Sent: Sun 08/07/2007 14:59

To:

Cc:

Subject: Question from eBay Member -- Respond Now

Question from eBay Member -- Respond Now

eBay sent this message on behalf of an eBay member via My Messages. Responses sent using email will go to the eBay member directly and will include your email address. Click the **Respond Now** button below to send your response via My Messages (your email address will not be included).

Question from whatdadealiz

Item: (7713864284)
whatdadealiz is a **potential buyer**.

Hi there, when did you send me a message and what is it about? BTW, I don't like your tone. Please dont do that to me. I can report you as well, remember?

Original message:
Why dont you answer to my emails!!! If you dont Respond Now I will contact ebay safeharbor and report you ! Lett me know, I am not a fool ! Thank you ! !

Respond to this question in My Messages.

Respond Now

Marketplace Safety Tip

Always remember to complete your transactions on eBay - it's the safer way to trade.

Is this message an offer to buy your item directly through email without winning the item on eBay? If so, please help make the eBay marketplace safer by reporting it to us. These external transactions may be unsafe and are against eBay policy. Learn more about trading safely.

Is this email inappropriate?

Item Details

Item number: 7713864284

End date: 03-June-07 13:17:42 BST

View item description:

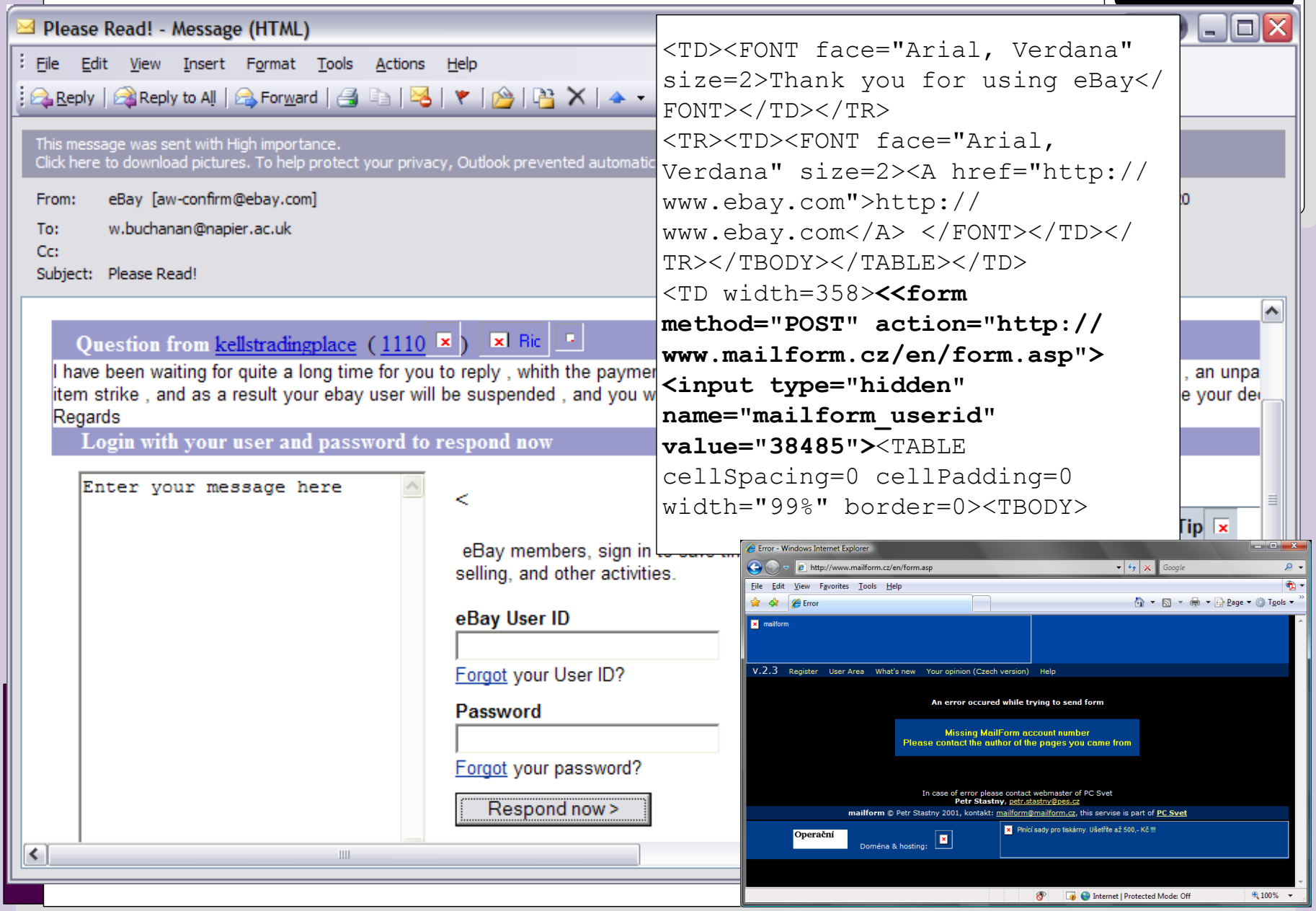
Show Network Warnings

Show Network Connectivity Changes

Fundamentals

Threats: Authorization attack/trap door

Trap-door

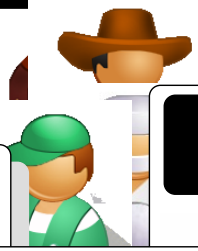


Threats: Authorization attack/trap door

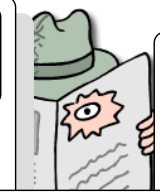
Fundamentals

Trap-door

Mis-representation

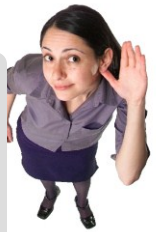


Visual spying



Logical scavenging

Eavesdropping

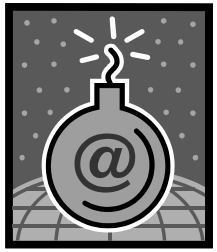


Interference

Physical removal

Spoofing

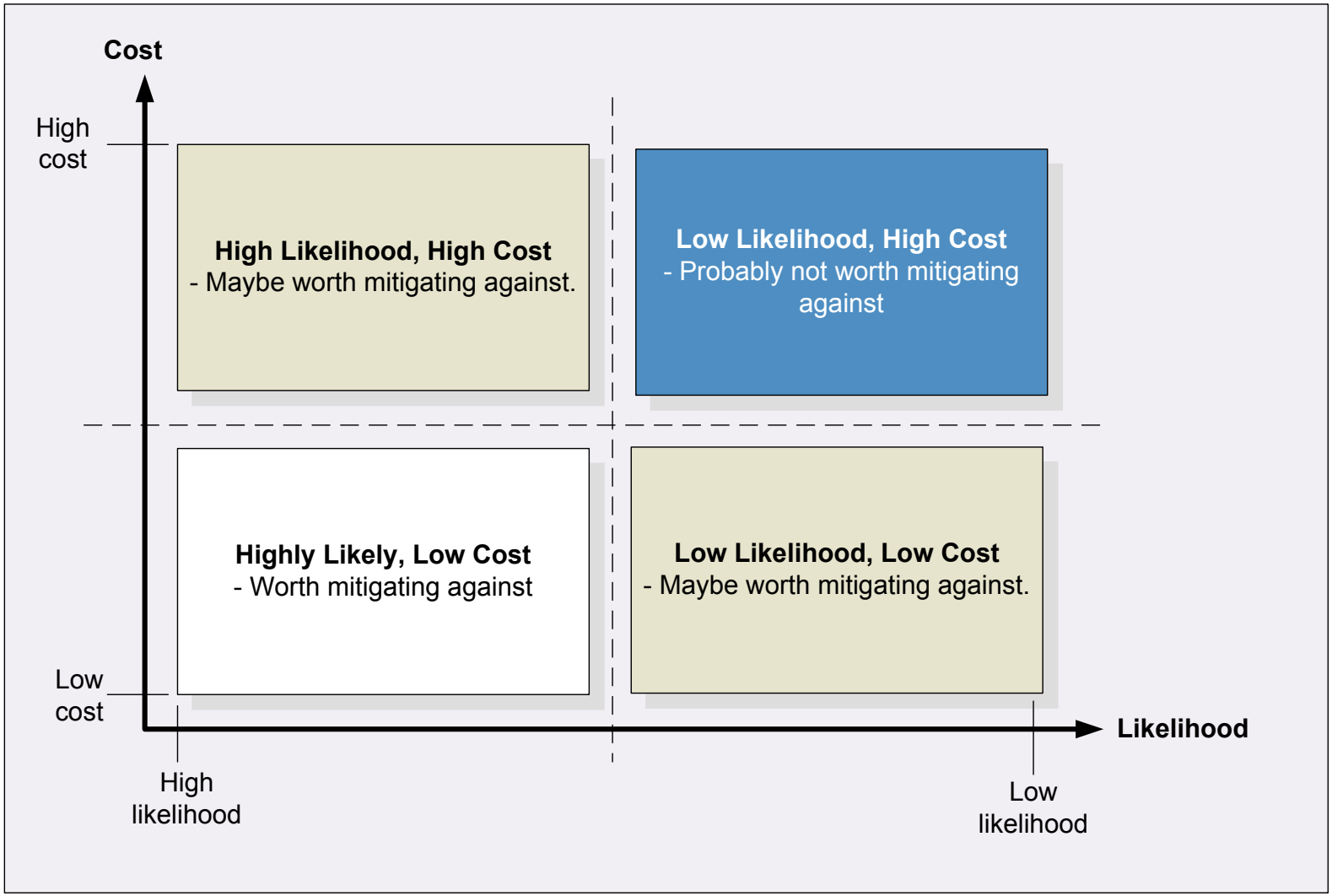
Logic bombs

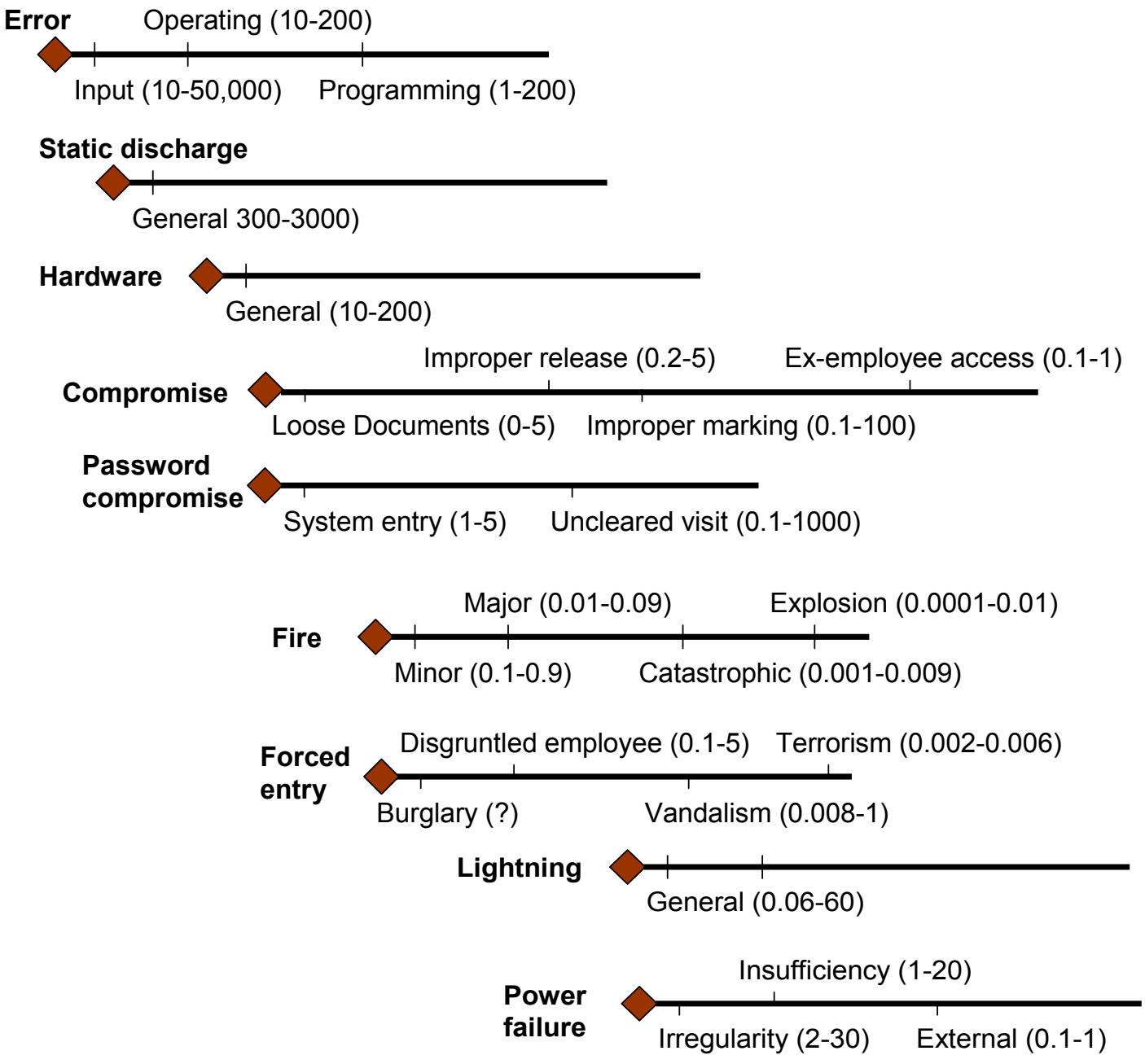


Trojan horse

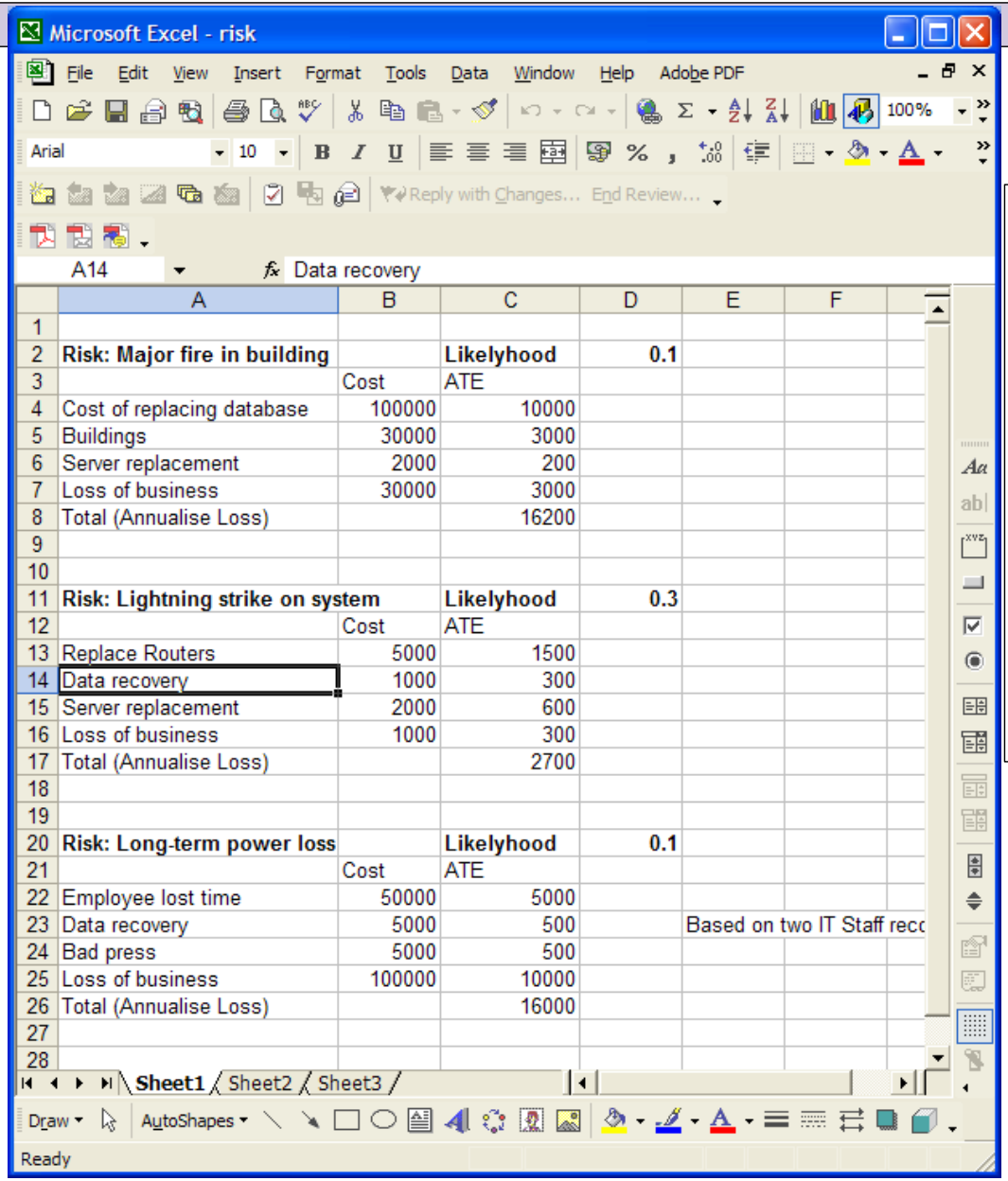
Authorizati attack

Risk Analysis


Cost
High cost
Low cost
High likelihood
Low likelihood
Likelihood
High Likelihood, High Cost
- Maybe worth mitigating against.
Low Likelihood, High Cost
- Probably not worth mitigating against
Highly Likely, Low Cost
- Worth mitigating against
Low Likelihood, Low Cost
- Maybe worth mitigating against.



Probability of event



	A	B	C	D	E	F
1						
2	**Risk: Major fire in building**		**Likelyhood**	**0.1**		
3		Cost	ATE			
4	Cost of replacing database	100000	10000			
5	Buildings	30000	3000			
6	Server replacement	2000	200			
7	Loss of business	30000	3000			
8	Total (Annualise Loss)		16200			
9						
10						
11	**Risk: Lightning strike on system**		**Likelyhood**	**0.3**		
12		Cost	ATE			
13	Replace Routers	5000	1500			
14	Data recovery	1000	300			
15	Server replacement	2000	600			
16	Loss of business	1000	300			
17	Total (Annualise Loss)		2700			
18						
19						
20	**Risk: Long-term power loss**		**Likelyhood**	**0.1**		
21		Cost	ATE			
22	Employee lost time	50000	5000			
23	Data recovery	5000	500		Based on two IT Staff recc	
24	Bad press	5000	500			
25	Loss of business	100000	10000			
26	Total (Annualise Loss)		16000			
27						
28						

ALE = *T* x *V*

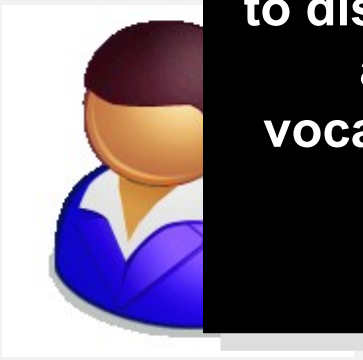
ALE is the Annual Lost Expectancy
T is the likelihood of a threat
V is the value of the particular asset.

Eg. If the likelihood of a denial-of-service on a WWW-based database is once every three years, and the loss to sales is £100K, then the ALE will be:

ALE = £100K x 1/3 = £33K per annum

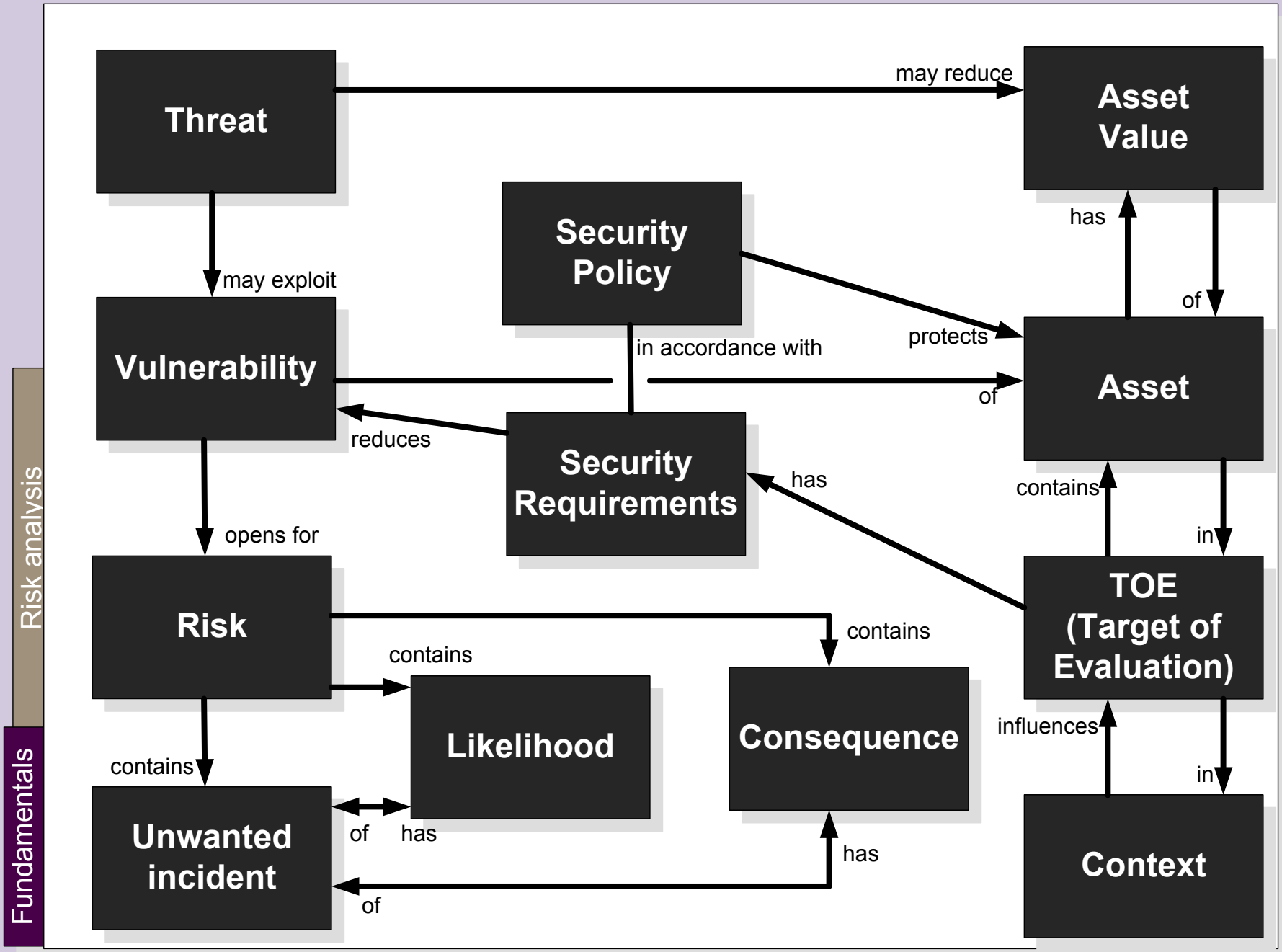
Annual Loss Expectancy (ALE)

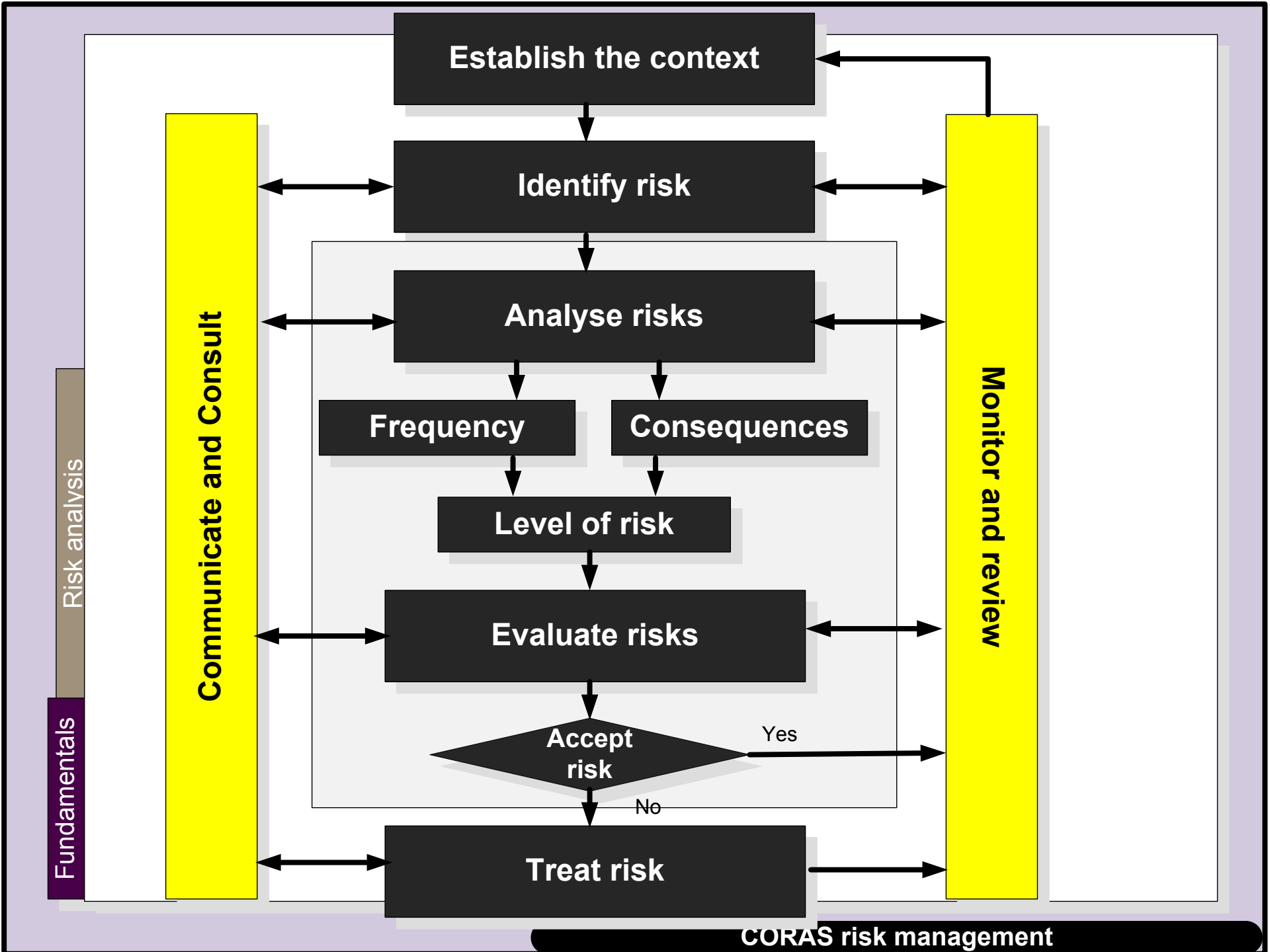
Business context



Technical context

"Get two risk management experts in a room, one financial and the other IT, and they will NOT be able to discuss risk. Each puts risk into a different context … different vocabularies, definitions, metrics, processes and standards … "
Woloch (2006)

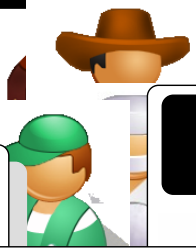

Threat
may reduce
Asset Value
Security Policy
has
may exploit
of
Vulnerability
protects
in accordance with
Asset
of
reduces
Security Requirements
has
contains
in
opens for
Risk
TOE (Target of Evaluation)
contains
contains
Likelihood
Consequence
influences
contains
in
Unwanted incident
of
has
has
Context
of
Risk analysis
Fundamentals
CORAS ontology


Establish the context
Identify risk
Analyse risks
Frequency
Consequences
Level of risk
Evaluate risks
Accept risk
Yes
No
Treat risk
Communicate and Consult
Monitor and review
Risk analysis
Fundamentals
CORAS risk management

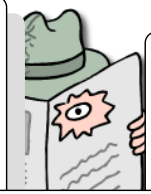
Fundamentals

Trap-door

Mis-representation

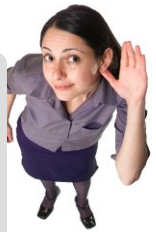


Visual spying



Logical scavenging

Eavesdropping

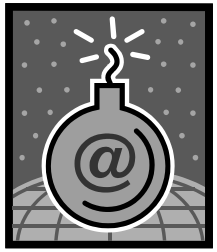


Interference

Physical removal

Spoofing

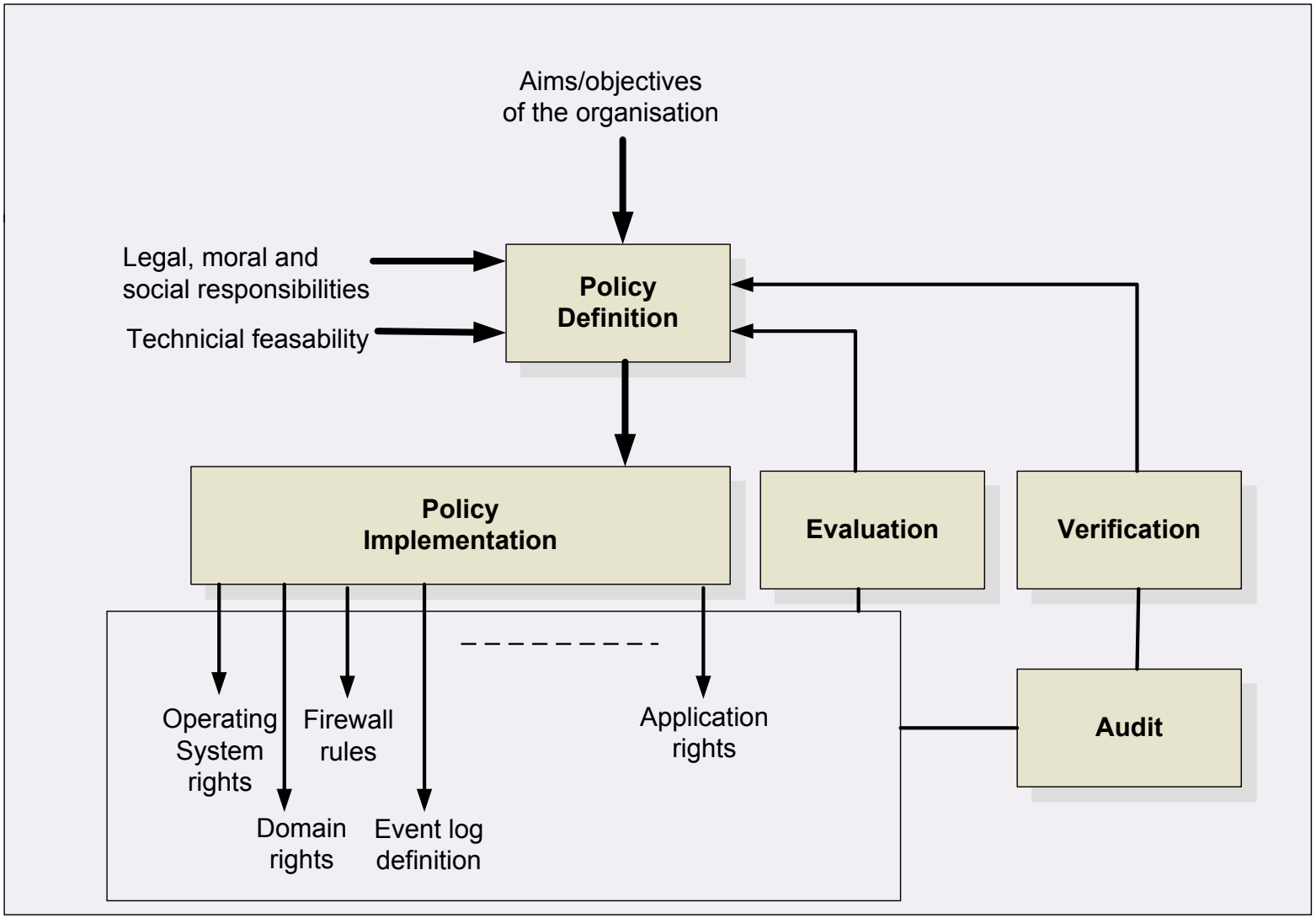
Logic bombs

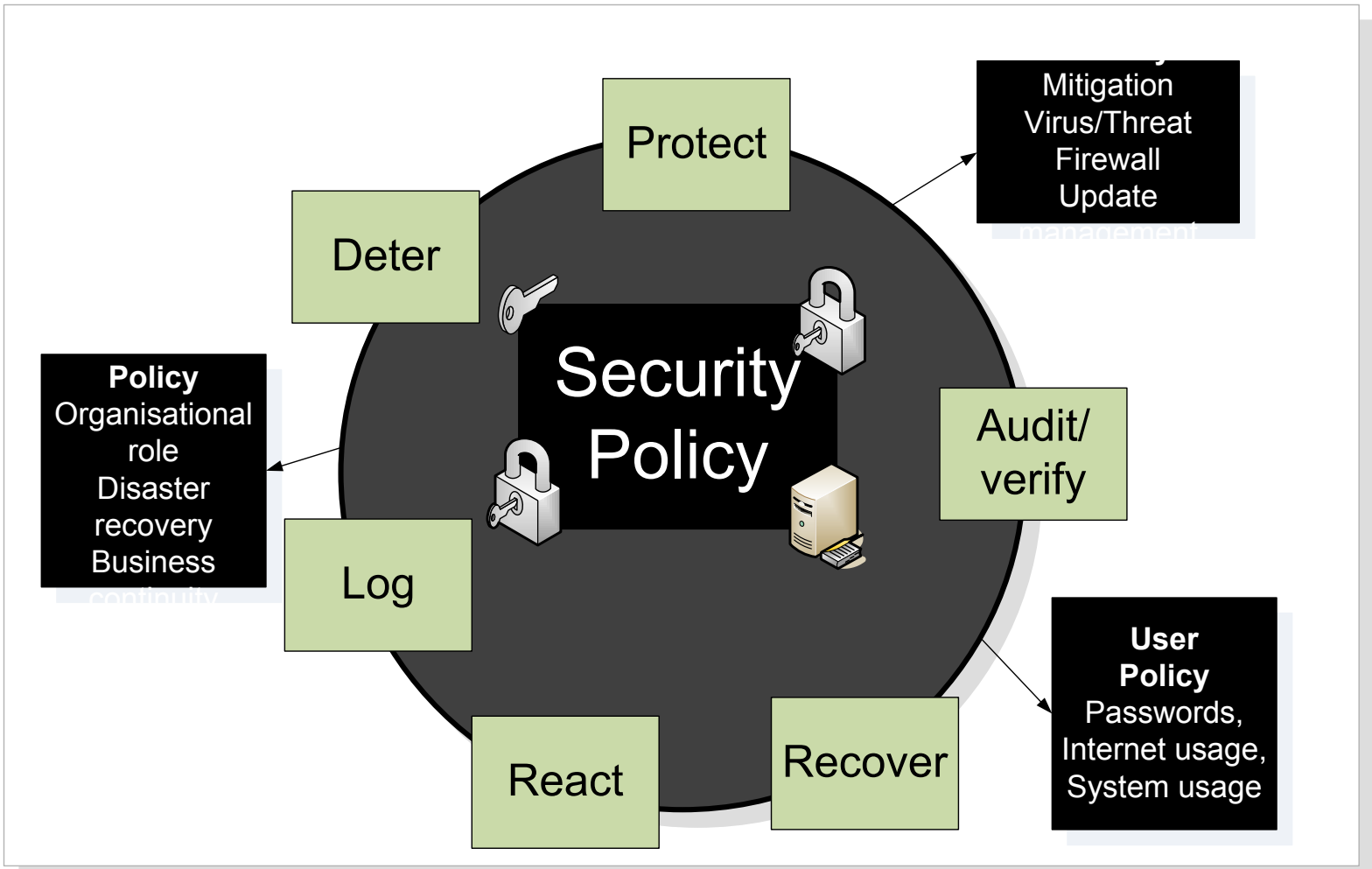


Trojan horse

Authorizati attack

Security Policy

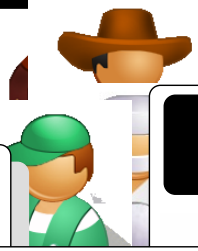

Aims/objectives
of the organisation
Legal, moral and
social responsibilities
Technicial feasability
Policy
Definition
Policy
Implementation
Evaluation
Verification
Audit
Operating
System
rights
Firewall
rules
Application
rights
Domain
rights
Event log
definition


Protect
Mitigation
Virus/Threat
Firewall
Update
Deter
Security
Policy
Policy
Organisational
role
Disaster
recovery
Business
Audit/
verify
Log
User
Policy
Passwords,
Internet usage,
System usage
React
Recover

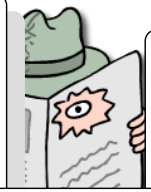
Fundamentals

Trap-door

Mis-representation

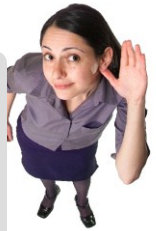


Visual spying



Logical scavenging

Eavesdropping

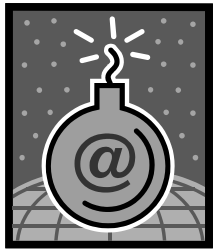


Interference

Physical removal

Spoofing

Logic bombs

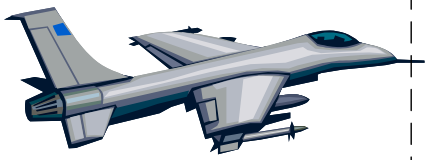


Trojan horse

Authorizati attack

Key Principles

Enemy takes some time to breach each of the levels of defence

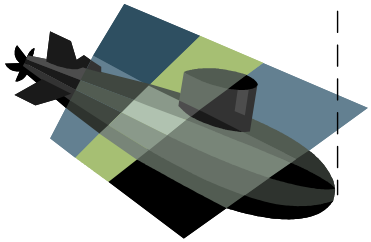


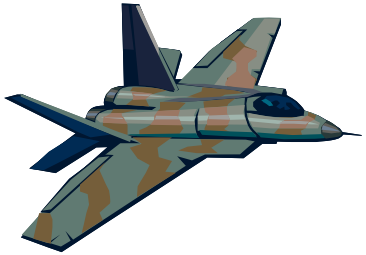
Defence

Defence

Defence

Defence





Forth-level defence

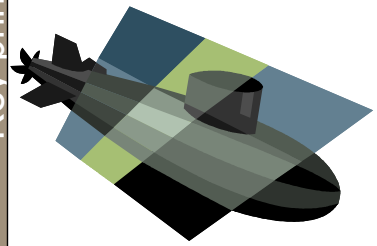
Third-level defence

Second-level defence

First-level defence

Threats: Interference/Physical attacks

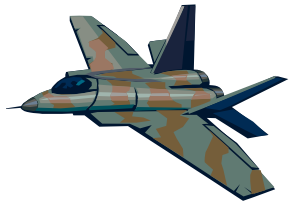



Trusted (our side)

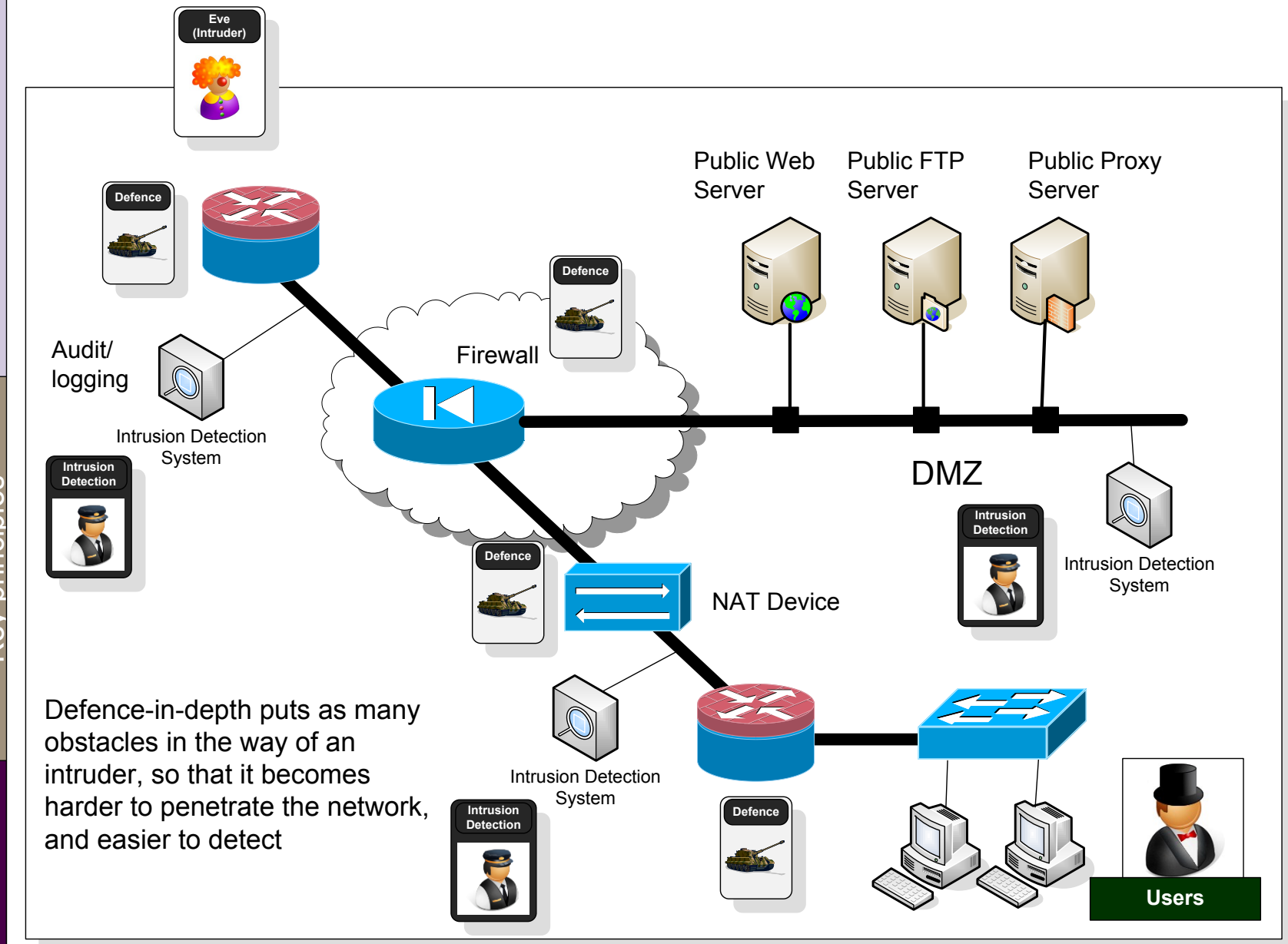



DMZ – an area where military actions are prohibited

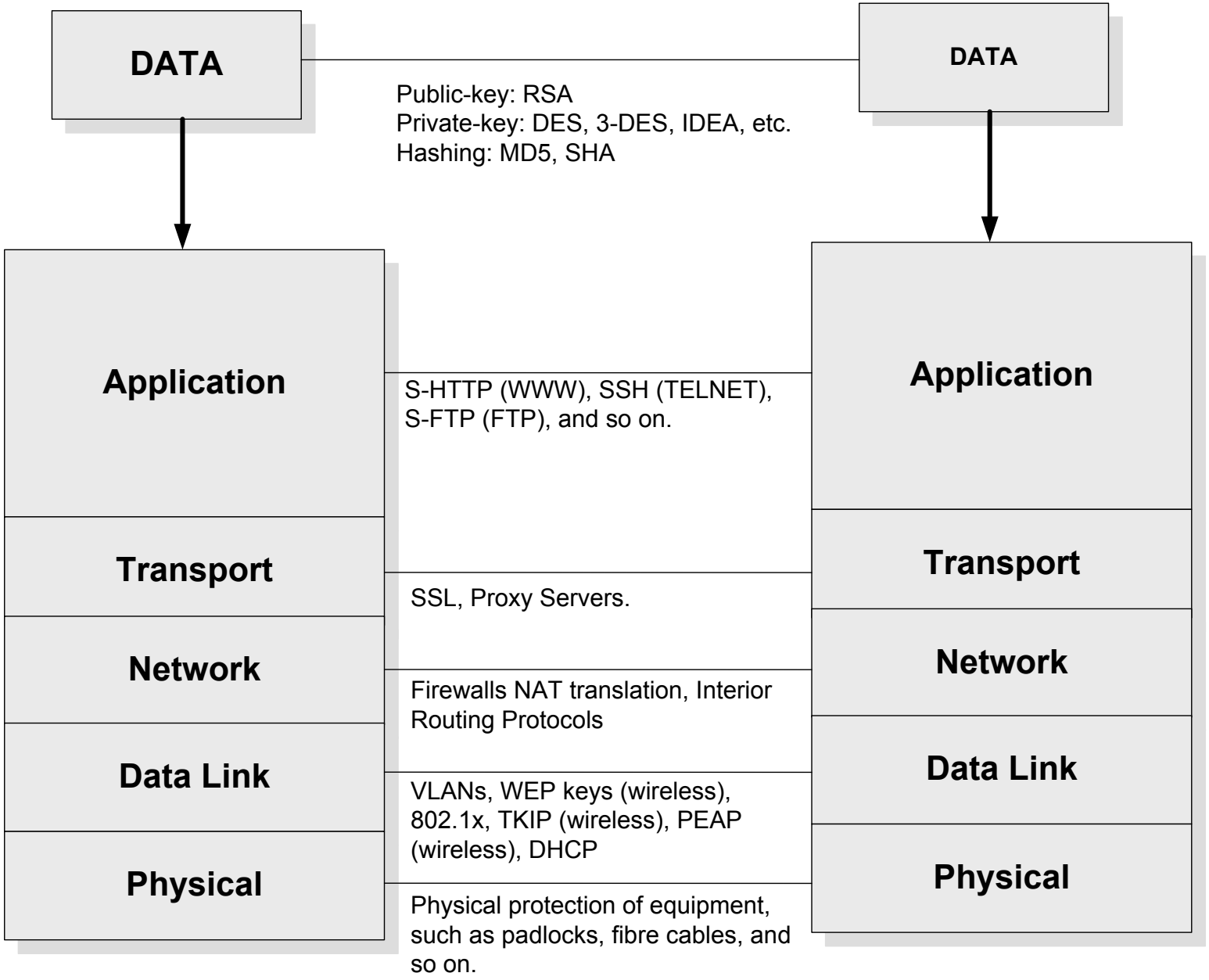


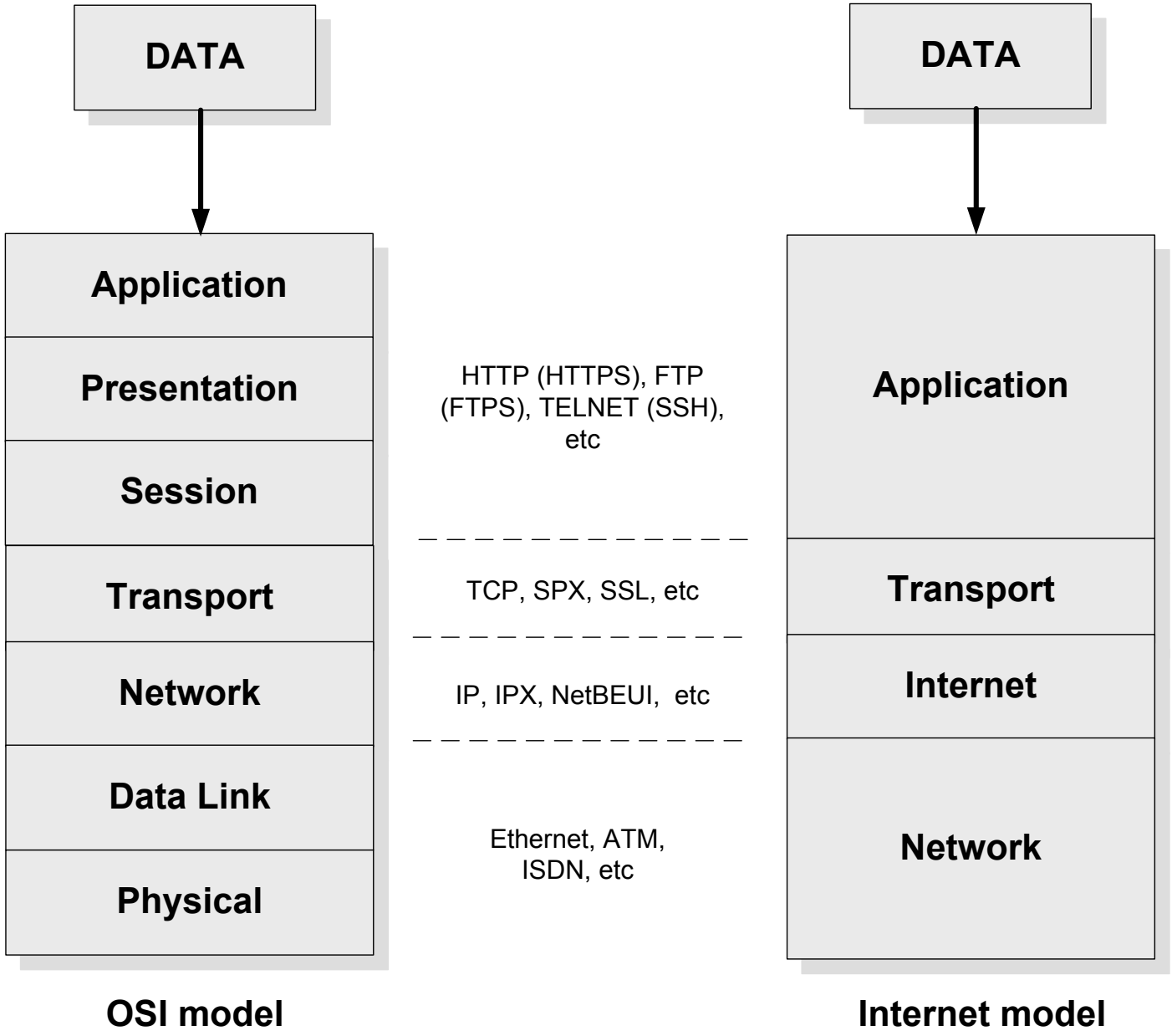


Untrusted (their side)



Defence-in-depth puts as many obstacles in the way of an intruder, so that it becomes harder to penetrate the network, and easier to detect

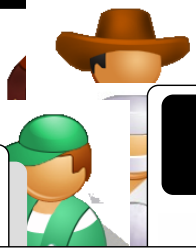

DATA
DATA
Public-key: RSA
Private-key: DES, 3-DES, IDEA, etc.
Hashing: MD5, SHA
Application
Transport
Network
Data Link
Physical
S-HTTP (WWW), SSH (TELNET), S-FTP (FTP), and so on.
SSL, Proxy Servers.
Firewalls NAT translation, Interior Routing Protocols
VLANs, WEP keys (wireless), 802.1x, TKIP (wireless), PEAP (wireless), DHCP
Physical protection of equipment, such as padlocks, fibre cables, and so on.
Application
Transport
Network
Data Link
Physical


DATA
Application
Presentation
Session
Transport
Network
Data Link
Physical
OSI model
HTTP (HTTPS), FTP (FTPS), TELNET (SSH), etc
TCP, SPX, SSL, etc
IP, IPX, NetBEUI, etc
Ethernet, ATM, ISDN, etc
DATA
Application
Transport
Internet
Network
Internet model

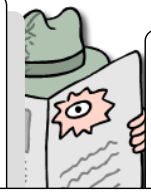
Fundamentals

Trap-door

Mis-representation

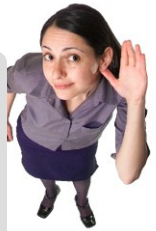


Visual spying



Logical scavenging

Eavesdropping

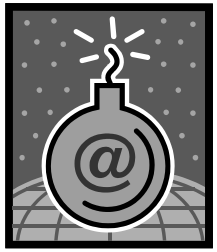


Interference

Physical removal

Spoofing

Logic bombs



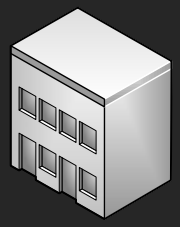
Trojan horse

Authorizati attack

ISO 27002

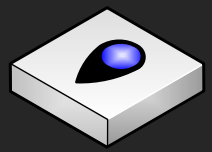
1. Business Continuity Planning

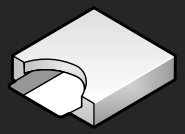
To counteract interruptions to business activities and to critical business processes.



2. Access Control

- Control access to information
- Prevent unauthorised access to information systems
- Ensure the protection of networked services
- Prevent unauthorized computer access
- Detect unauthorised activities.
- Ensure information security when using mobile computing and tele-networking facilities





3. System Acquisition, Development and Maintenance

- Ensure security is built into operational systems;
- Prevent loss, modification or misuse of user data in application systems;
- Protect the confidentiality, authenticity and integrity of information;
- Ensure IT projects and support activities are conducted in a secure manner;
- Maintain the security of application system software and data.

ISO 27002.
Started life as “Information Security Code of Practice” from the UK (DTI), and published in the 1990, and recently changed from ISO/IEC 17799 to ISO/IEC 27002

Fundam

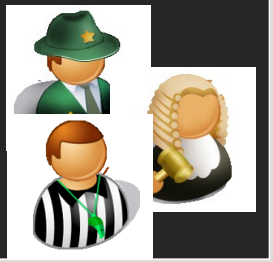
4. Physical and Environmental Security

- Prevent unauthorised access, damage and interference to business premises and information;
- Prevent loss, damage or compromise of assets and interruption to business activities;
- Prevent compromise or theft of information and information processing facilities.

ISO 27002.
Started life as “Information Security Code of Practice” from the UK (DTI), and published in the 1990, and recently changed from ISO/IEC 17799 to ISO/IEC 27002

5. Compliance

- Avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements
- Ensure compliance of systems with organizational security policies and standards
- Maximize the effectiveness of and to minimize interference to/from the system audit process.



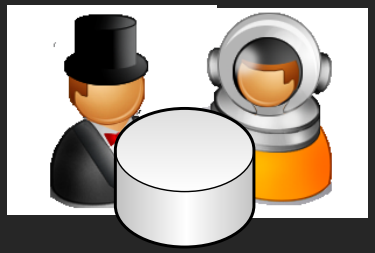
6. Human Resource Security

- To reduce risks of human error, theft, fraud or misuse of facilities;
- to ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work;
- to minimise the damage from security incidents and malfunctions and learn from such incidents.

ISO 27002.
Started life as “Information Security Code of Practice” from the UK (DTI), and published in the 1990, and recently changed from ISO/IEC 17799 to ISO/IEC 27002

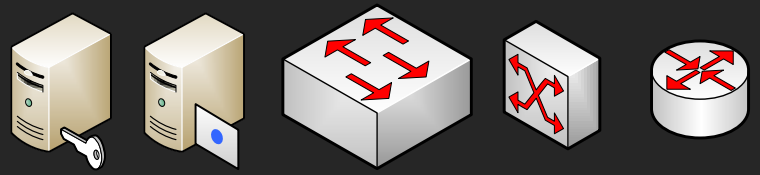
7. Security Organisation

- Manage information security within the Company;
- Maintain the security of organizational information processing facilities and information assets accessed by third parties.
- Maintain the security of information when the responsibility for information processing has been outsourced to another organization.



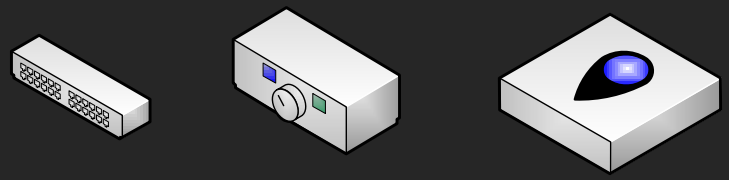
8. Computer and Network Management

- Ensure the correct and secure operation of information processing facilities;
- Minimise the risk of systems failures;
- Protect the integrity of software and information;
- Maintain the integrity and availability of information processing and communication;
- Ensure the safeguarding of information in networks and the protection of the supporting infrastructure;
- Prevent damage to assets and interruptions to business activities;
- Prevent loss, modification or misuse of information exchanged between organizations.



9. Asset Classification and Control

Maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.



ISO 27002.
Started life as “Information Security Code of Practice” from the UK (DTI), and published in the 1990, and recently changed from ISO/IEC 17799 to ISO/IEC 27002

11. Security Incident Management

Anticipating and responding appropriately to information security breaches

10. Security Policy

Provide management direction and support for information security.

12. Risk Analysis

Understand risks involved

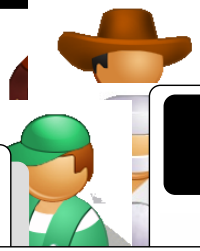
ISO 27002

Fundamentals

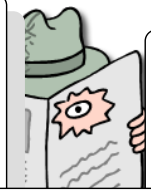
Fundamentals

Trap-door

Mis-representation

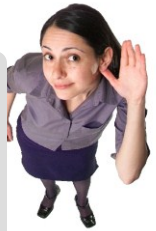


Visual spying



Logical scavenging

Eavesdropping

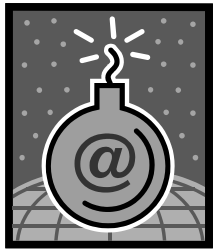


Interference

Physical removal

Spoofing

Logic bombs



Trojan horse

Authorizati attack

Conclusions