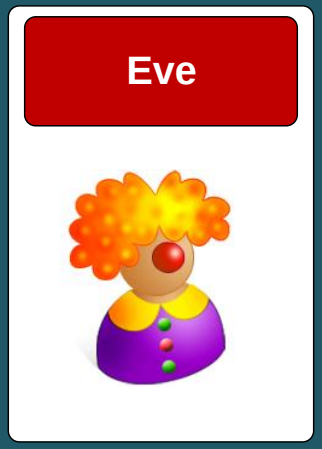
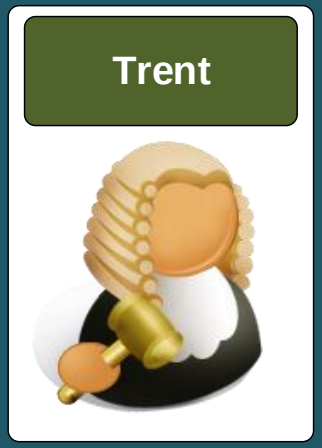
Incident Response

- Introduction.
- Risk Analysis.
- Risk Management.
- Outline of threats.
- Data Loss.
- Fundamentals.

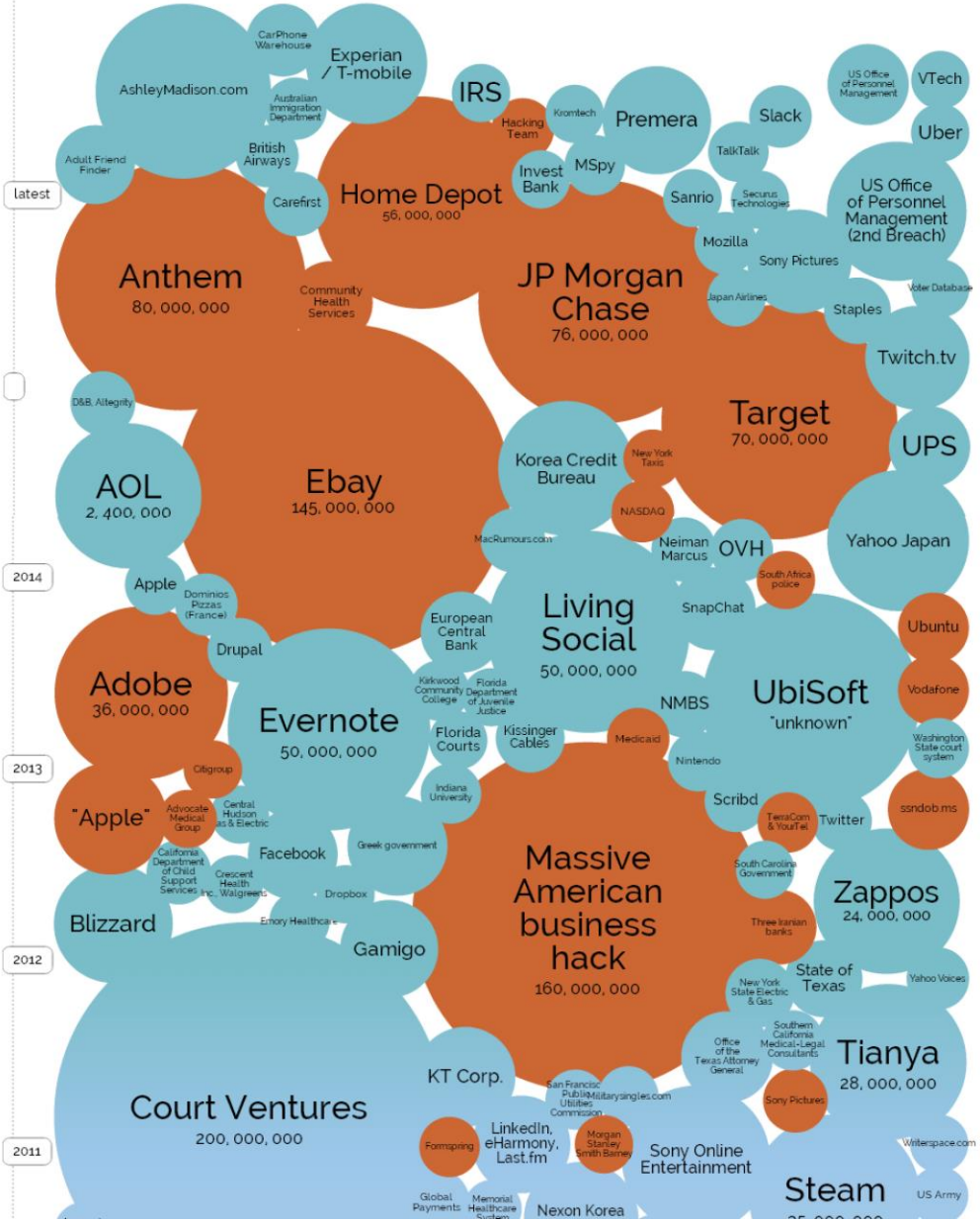




Author: Prof Bill Buchanan

Types

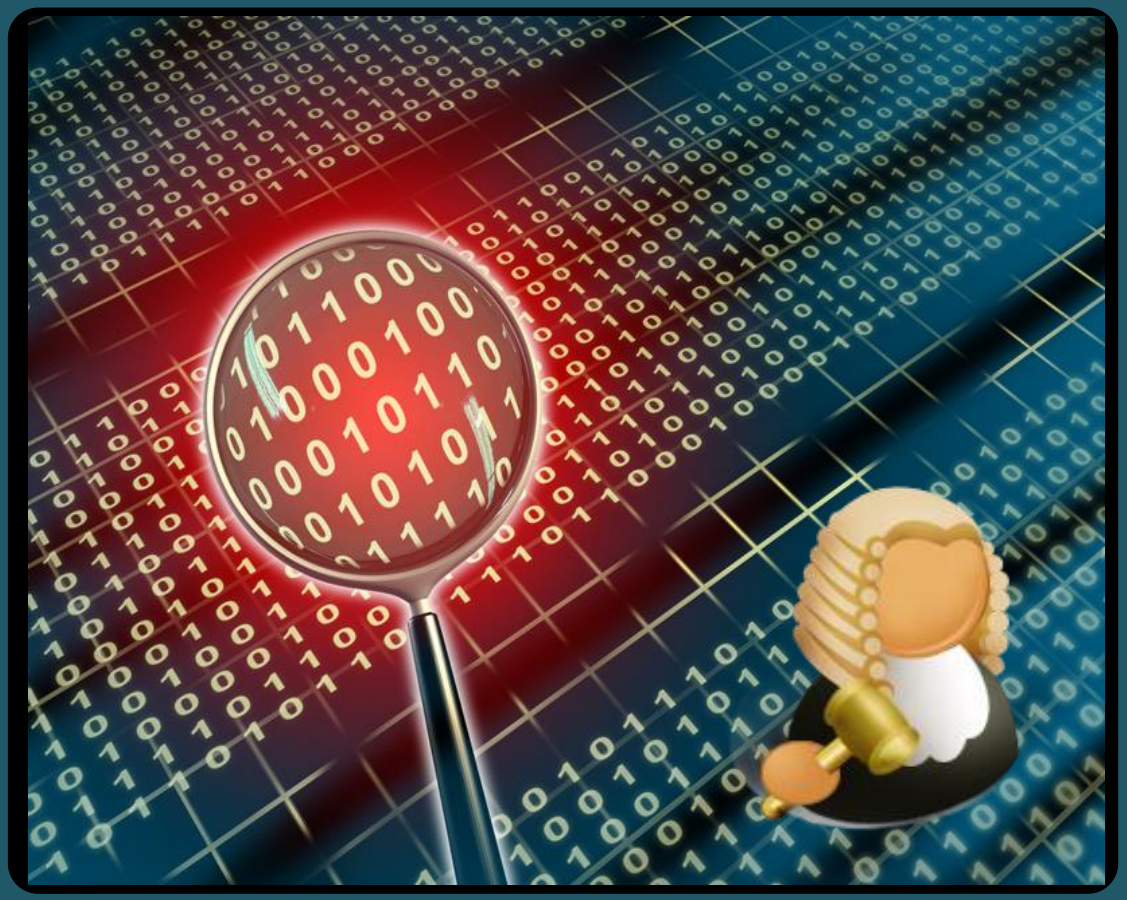
Inc Response



Author: Prof Bill Buchanan

Some data breaches

Incident Response



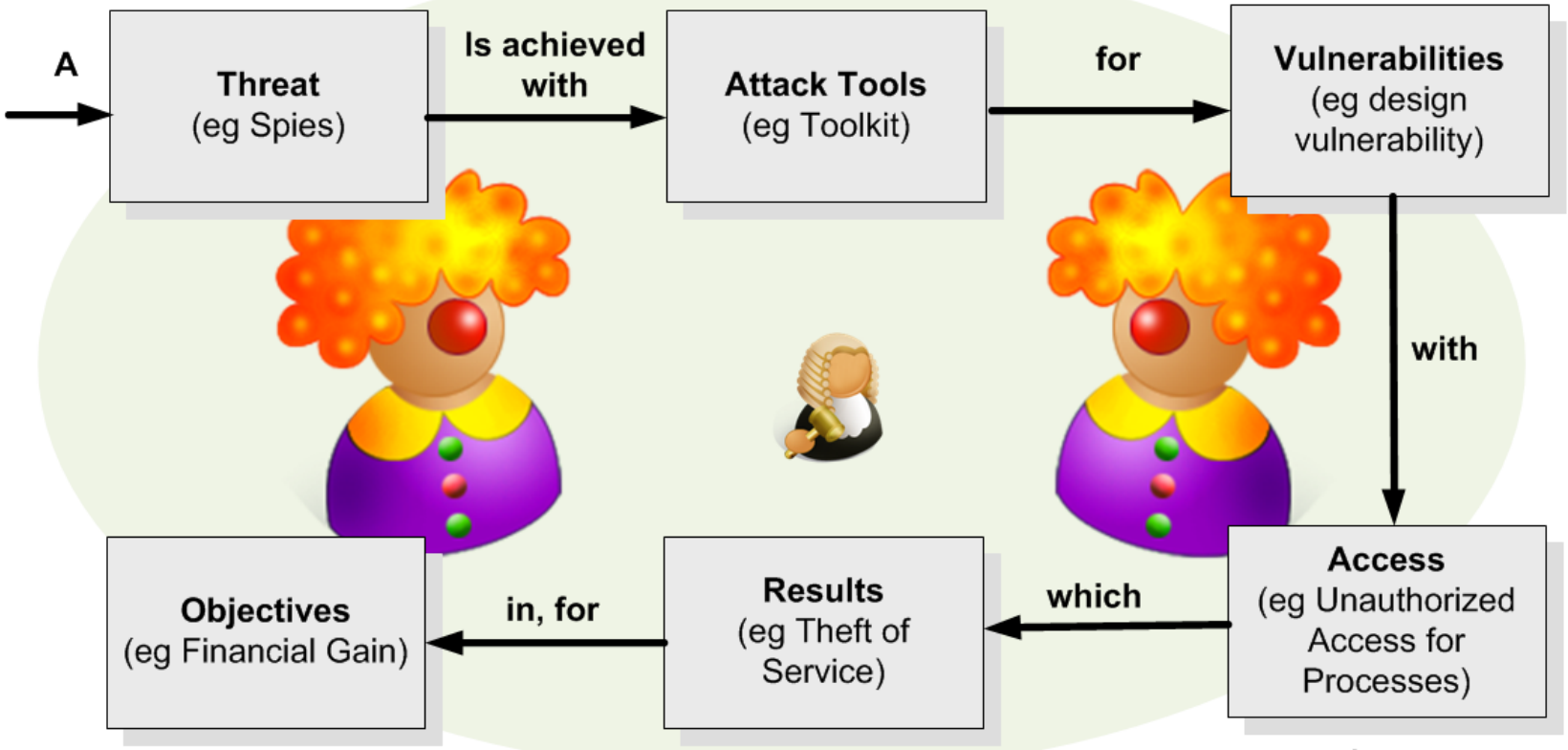
Incident Taxonomy

Author: Prof Bill Buchanan

A Threat:
- Hacker.
- Spies
- Terrorists.
- Corporate Raiders.
- Professional Criminals.
- Vandals.
- Military Forces.

is achieved with Attack Tools:
- User command.
- Script or program.
- Autonomous Agent.
- Toolkit
- Distributed Tool.
- Data Tap.

for Vulnerabilities:
- Implementation vulnerability.
- Design vulnerability.
- Configuration vulnerability.



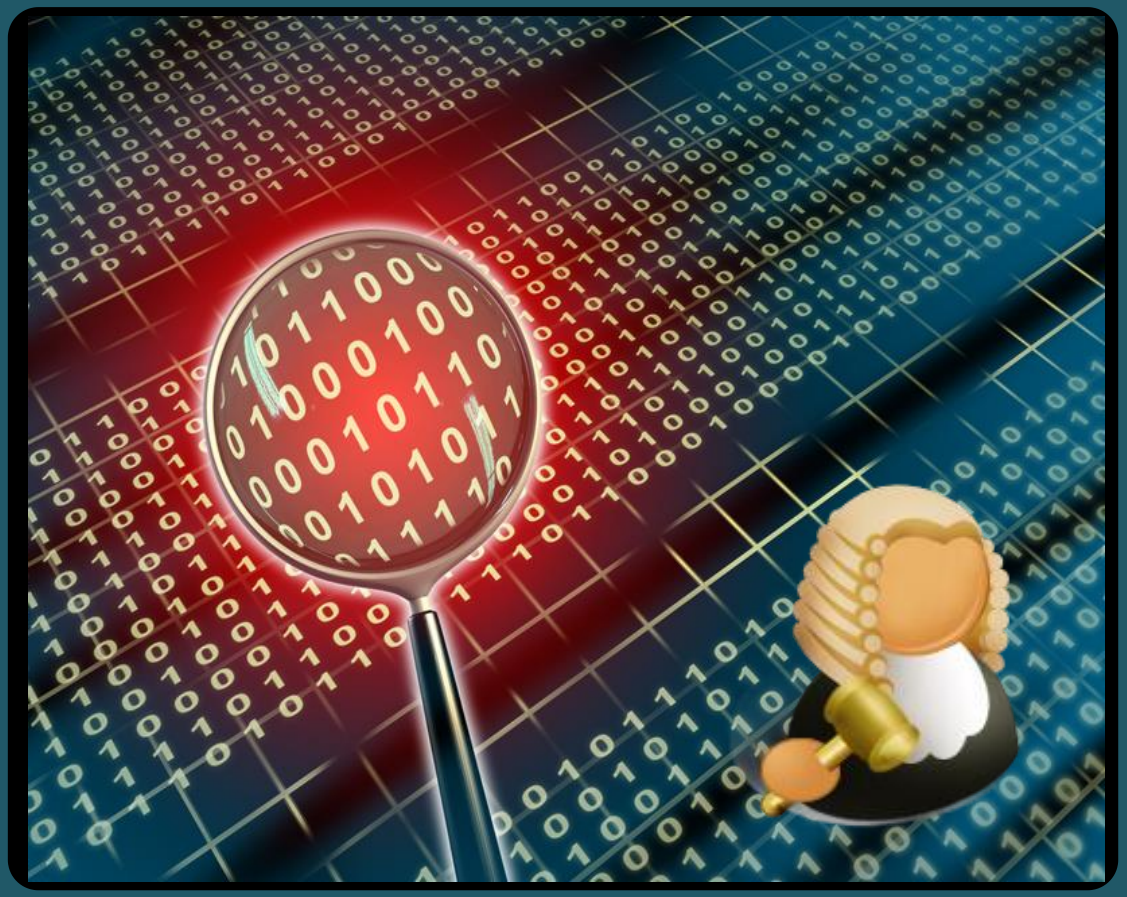
for Objectives:
- Challenge/Status.
- Political Gain.
- Financial Gain.
- Damage.
- Destruction of an Enemy.

which Results in:
- Corruption of Information.
- Disclosure of Information.
- Theft of Service.
- Denial-of-Service.

with Access for:
- Files.
- Data in transit.
- Objects in Transit.
- Invocations in Transit.

Author: Prof Bill Buchanan

Incident Response



Data Sources/Timeline

Author: Prof Bill Buchanan

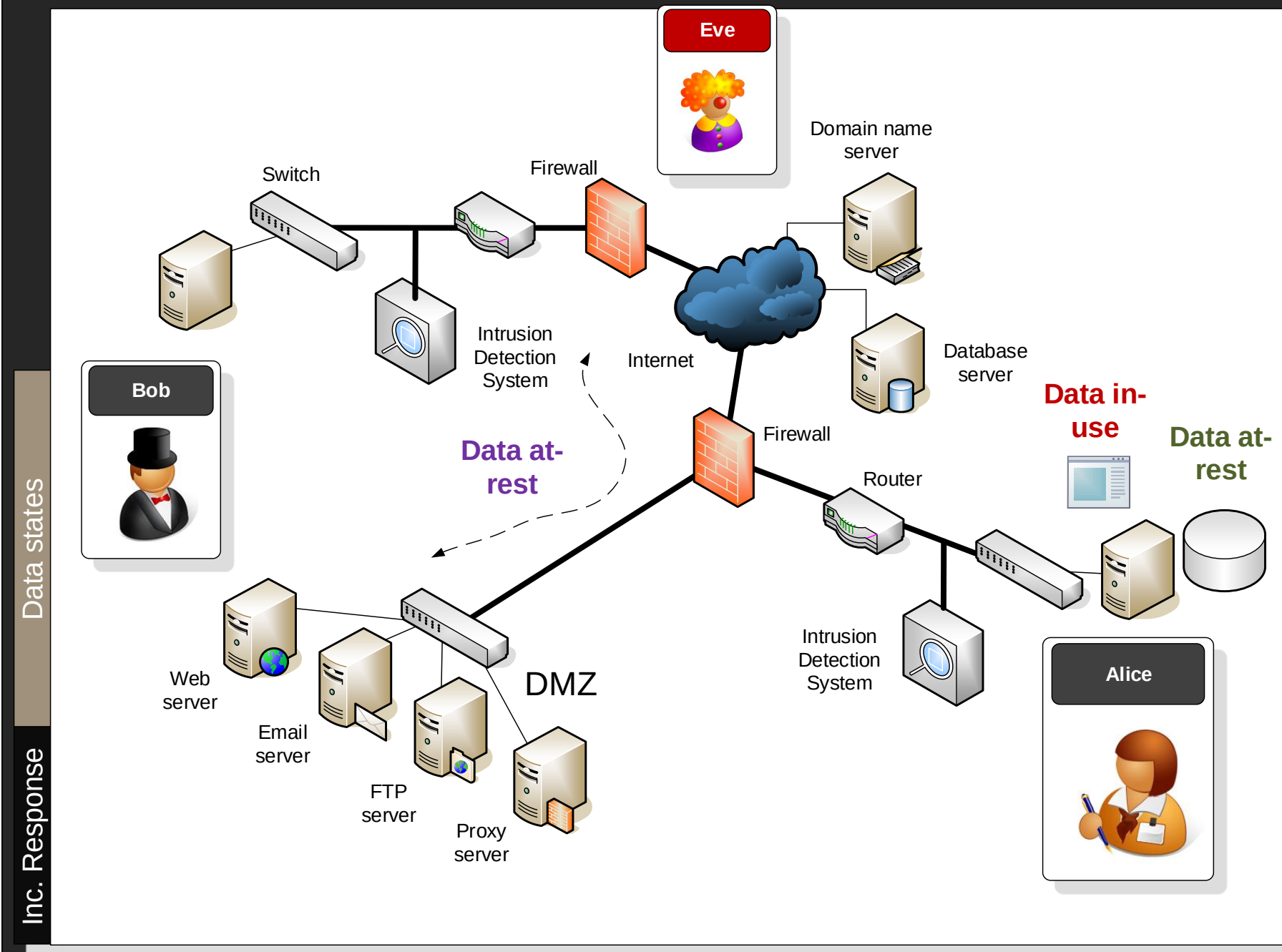
Before Incident

During Incident

After Incident

Intrusion Detection

Author: Prof Bill Buchanan



Data in-motion, data in-use and data at-rest

Before Incident	During Incident	After Incident

Timeline

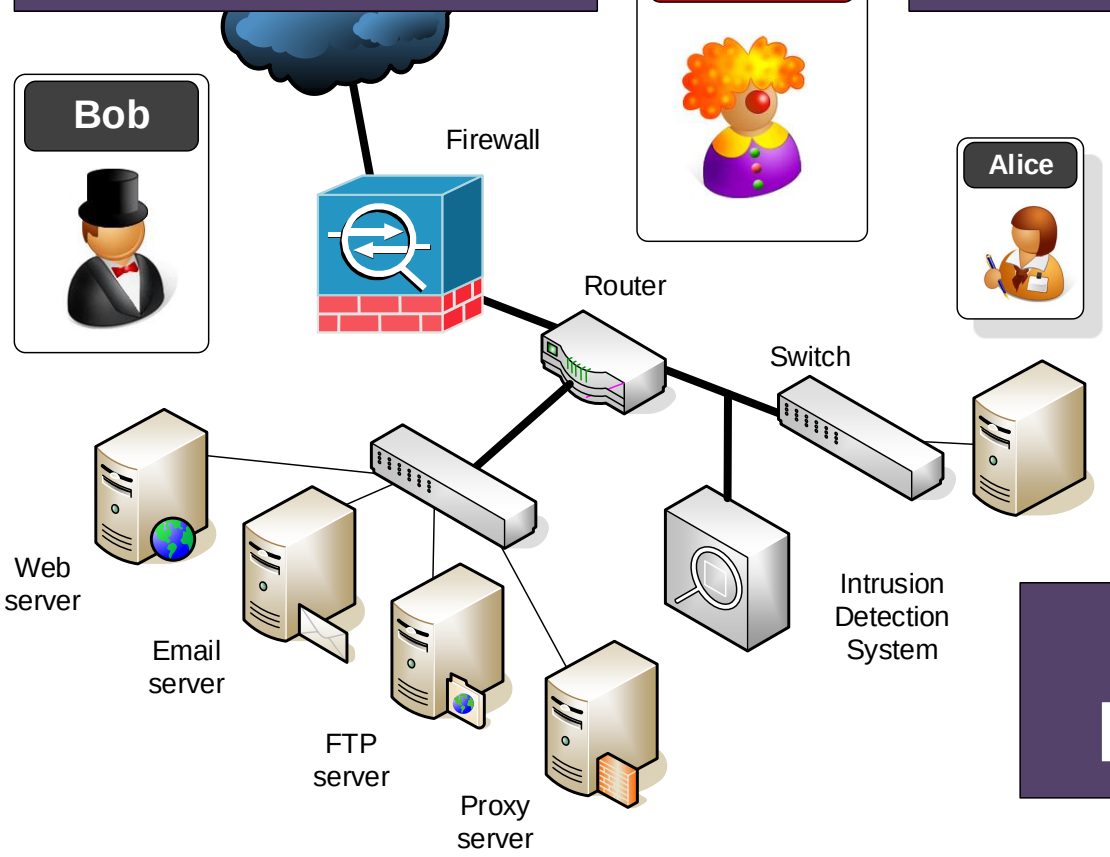
Data At Rest	Files, Directories, File Rights, Domain Rights, etc.	File changes, File CRUD (Create, Delete, Update, Delete), Thumbprints
Data In-Motion	Network scanners, Intrusion Detection Systems, Firewall logs, etc	Network packet logs, Web logs, Security logs
Data In-Process	Processes, Threads, Memory, etc.	Security Log, Application Log, Registry, Domain Rights.

Author: Prof Bill Buchanan

V- Velocity [Speed of data generation]

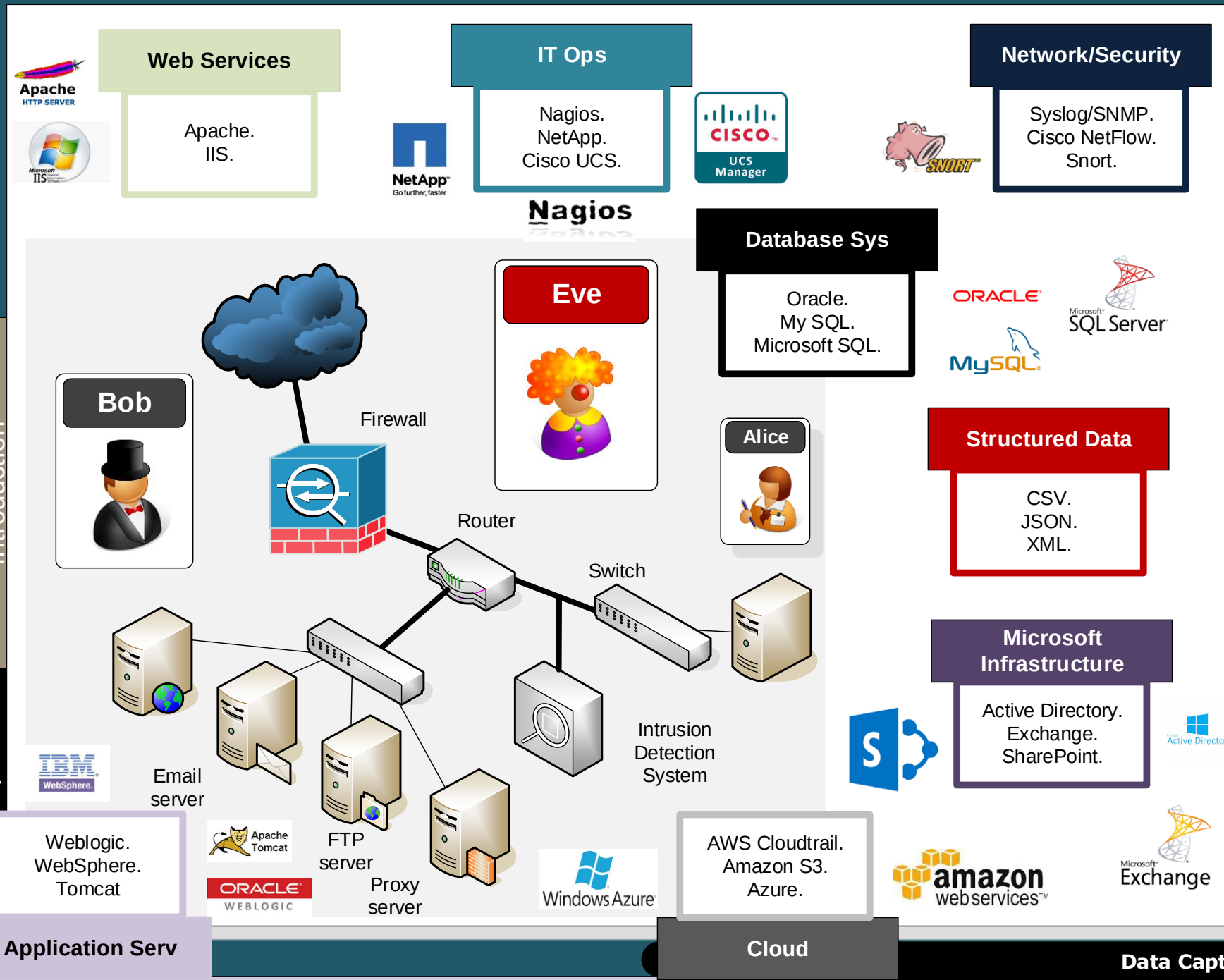
V- Veracity [Trustworthiness]

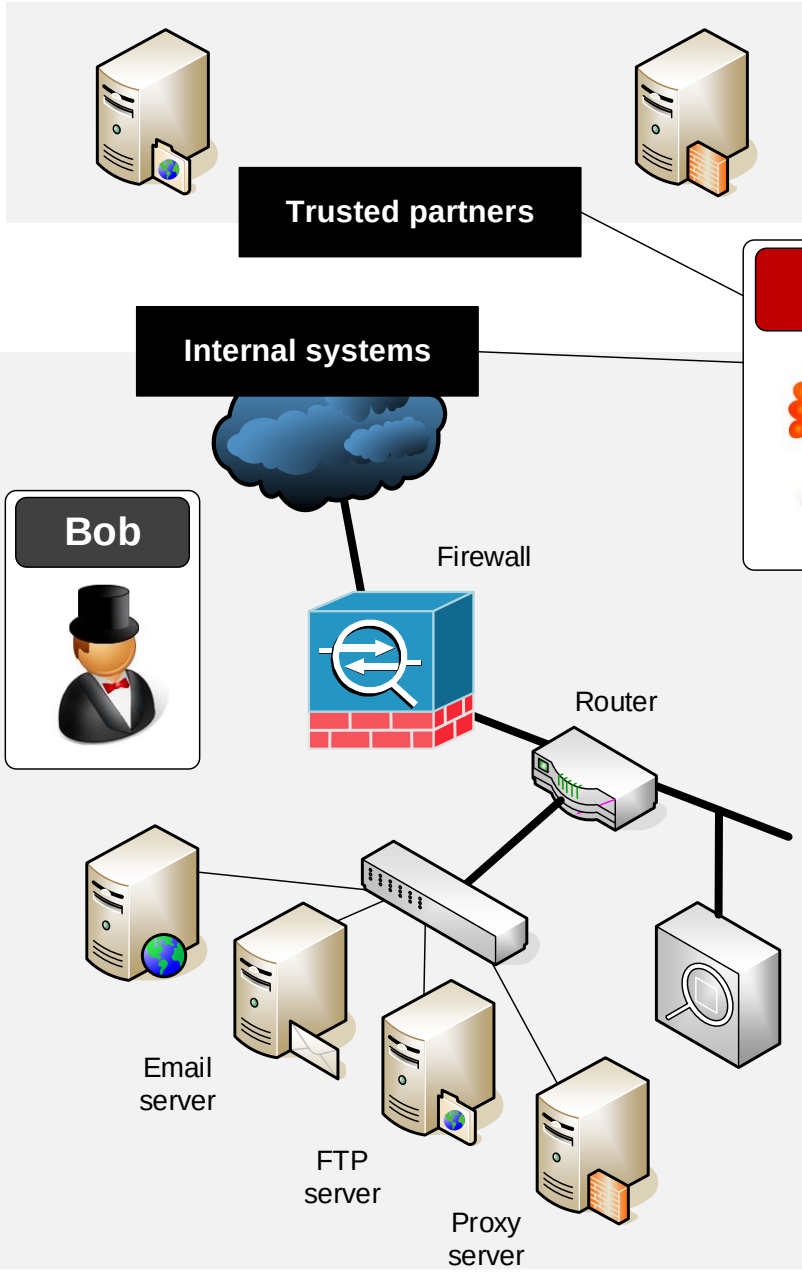
V- Variety [Different forms of data]

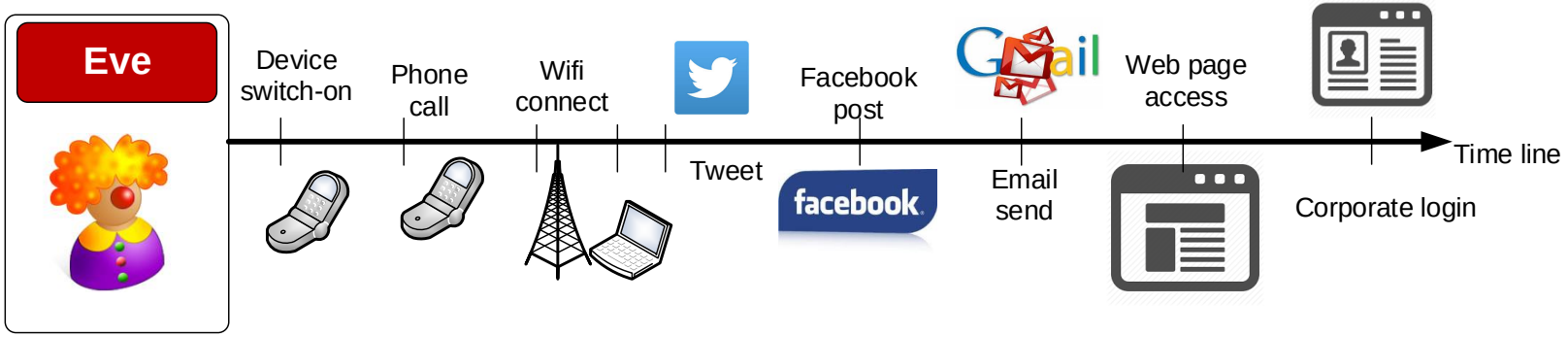


- Management report
- Sales analysis
- Targeted marketing
- Trending/Correlation
- Incident Response

V- Volume [Scale of data]


Web Services
Apache.
IIS.
IT Ops
Nagios.
NetApp.
Cisco UCS.
Network/Security
Syslog/SNMP.
Cisco NetFlow.
Snort.
Nagios
Database Sys
Oracle.
My SQL.
Microsoft SQL.
Eve
Bob
Alice
Firewall
Router
Switch
Structured Data
CSV.
JSON.
XML.
Microsoft Infrastructure
Active Directory.
Exchange.
SharePoint.
Intrusion Detection System
Email server
FTP server
Proxy server
Weblogic.
WebSphere.
Tomcat
AWS Cloudtrail.
Amazon S3.
Azure.
Introduction
Inc Response
Application Serv
Cloud
Data Capture


Trusted partners
Internal systems
Bob
Eve
Firewall
Router
Email server
FTP server
Proxy server
Cloud service providers
Communication service providers
Gmail
WhatsApp
facebook
LinkedIn
Windows Live
Dropbox
WordPress
Pinterest
myspace
foursquare
BT
Virgin media
vodafone
sky



Cloud service providers

Logs/Email

Communication service providers

Call record

Location record

Web log

Web services

Web/Domain Log

Device logs

System Log

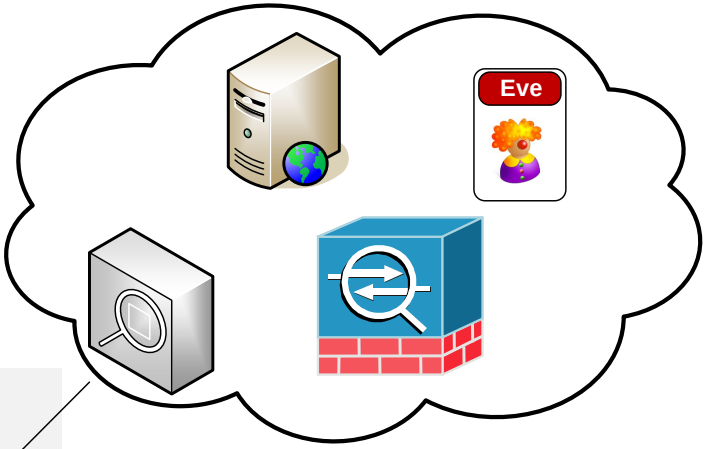
Internet cache

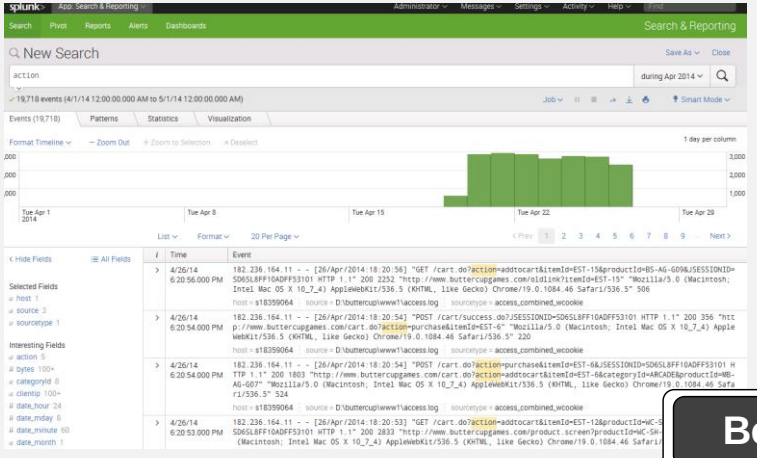
Basic timeline

Introduction

Inc Response

Eve





SIEM Package (Splunk)

Logs/alerts

BBC NEWS

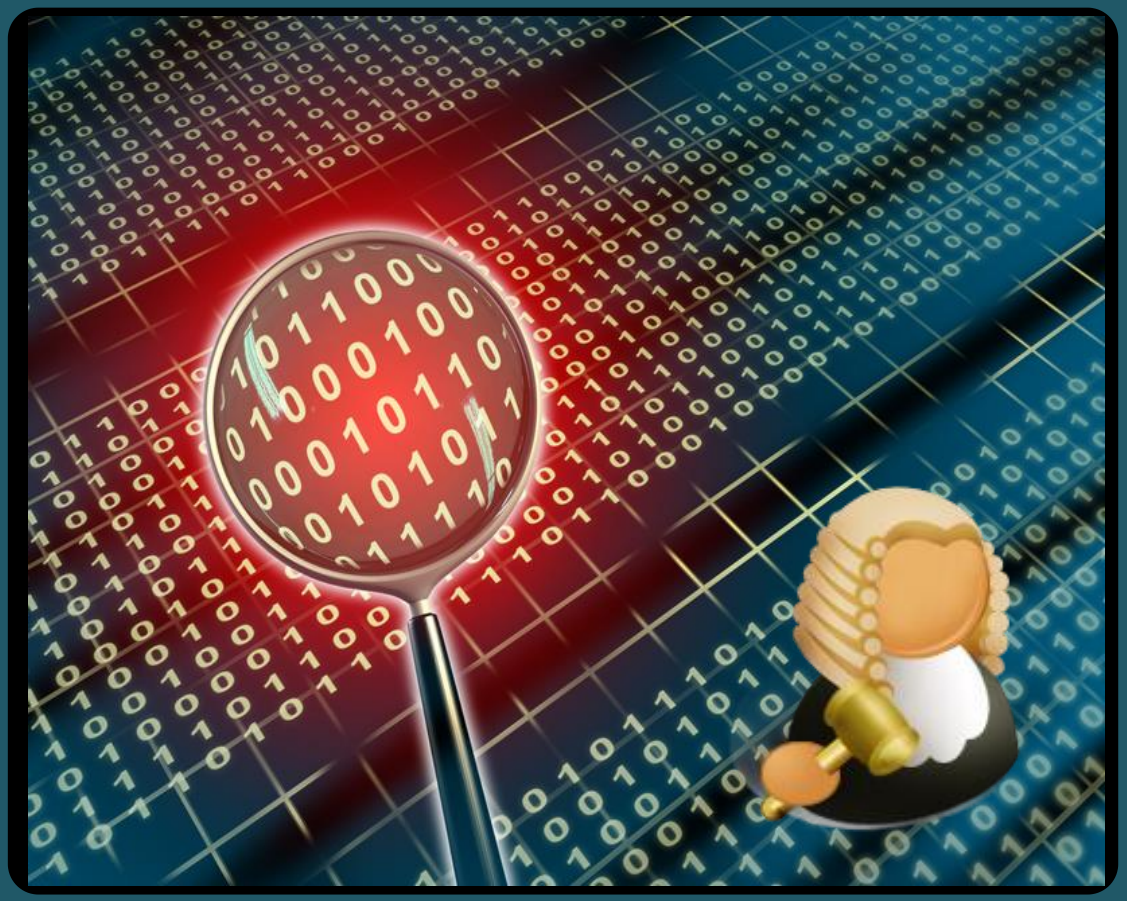
News feeds

Bob

Security alerts

Security Operations Centre

Incident Response



Patterns of Intrusion

Author: Prof Bill Buchanan

Intruder gains public information about the systems, such as DNS and IP information

Intruder gains more specific information such as subnet layout, and networked devices.

Outside reconnaissance

Inside reconnaissance

Intrusion Detection

Intrusion Detection

Intrusion Detection

Eve

From code yellow to code red ...

Exploit

Intruder finds a weakness, such as cracking a password, breaching a firewall, and so on.

Intrusion Detection

Foothold

Once into the system, the intruder can then advance up the privilege levels,

Intrusion Detection

Bob

Profit

Data stealing, system damage, user abuse, and so on.

Author: Prof Bill Buchanan

Typical pattern of intrusion …

Types

Inc Response

Preparation (hrs to mons)

Reconnaissance

Weaponization

Intrusion (minutes)

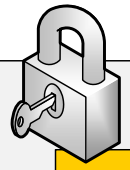
Delivery

Explotation

Installation

Eve

From code yellow to code red ...



Bob

Action on Objective

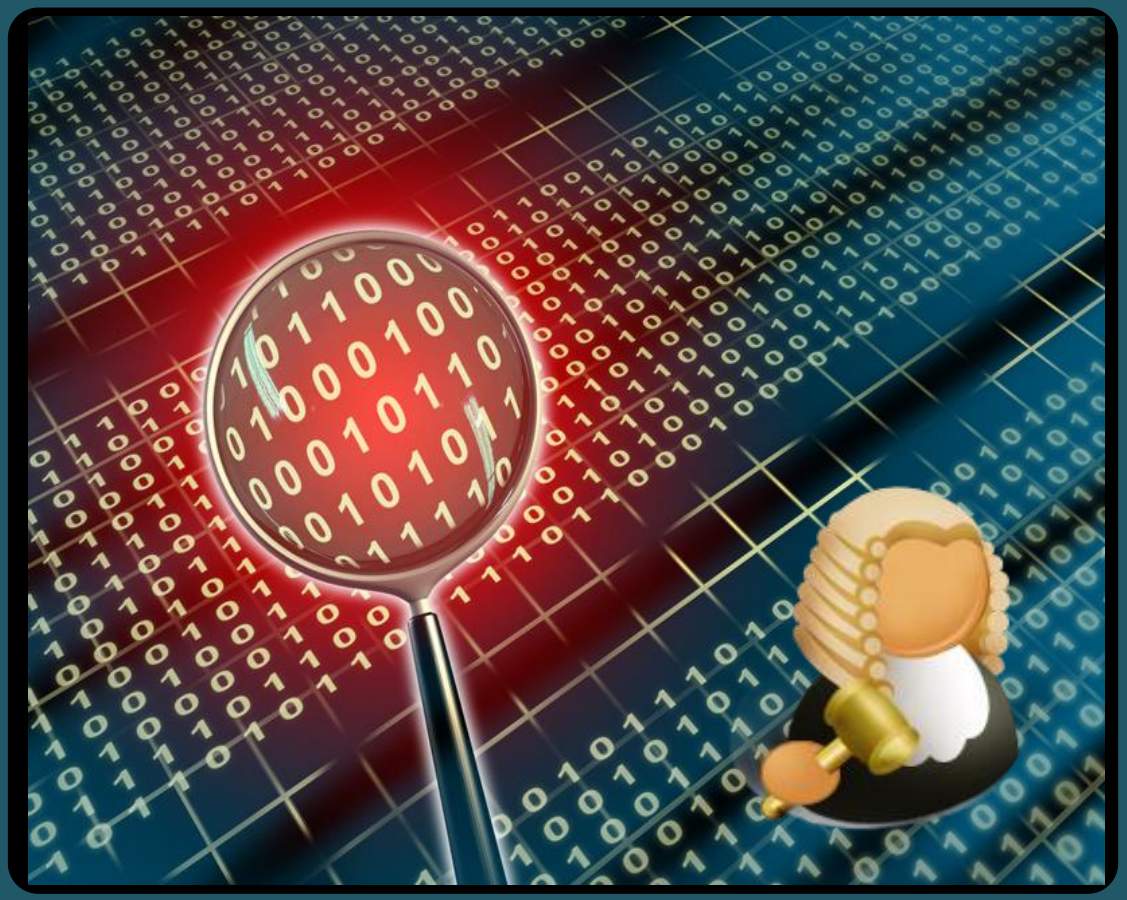
Command and Control

Active Breach (months)

Author: Prof Bill Buchanan

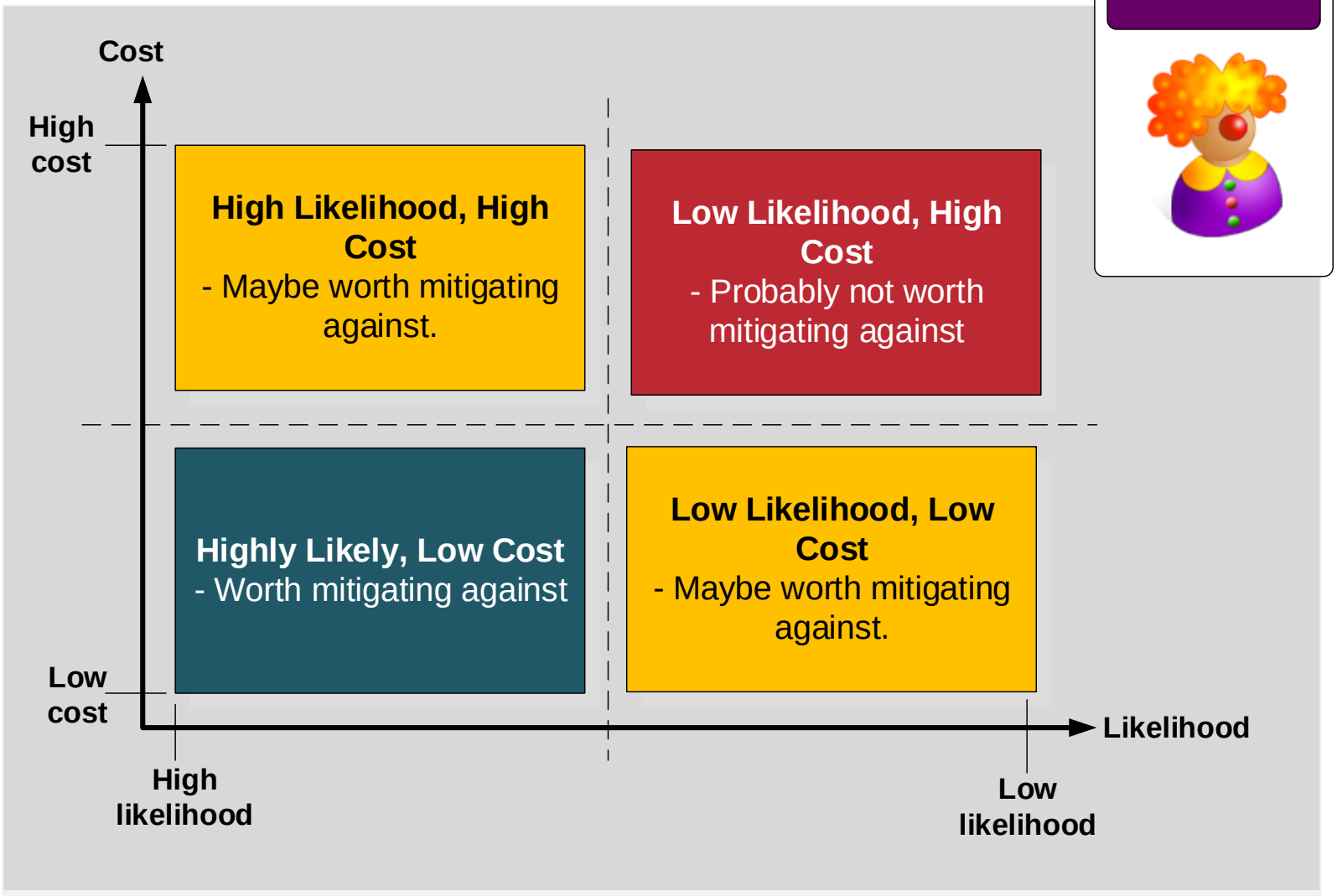
Cyber Kill Chain ®

Incident Response

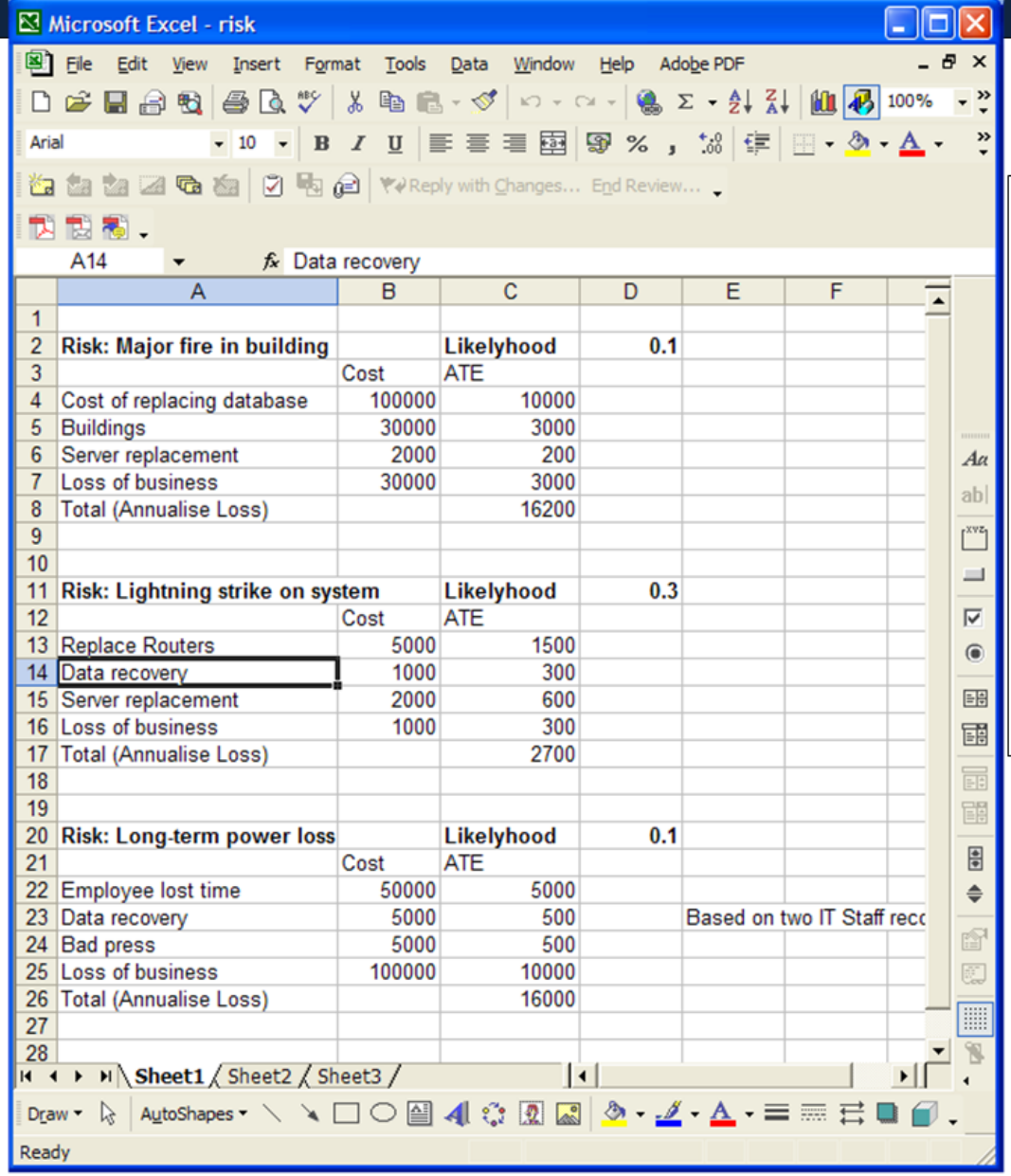


Risk Analysis

Author: Prof Bill Buchanan



Author: Prof Bill Buchanan



	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						

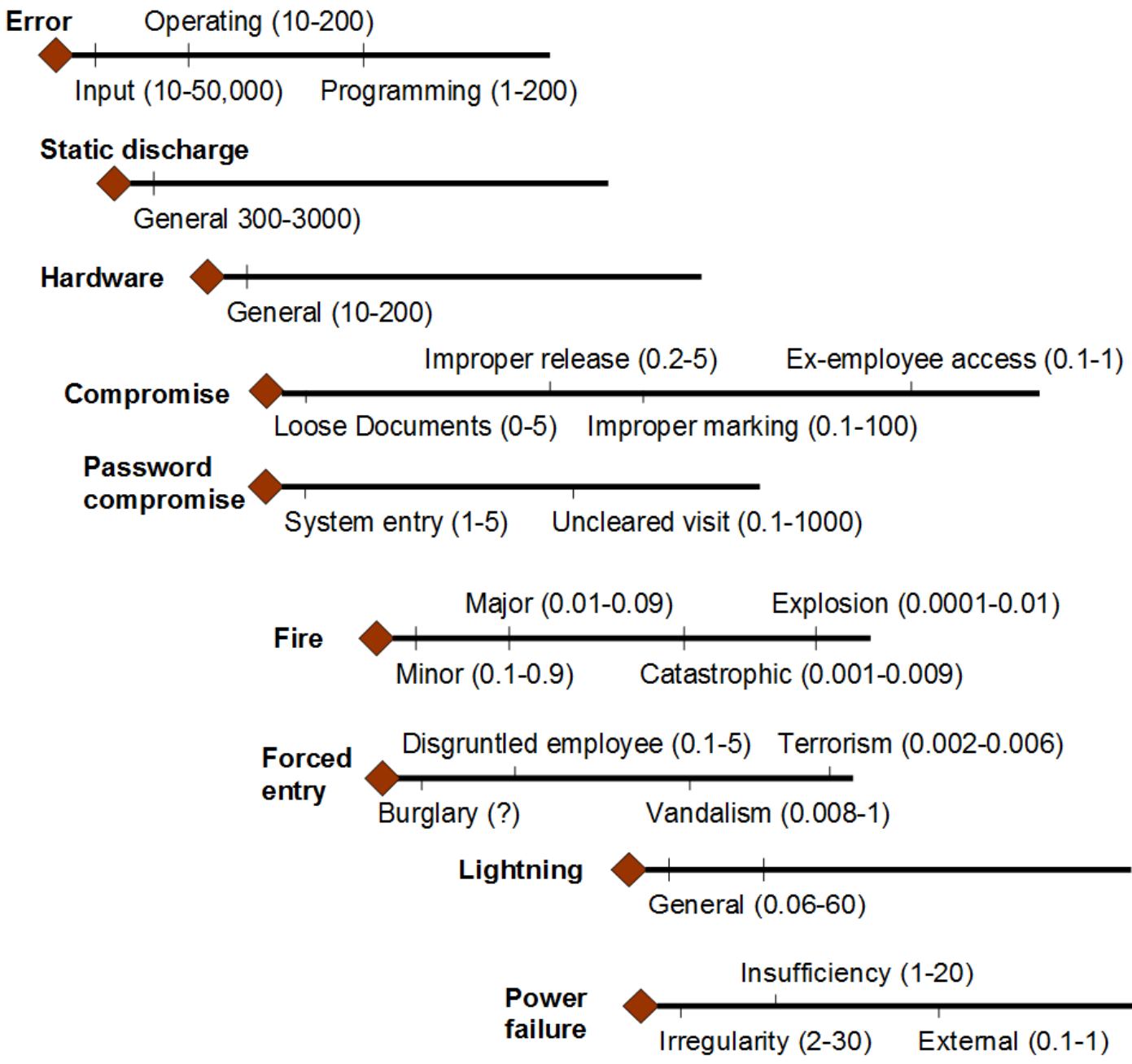
ALE = *T* x *V*

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:

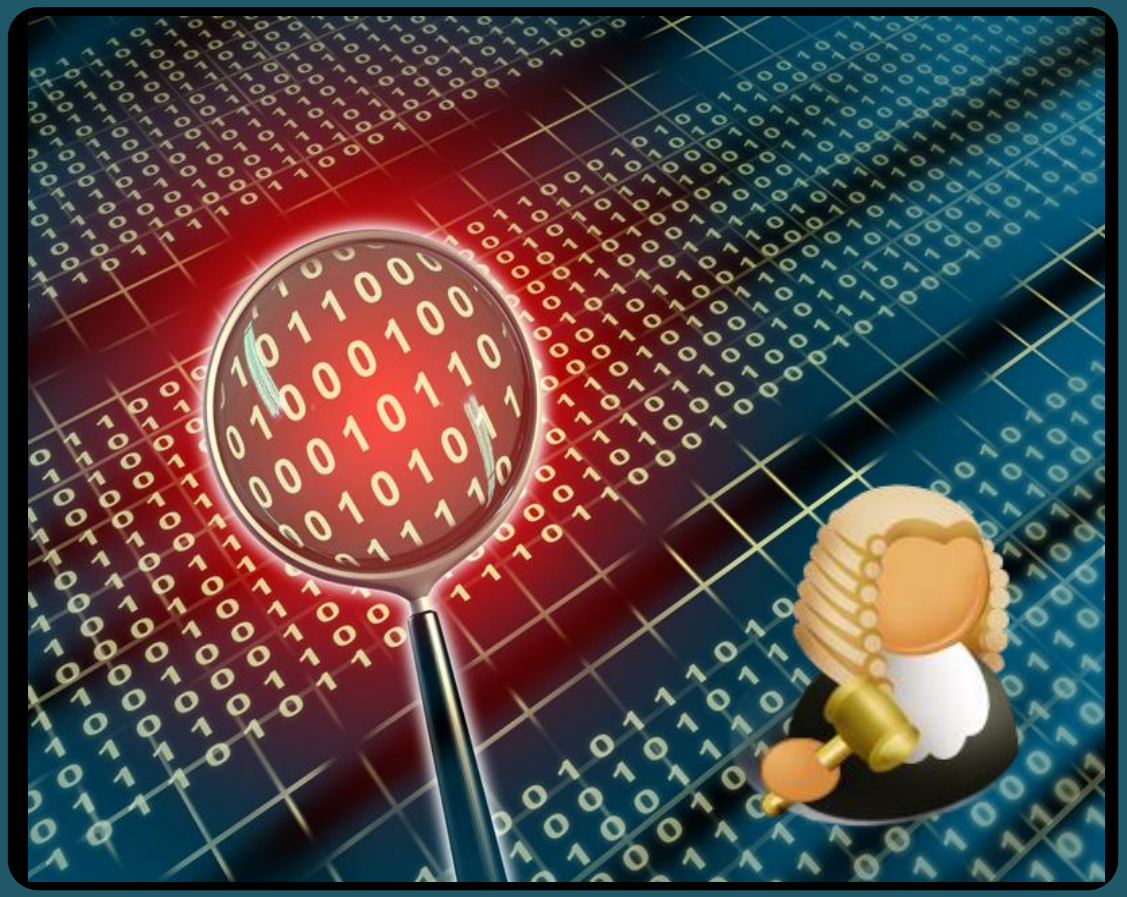
ALE = £100K x 1/3 = £33K per annum

Author: Prof Bill Buchanan



Author: Prof Bill Buchanan

Incident Response



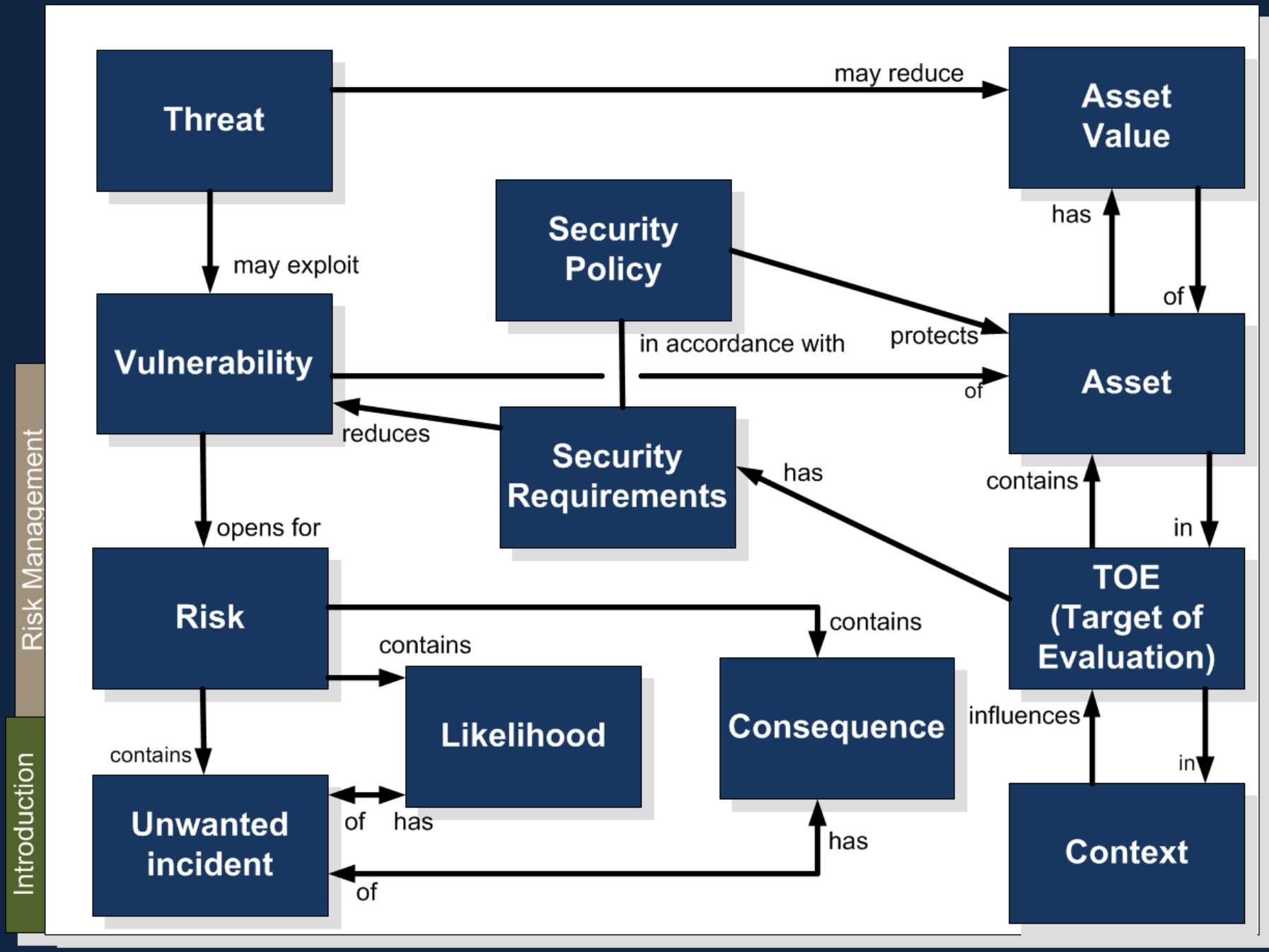
Risk Management

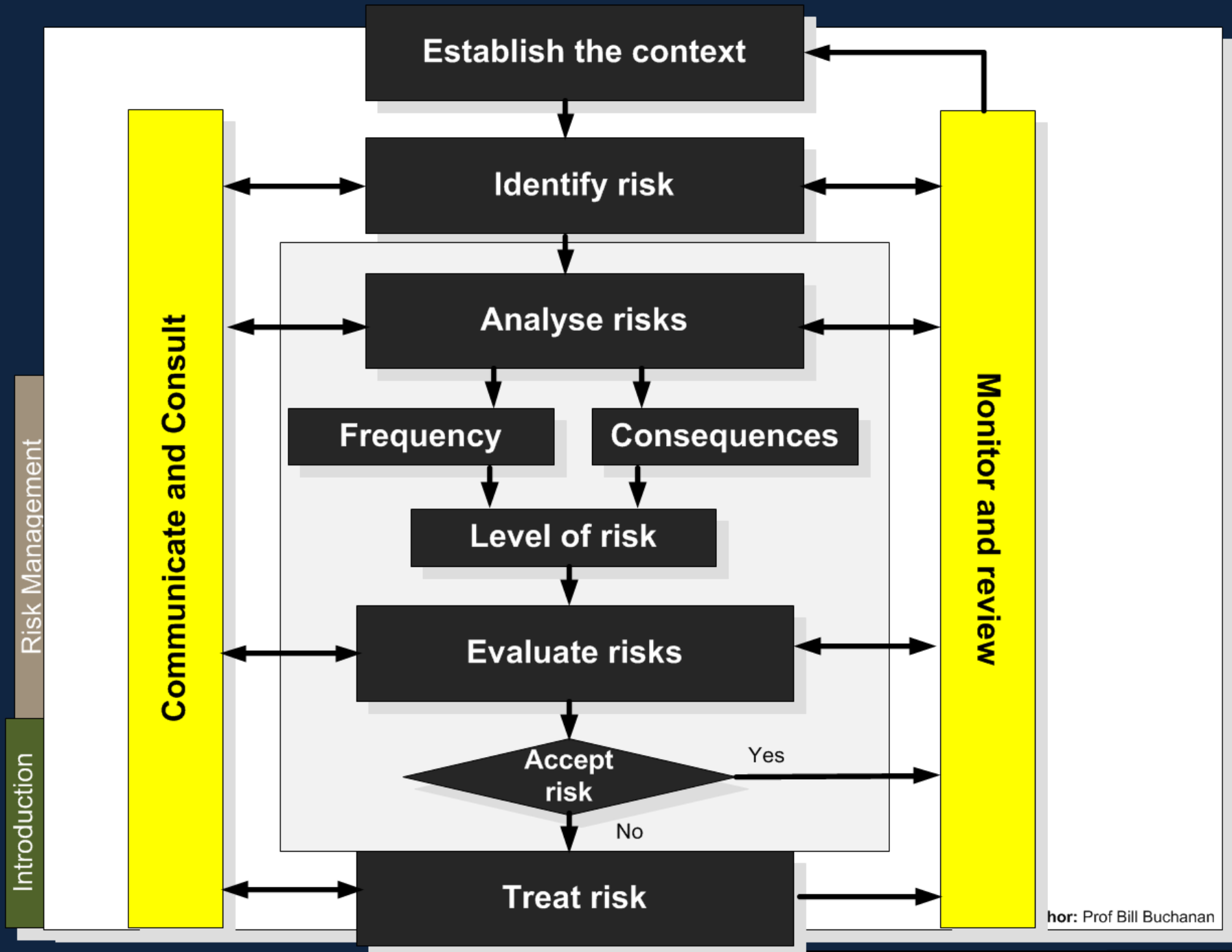
Author: Prof Bill Buchanan

Business context

Technical context

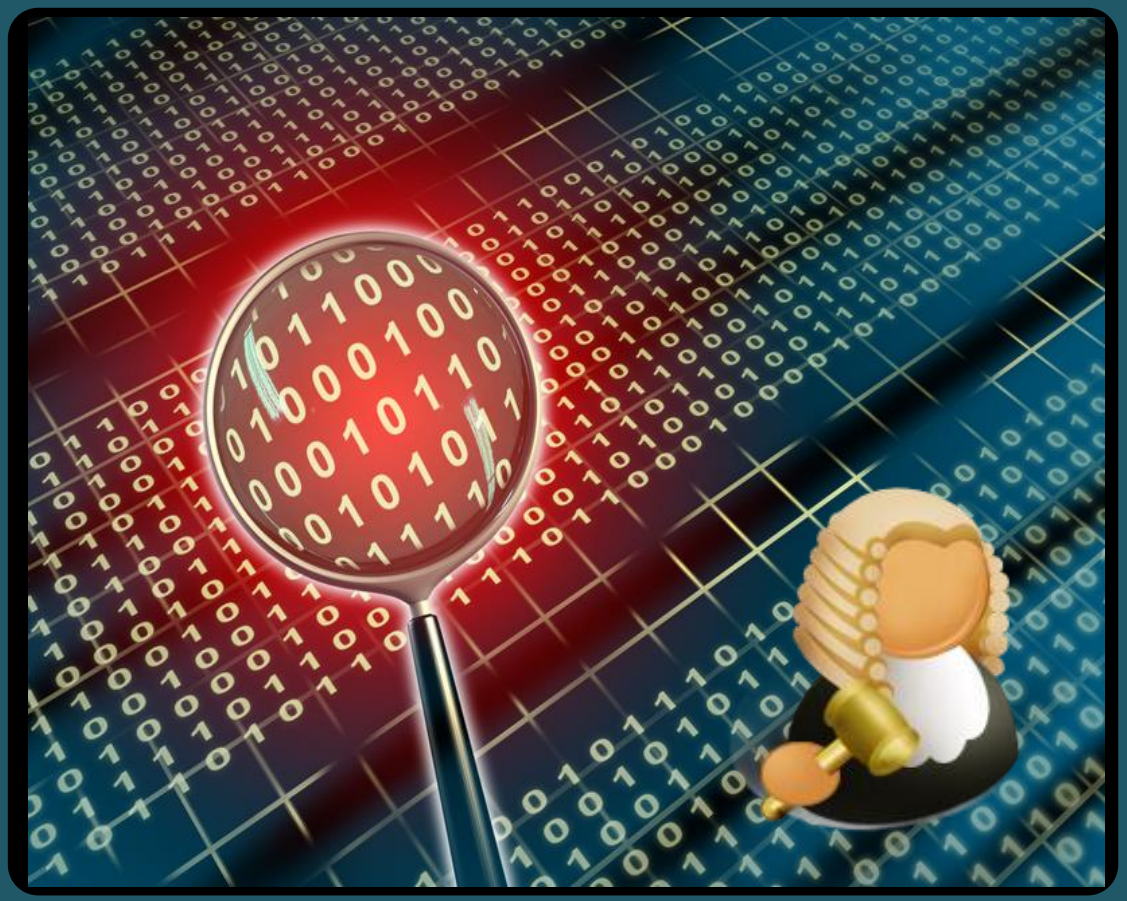
"Get two risk management experts in a room, one financial and the other IT, and they will NOT be able to discuss risk. Each puts risk into a different context … different vocabularies, definitions, metrics, processes and standards … "
Woloch (2006)


Threat
may reduce
Asset Value
Security Policy
has
may exploit
of
Vulnerability
in accordance with
protects
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 Management
Introduction
CORAS ontology



CORAS risk management

Incident Response

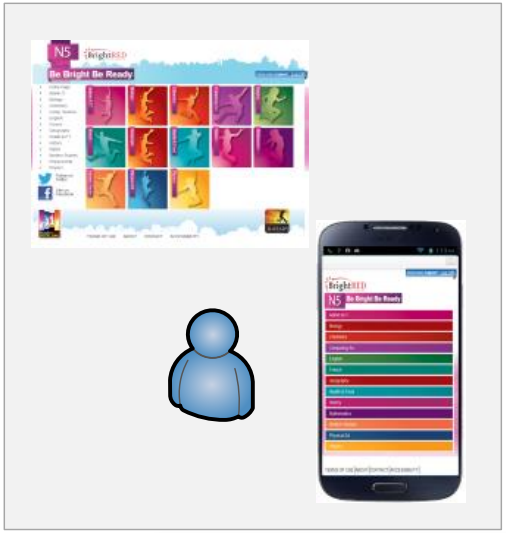


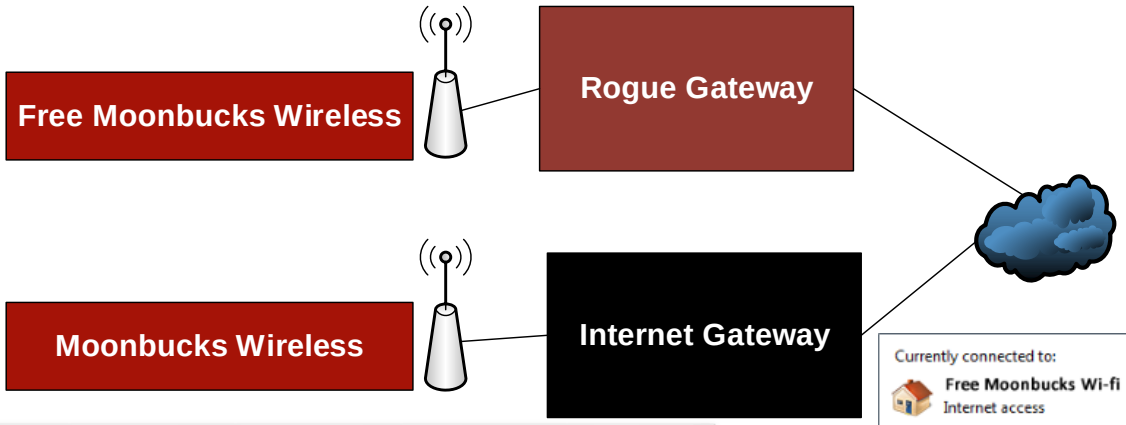
Some Threats

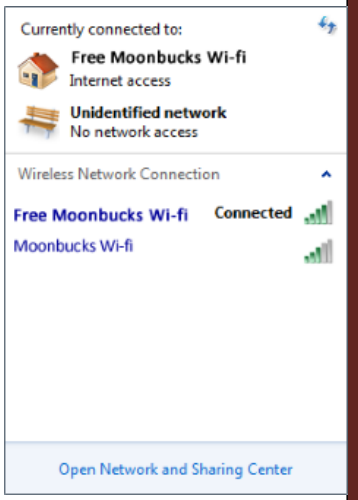
Author: Prof Bill Buchanan

Risk 2: Rogue SSID/Gateway

Edinburgh Napier UNIVERSITY



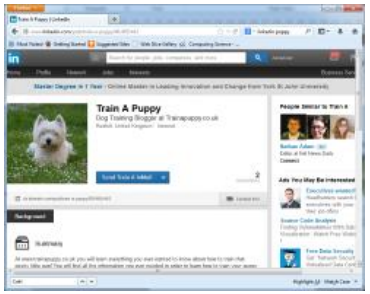




Risk 3: Lack of Separation

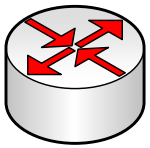
Edinburgh Napier UNIVERSITY

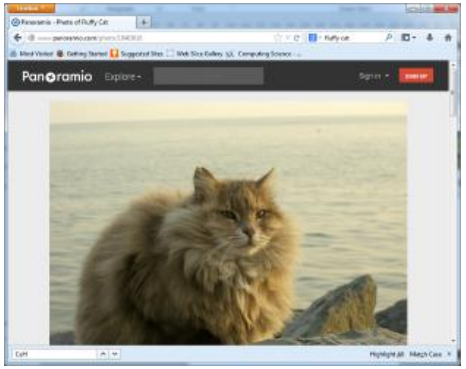
Business Life



Home Life

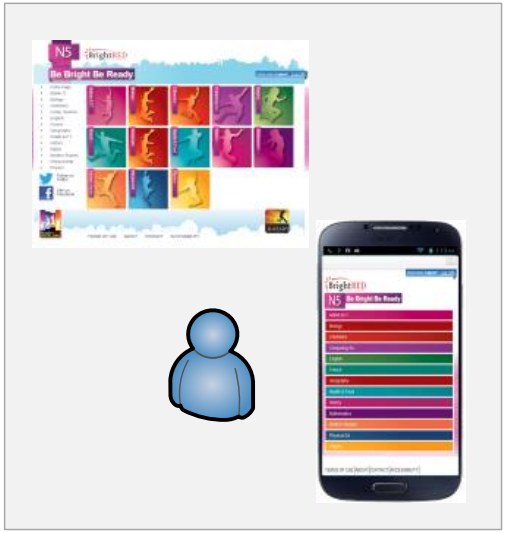
Corporate Firewall





Risk 4: One Password Fits All

Edinburgh Napier UNIVERSITY



Adobe

150 million accounts compromised

#	Count	Ciphertext	Plaintext
1.	1911938	EQ7fIpT7i/Q=	123456
2.	446162	j9p+HwtWWT86aMjgZFLzYg==	123456789
3.	345834	L8qbAD3jl3jioxG6CatHBw==	password
4.	211659	BB4e6X+b2xLioxG6CatHBw==	adobe123
5.	201580	j9p+HwtWWT/ioxG6CatHBw==	12345678
6.	130832	5djv7ZCI2ws=	qwerty
7.	124253	dQi0asWPYvQ=	1234567
8.	113884	7LqYzKVeq8I=	111111
9.	83411	PMDTbP0LZxu03SwrFUvYGA==	photoshop
10.	82694	e6MPXQ5G6a8=	123123

TJ-maxx Marshalls

47 million accounts

LinkedIn

6.5 million accounts (June 2013)

Windows Live

One account hack … leads to others

1 million accounts – in plain text. 77 million compromised

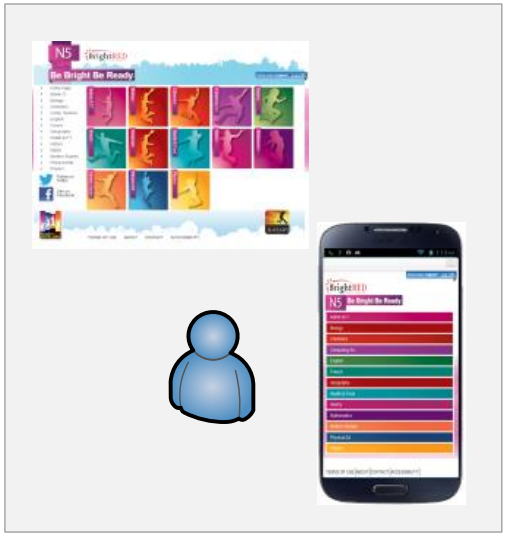
Dropbox compromised 2013

citigroup

200,000 client accounts

Risk 4: One Password Fits All

Edinburgh Napier UNIVERSITY

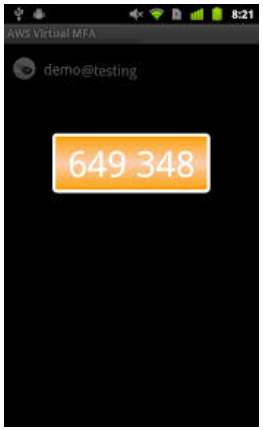


Adobe

150 million accounts compromised

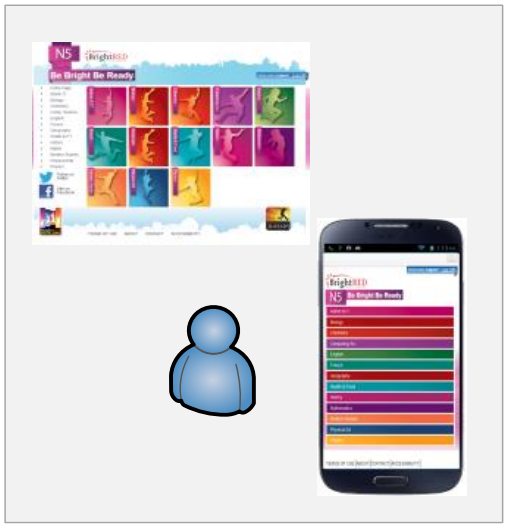
#	Count	Ciphertext	Plaintext
1.	1911938	EQ7fIpT7i/Q=	123456
2.	446162	j9p+HwtWWT86aMjgZFLzYg==	123456789
3.	345834	L8qbAD3jl3jioxG6CatHBw==	password
4.	211659	BB4e6X+b2xLioxG6CatHBw==	adobe123
5.	201580	j9p+HwtWWT/ioxG6CatHBw==	12345678
6.	130832	5djv7ZCI2ws=	qwerty
7.	124253	dQi0asWPYvQ=	1234567
8.	113884	7LqYzKVeq8I=	111111
9.	83411	PMDTbP0LZxu03SwrFUvYGA==	photoshop
10.	82694	e6MPXQ5G6a8=	123123

Two-factor everything in the Cloud

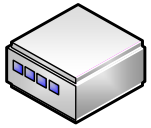


Risk 5: Device Poisoning

Edinburgh Napier UNIVERSITY



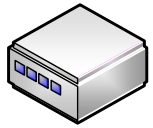
Who has this IP address (192.168.0.1)?



ARP Poisoning

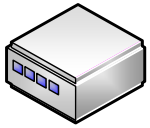
Here is my MAC address (11:22:33:44:55:66)

Gateway (192.168.0.1)



Here is my MAC address (22:33:44:55:66)

DHCP Request ...



Here is your IP address, Gateway, and DNS IP

DNS Poisoning

1 0.000000 0.0.0.0 255.255.255.255 DHCP 314 DHCP Discover - Transaction ID 0x3d1d
Frame 1: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits)
Ethernet II, Src: Grandstr_01:fc:42 (00:0b:82:01:fc:42), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)

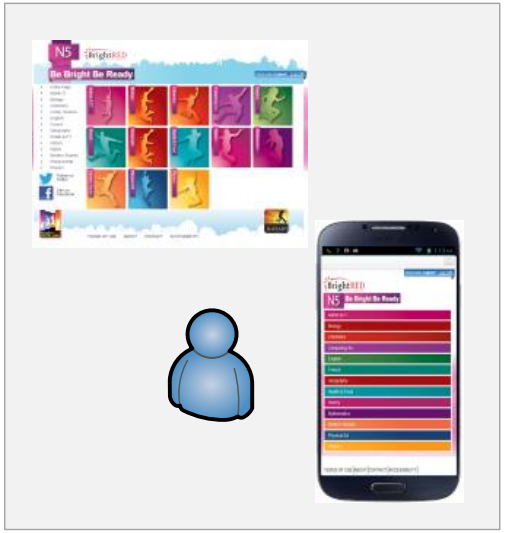
2 0.000295 192.168.0.1 192.168.0.10 DHCP 342 DHCP Offer - Transaction ID 0x3d1d
Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: DellComp_ad:f1:9b (00:08:74:ad:f1:9b), Dst: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.10 (192.168.0.10)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)

3 0.070031 0.0.0.0 255.255.255.255 DHCP 314 DHCP Request - Transaction ID 0x3d1e
Frame 3: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits)
Ethernet II, Src: Grandstr_01:fc:42 (00:0b:82:01:fc:42), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)

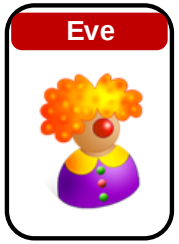
4 0.070345 192.168.0.1 192.168.0.10 DHCP 342 DHCP ACK - Transaction ID 0x3d1e
Frame 4: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: DellComp_ad:f1:9b (00:08:74:ad:f1:9b), Dst: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.10 (192.168.0.10)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)

Risk 6: Unpatched Systems

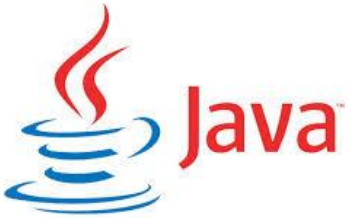
Edinburgh Napier UNIVERSITY



CVE-2007-0071
Adobe Flash Player.
Integer overflow



Phoenix Exploit Kit



CVE-2013-5331
Adobe Flash Player.
Run code on machine.

CVE-2013-1723
Java Exploit

CrimeBoss

http://asecuritysite.com/subjects/chapter14

Cyberterrorism. This can be attacks against critical national infrastructures, such as power plants, oil refineries, and so on,

Natural Disasters

Natural Disasters. This includes storms, hurricanes, fire, floods, earthquakes, and natural events

Cyberterror

Eavesdropping

Eavesdropping. This involves intercepting communications.

Logical scavenging

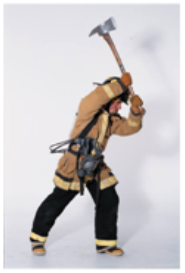
Logical scavenging. This involves scavenging through discarded media.

Author: Prof Bill Buchanan

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 actual physical attack on the hardware.
Physical removal. This involves the actual physical removal of hardware.

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.

Author: Prof Bill Buchanan

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

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

Best project ever!
Click here

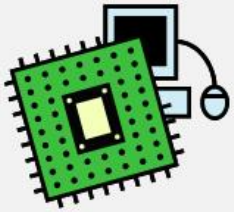
Trojan horse

Logic bombs

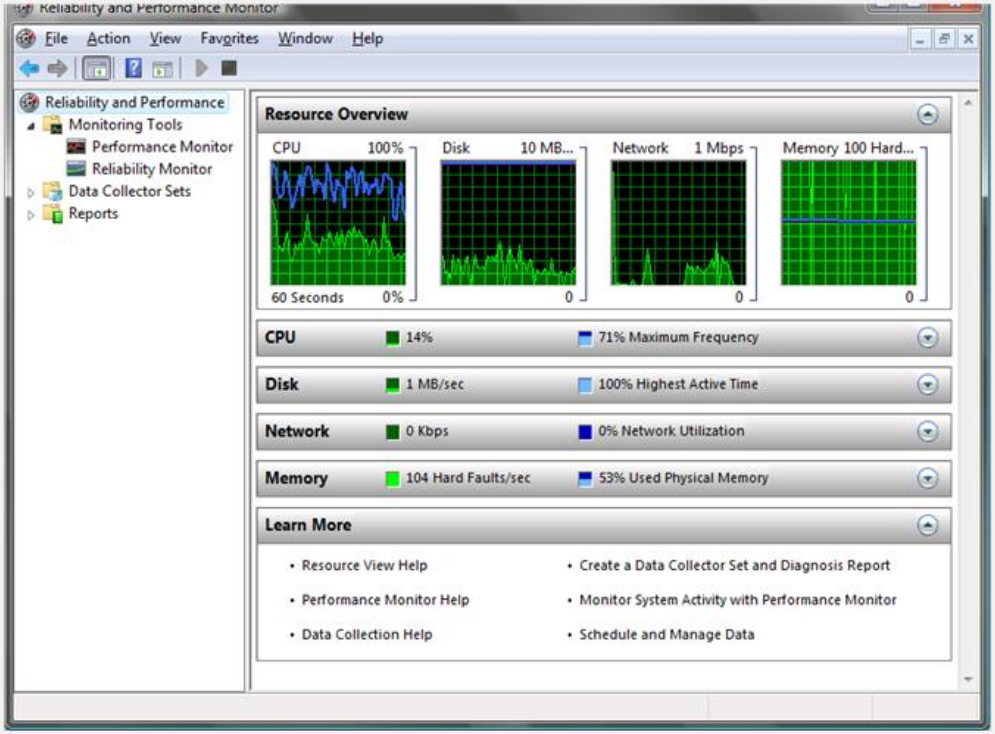
The email contains a Trojan virus

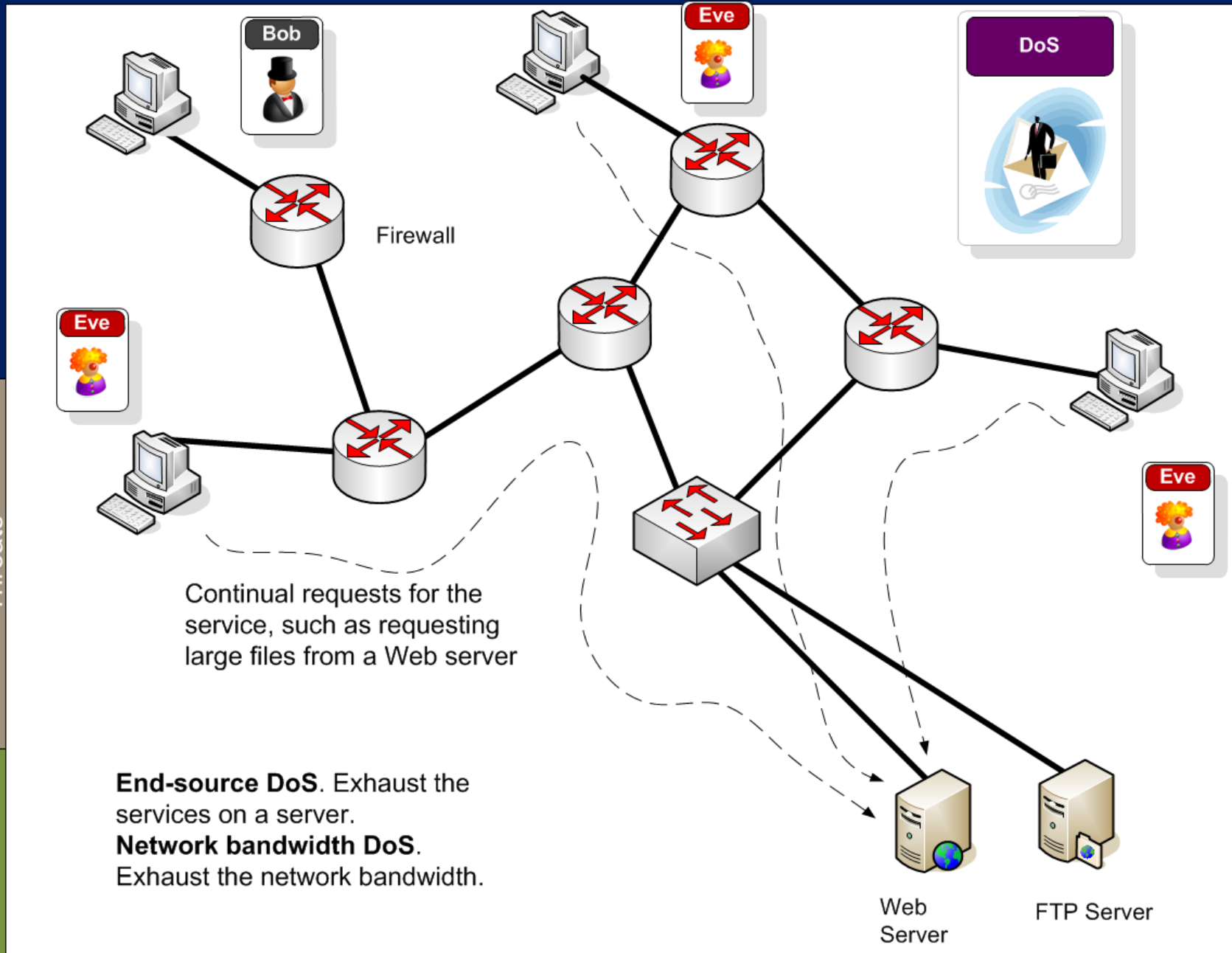
Author: Prof Bill Buchanan

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. This involves attaching program which self replicate themselves.



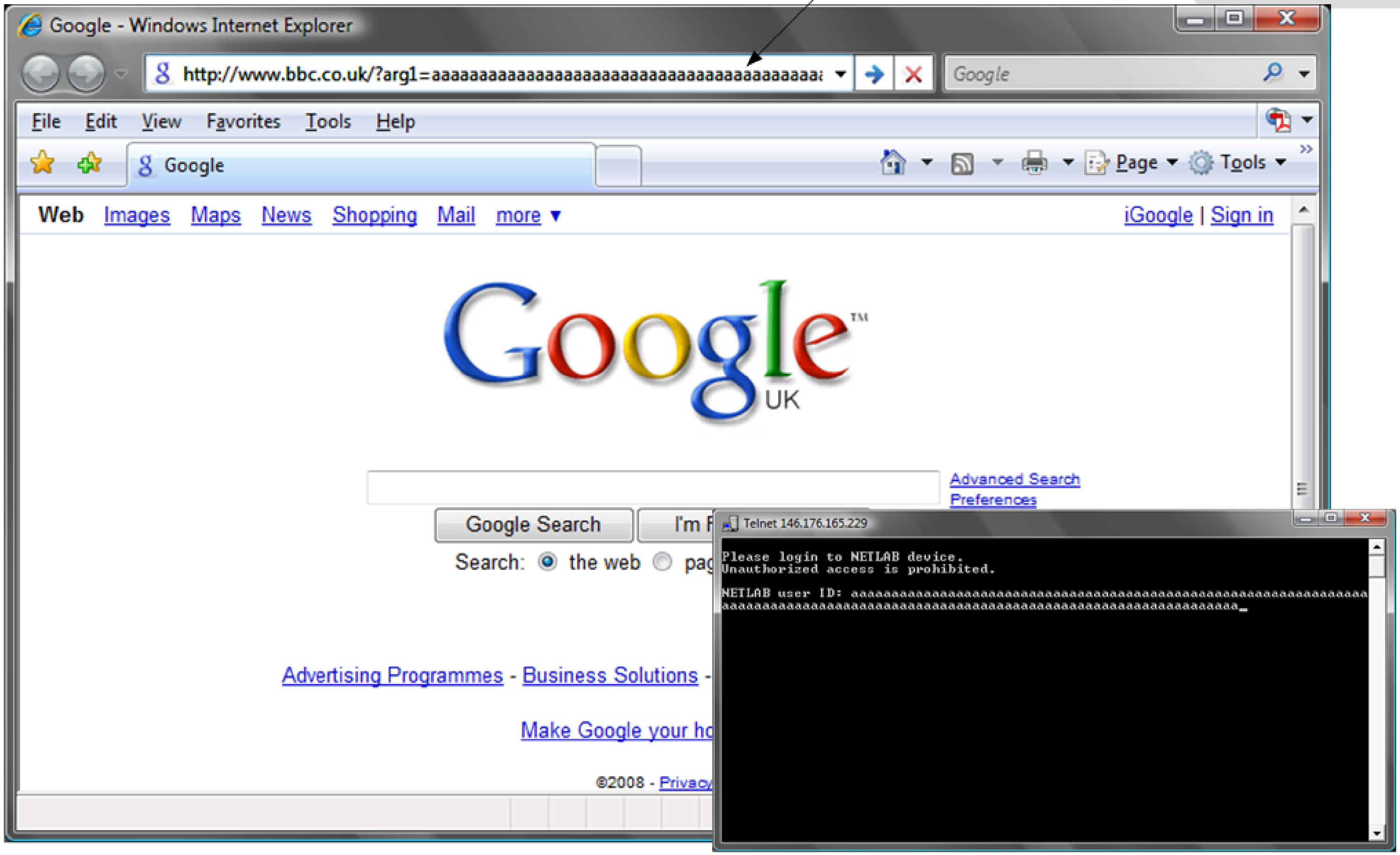


End-source DoS. Exhaust the services on a server.
Network bandwidth DoS. Exhaust the network bandwidth.

Author: Prof Bill Buchanan

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



Active attack

Author: Prof Bill Buchanan

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).

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

Author: Prof Bill Buchanan

Spoofing. This involves the spoofing of devices.

Spoofing

Bob

Hello… I'm Bob!

Hello… I'm Bob!

Eve

Hello… I'm Bob!

Hello… I'm Bob!

Im-personation

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

I'm a nuclear scientist

I'm a brain surgeon

Author: Prof Bill Buchanan

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.

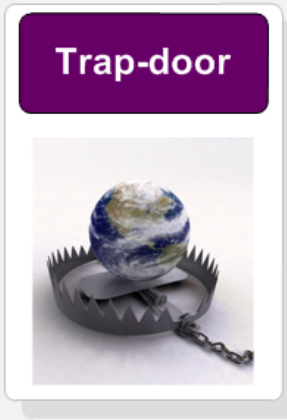
Hello…

Hello… Goodbye

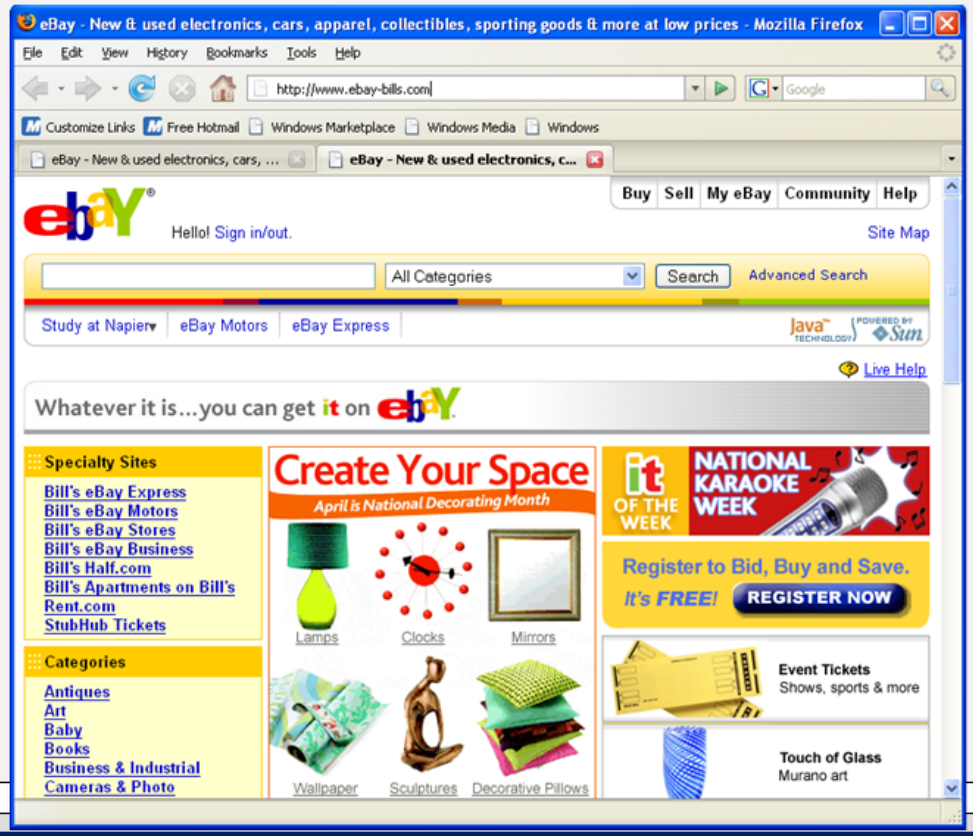
A virus has piggybacked onto an email

Author: Prof Bill Buchanan

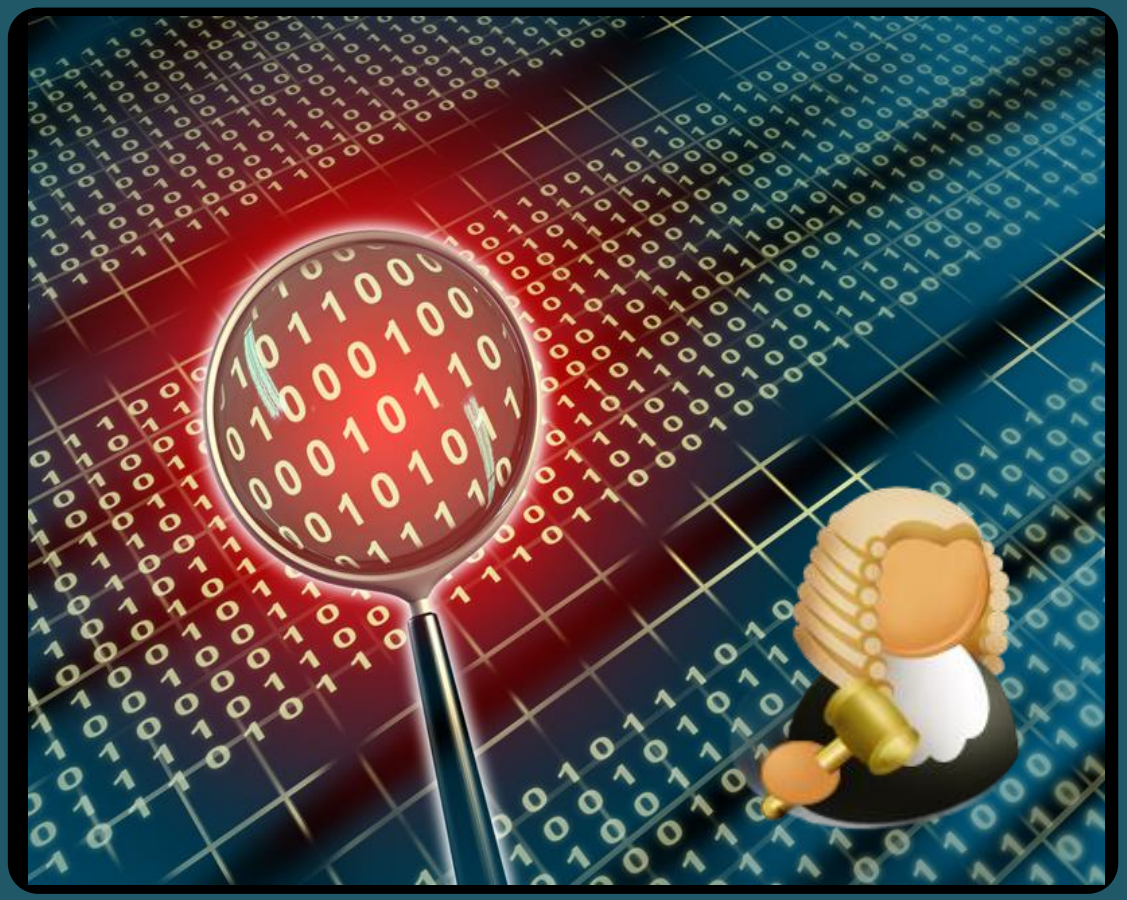
Authorization attacks. This involves trying to gain access to a higher level of authorization than is valid for the user, such as with password attacks.



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.

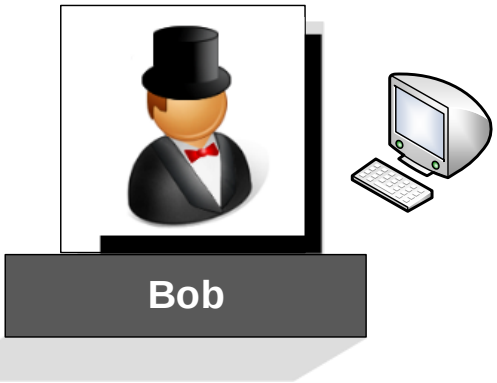


Incident Response



A Few Fundamentals

Author: Prof Bill Buchanan



13610163252

Octal

Hex

5e 20 e6 aa

Base-64

XiDmqg==

'A' 'B' 'C' 'D'

ASCII characters

01000001 01000010
01000011 01000100

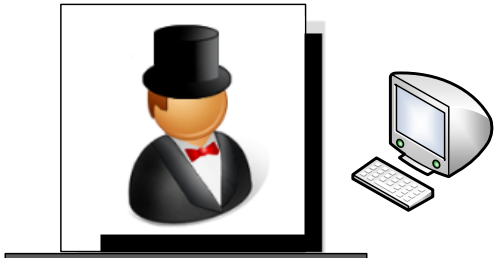
Byte values

Encryption/
Encoding

01011110 00100000
11100110 10101010

^ æª

ASCII



Decimal	Binary	Oct
0	000	0
1	001	1
2	010	2
3	011	3
4	100	4
5	101	5
6	110	6
7	111	7

Bit stream

0101 1110 0010 0000 1110 0110 1010 1010

Hex

5 e 2 0 e 6 a a

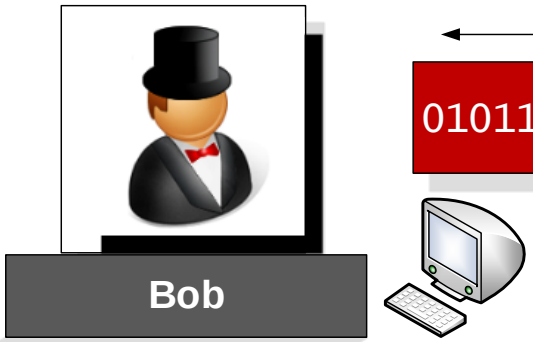
What is 0100111011110001?

Decimal	Binary	Hex
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

0101 1110 0010 0000 1110 0110 1010 1010

24-bit width

010111 100010 000011 100110 101010 100000 = =



Bit stream

010111 100010 000011 100110 101010 100000

X I D m q g = =

Base-64

Val	Enc	Val	Enc	Val	Enc	Val	Enc
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

abc	24 bits	(4*6)	YWJj
abcd	32 bits	(5*6) + (2+4) + 12 bits	YWJjZA==
abcde	40 bits	(8*6) + (2+4) + 4 bits	YWJjZGU=

hello

MD5 5D41402ABC4B2A76B9719D911017C592

128 bits (32 hex characters)

SHA-1 AAF4C61DDCC5E8A2DABEDE0F3B482CD9AEA9434D

160 bits (40 hex characters)

SHA-256 SHA-384 SHA-512

```
$ cat hello.txt
Hello
$ openssl md5 hello.txt
MD5(c:\hello.txt)=
5d41402abc4b2a76b9719d911017c592

$ echo -n "hello" | openssl md5
     (stdin)= 5d41402abc4b2a76b9719d911017c592
```

[character_group]	Match any single character in character_group Example: gr[ae]y – gray, grey
[^character_group]	Match any single character in character_group Example: gr[^ae]y – grby, grcy
[a-z]	Character range Example a, b, c … z
{n}	Matches previous character repeated n times
a{n,m}	Matches between n and m or a
\d	Matches a digit
.	Single character
(a | b)	Matches a or b
a?	Zero or one match of a
a*	Zero or more match of a
a+	One or more match of a
$	Match at the end
Escape:	\s (space)

Telephone: \\d{3}[-.]?\\d{3}[-.]?\\d{4}

444.444.2312

Year: [0-9]{4}

1961

test@home.com

Email: [a-zA-Z0-9._%+-]+@[a-zA-Z0-9._%+-]

5555-1234-3456-4312

```
Master:    5\\d{3}(\\s|-)?\\d{4}(\\s|-)?\\d{4}(\\s|-)?\d{4}
Am Ex:     3\\d{3}(\\s|-)?\\d{6}(\\s|-)?\\d{5}
Visa:      4\\d{3}(\\s|-)?\\d{4}(\\s|-)?\\d{4}(\\s|-)?\d{4}
```

1.2.3.4

IP: [0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}.[0-9]{1,3}

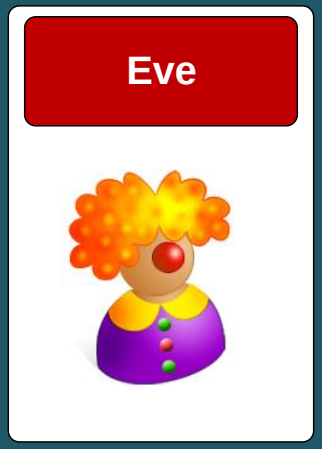
Data Formats

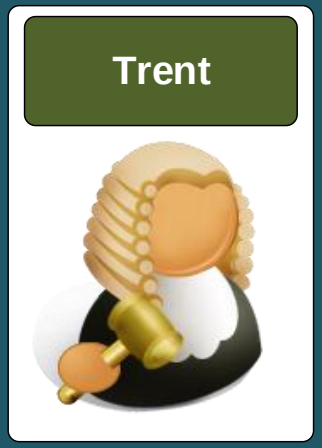
DLP

RegEx

Incident Response

- Introduction.
- Risk Analysis.
- Risk Management.
- Outline of threats.
- Data Loss.
- Fundamentals.





Author: Prof Bill Buchanan