What does this represent?

am U ity

HØGSKOLEN
I ÅLESUND
Aalesund University College

Information Asset Management

Is IT important?

Adrian Seccombe
November 2011

www.cs.surrey.ac.uk

Thanks to those who will engage!

Over the last few years I have found…

…those that engage, succeed!

So what DOES this represent?

amUity

Framing: Why is IAM key?

- Information as Assets
  - Information is at the heart of all human endeavours, it has value based on a number of key attributes, we will explore those attributes and your role in protecting them.

Classification, an Early Glimpse

Amber: Sensitive	Red: Highly Sensitive
Green : Internal Use	White : Public

Aalesund
University
College

Classification, a reminder.

Amber: Sensitive
I will rarely, if ever share such information with you, I will flag when I do.

Red: Highly Sensitive
I will never share this type of information with you.

Green : Internal Use
A good proportion of the information we will discuss

White : Public
The majority of the information we will discuss

My Aim

- To give you a BRIEF view of Information Asset Management (IAM) techniques
  - an understanding of the impact, positive and negative, of the right and wrong use of Information Technology
  - ability to consider the implications of the changing use of Information Technology.
  - practise application of some of the IAM techniques and think about how you might apply others

There are two kinds of people…

- …in the world, those who agree there are two kinds of people and those who don’t!

  Robert Benchley, Benchley's Law of Distinction

  US actor, author, & humorist (1889 – 1945)

- It turns out to be a little more complicated though!!

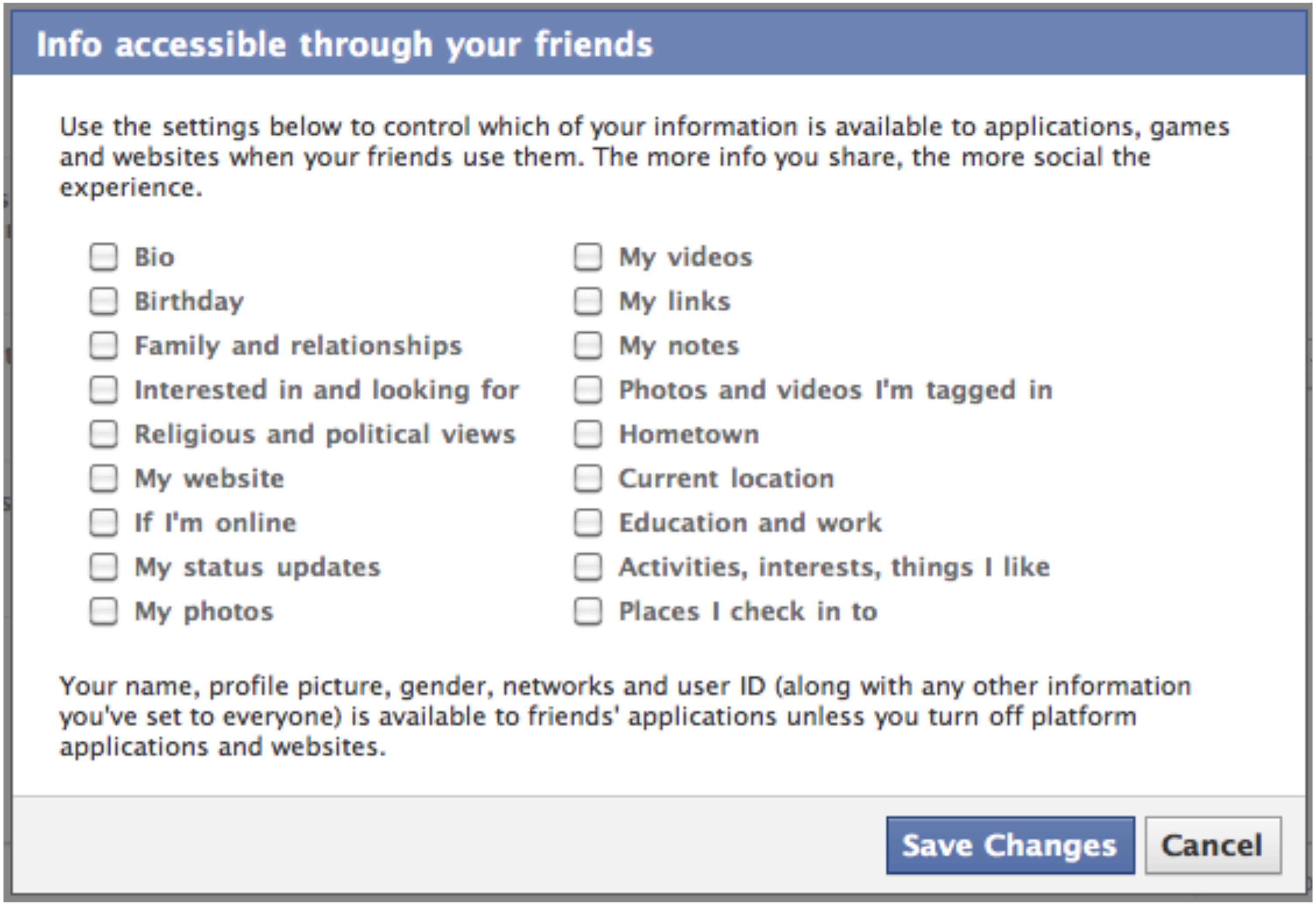
What is your FaceBook stance?

- Public, share Friends publicly
- Public, protect Friends
- Visible, Private, share Friends publicly
- Visible, Private, protect Friends
- Invisible

- Which do you think is best?
- Which do you think is worst?

What are your settings here?

Aalesund University College



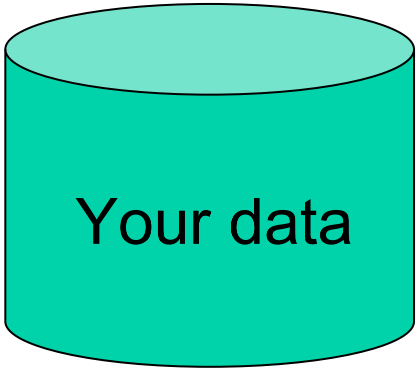
Info accessible through your friends

Use the settings below to control which of your information is available to applications, games and websites when your friends use them. The more info you share, the more social the experience.

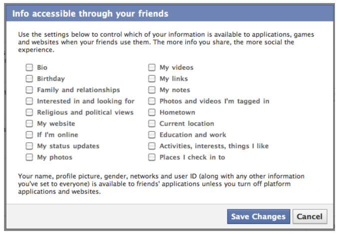
- □ Bio
- □ Birthday
- □ Family and relationships
- □ Interested in and looking for
- □ Religious and political views
- □ My website
- □ If I'm online
- □ My status updates
- □ My photos
- □ My videos
- □ My links
- □ My notes
- □ Photos and videos I'm tagged in
- □ Hometown
- □ Current location
- □ Education and work
- □ Activities, interests, things I like
- □ Places I check in to

Your name, profile picture, gender, networks and user ID (along with any other information you've set to everyone) is available to friends' applications unless you turn off platform applications and websites.

Why does it matter?



Filter

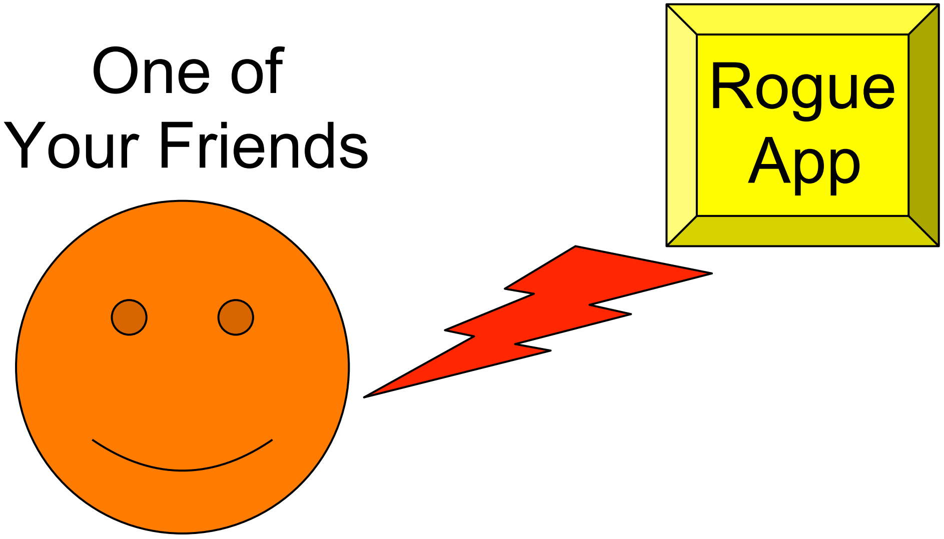


Info accessible through your friends

Use the settings below to control which of your information is available to applications, games and websites when your friends use them. The more info you share, the more social the experience.

- □ Bio
- □ Birthday
- □ Family and relationships
- □ Interested in and looking for
- □ Religious and political views
- □ My website
- □ If I'm online
- □ My status updates
- □ My photos
- □ My videos
- □ My links
- □ My notes
- □ Photos and videos I'm tagged in
- □ Hometown
- □ Current location
- □ Education and work
- □ Activities, interests, things I like
- □ Places I check in to

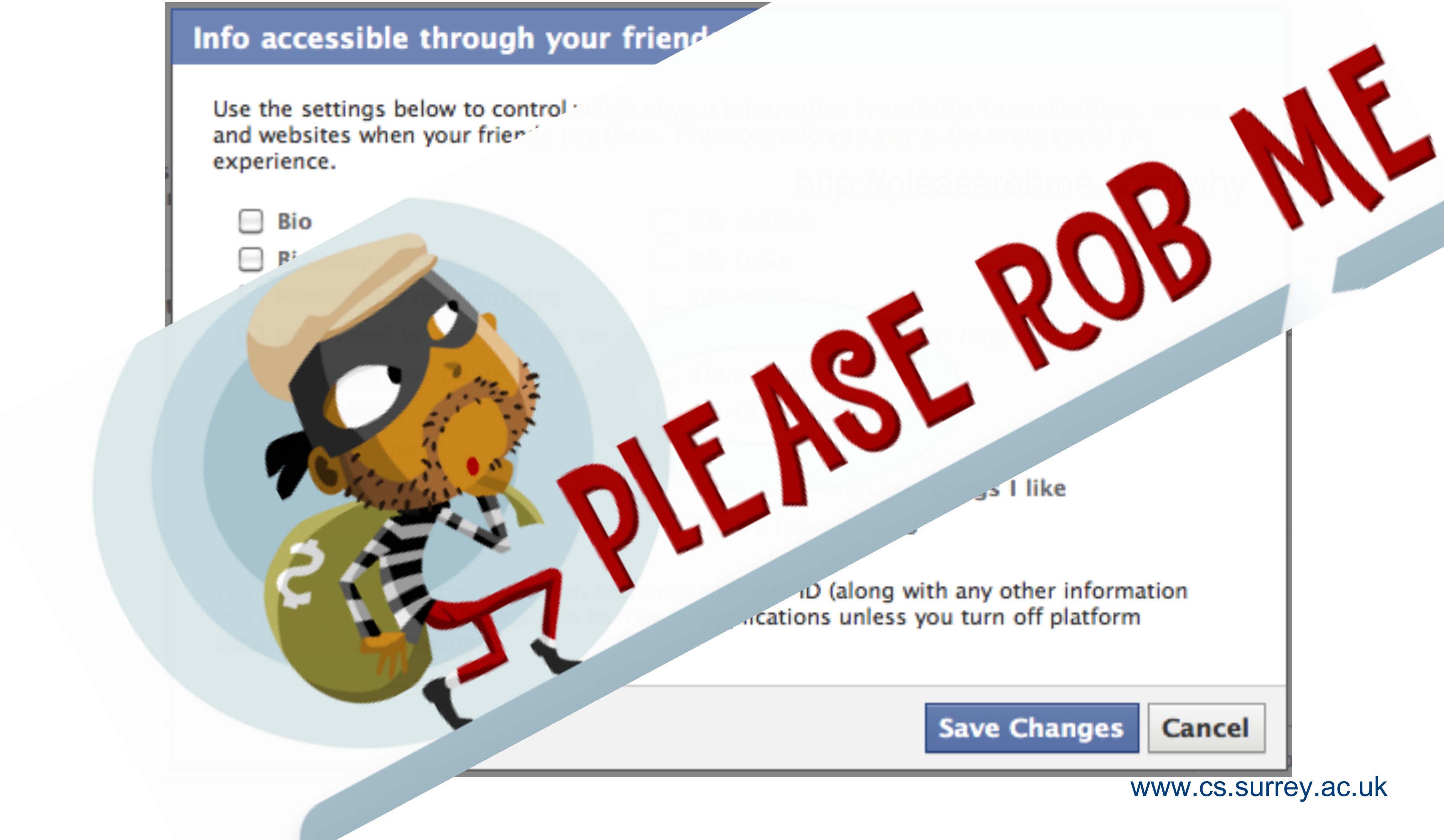
Your name, profile picture, gender, networks and user ID (along with any other information you've set to everyone) is available to friends' applications unless you turn off platform applications and websites.



How will you know its gone?

Which friend signed up for what Rogue App?

What are your settings here?



Info accessible through your friend

Use the settings below to control which of your information is available to applications, games and websites when your friends use them. The more info you share, the more social the experience.

□ Bio

□ Bi

□ My videos

□ My links

□ My notes

gs I like

ID (along with any other information

ications unless you turn off platform

Exercise One
What is your FaceBook stance?

- Public, share Friends publicly
- Public, protect Friends
- Visible, Private, share Friends publicly
- Visible, Private, protect Friends
- Invisible
- Not on FaceBook
- Don’t Remember

Exercise One
What is your FaceBook stance?

Each Group to present back to the room

- The different stances in your group
- Which you think are best
- Which you think are worst
- The potential impacts of the stances
- Actions your group proposes to protect the folks inside and outside of the room

Facebook Policy Extract

- “When you use Facebook, certain information you post or share with third parties (e.g., a friend or someone in your network), such as personal information, comments, messages, photos, videos, Marketplace listings or other information, may be shared with other users in accordance with the privacy settings you select. All such sharing of information is done at your own risk. Please keep in mind that if you disclose personal information in your profile or when posting comments, messages, photos, videos, Marketplace listings or other items , this information may become publicly available.”

Source: http://www.facebook.com/home.php?ref=logo#/policy.php?ref=pf

Aalesund University College

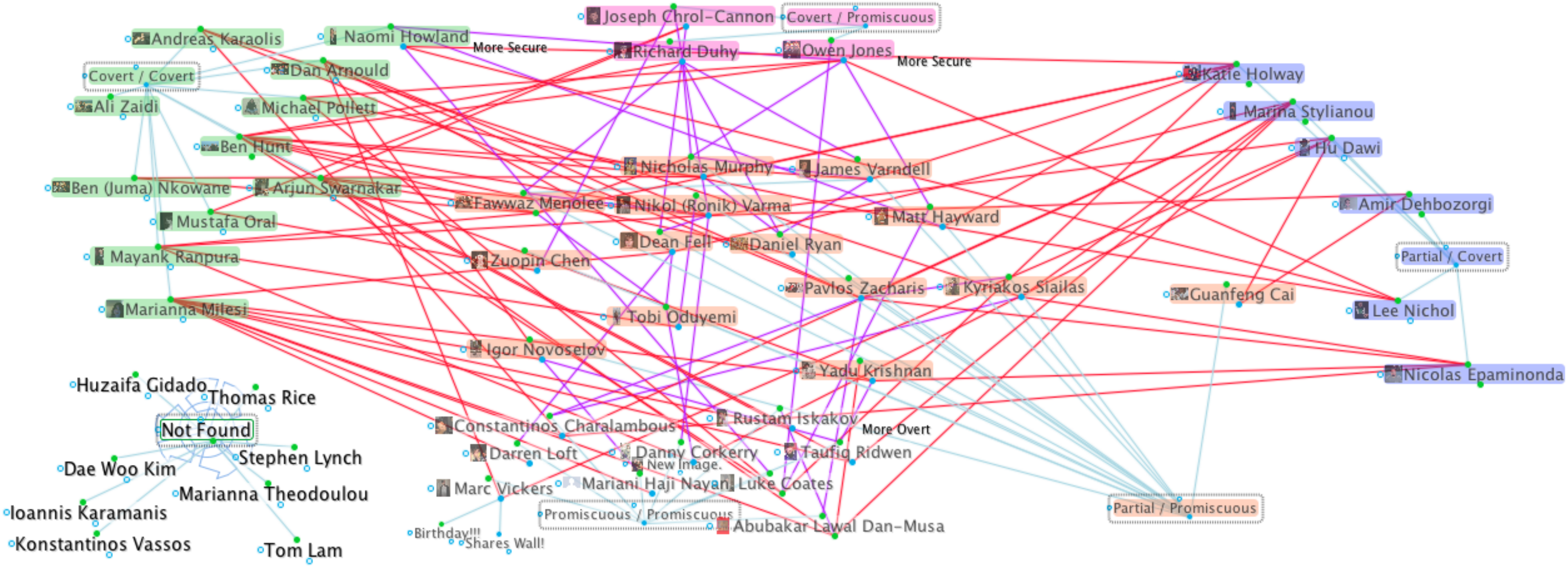
A message…

- You can find a useful video in the link below…
- http://chris.pirillo.com/do-you-have-any-social-networking-advice-for-students/
- My own son didn’t really listen
- Should I put the link here???

Source: live.pirillo.com

Aalesund
University
College

The state of play February 6th



This page will be made available on Ulearn as it represents your publically available stance

So the Key Learnings are…

- Behave Virtually as you would want to be actually seen or known …
  …in the “real” Physical world”.
- Look after the information of others as you would have them look after yours.

Framing: Why is IAM key?

- Information as Assets
  - Information is at the heart of all human endeavours, it has value based on a number of key attributes:
    - Privacy
    - Accuracy
    - Freshness
    - …

Exercise Two
Information Criteria

Each Group to

- Brainstorm a list of Information Attributes
- Group these Attributes into like sets
- Give Names to these sets
- Develop simple examples of the potential impact of failure to protect a set.
- Present sets and examples to the class.

Timing Develop: 15 Mins, Present: 15 Mins

COBIT Information Criteria

Effectiveness deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.

Efficiency concerns the provision of information through the optimal (most productive and economical) use of resources.

Confidentiality concerns the protection of sensitive information from unauthorised disclosure.

Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.

Availability relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

Compliance deals with complying with the laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria as well as internal policies.

Reliability relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities.

Information Risk

We will be discussing:

- Types of Information Risk
- Impacts of Information Risks
- Classification of Information Sensitivity
- Threats and Vulnerabilities
- Information Risk Mitigation and Controls

*Approximate values

Impacts of Information Risks

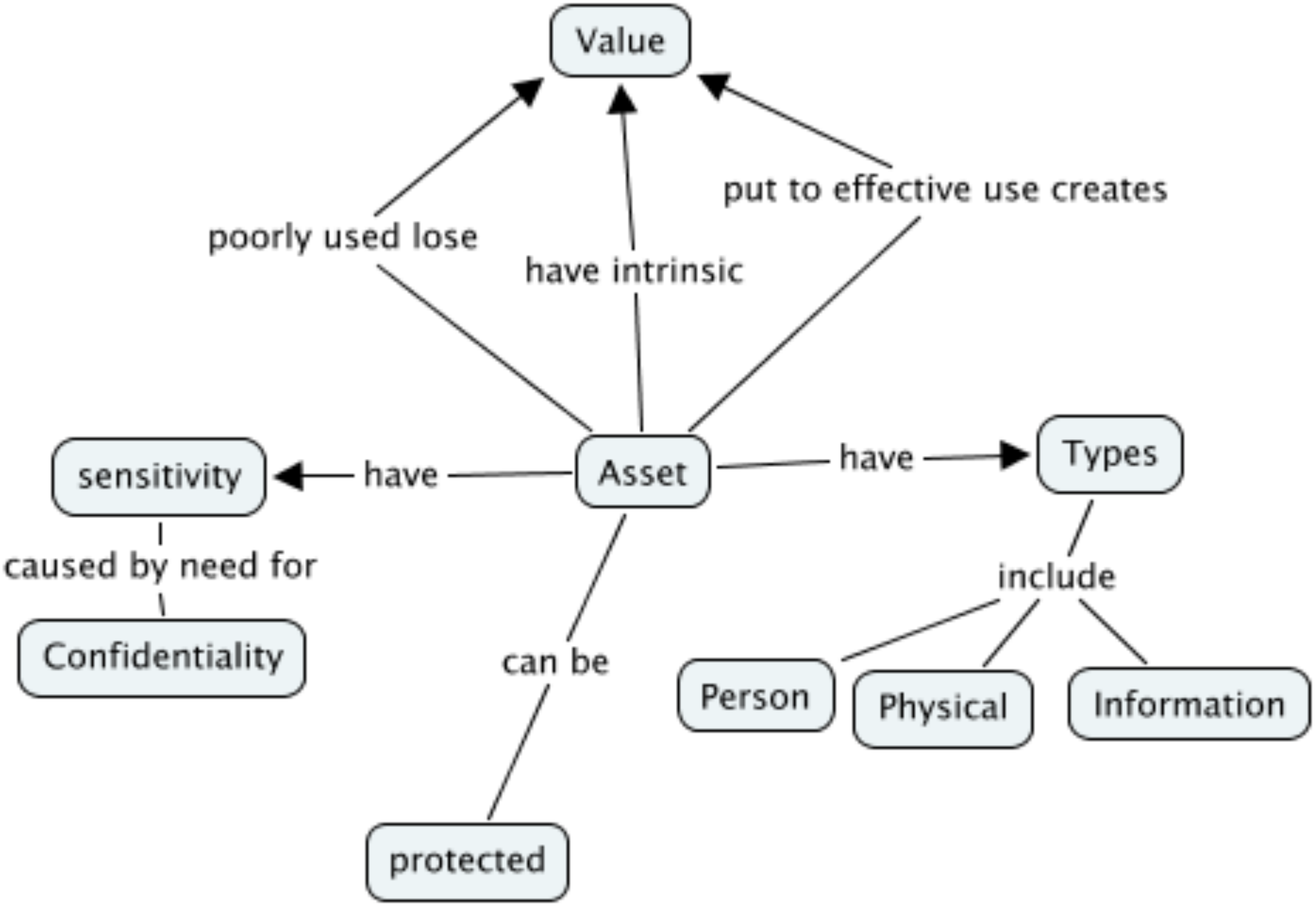
- (#1) Personal Impacts
- (#2) Business Impacts
- (#3) Societal Impacts
- (#4) Geo-Political Impacts
- (#5) Environmental Impacts

- All can create Economic Impacts

Concept Mapping 101

- List and Define the related terms
- Identify the relevant primary linkages (Avoid secondary and tertiary linkages)
- Describe these linkages in a manner that makes clear the reason for, or cause of the linkage
- Do NOT define one of the terms when describing the linkage.

Spot the deliberate mistakes!



COBIT Information Criteria

Effectiveness deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.

Efficiency concerns the provision of information through the optimal (most productive and economical) use of resources.

Confidentiality concerns the protection of sensitive information from unauthorised disclosure.

Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.

Availability relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

Compliance deals with complying with the laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria as well as internal policies.

Reliability relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities.

DoS attack of fbi.gov by??

- You guessed it by themselves
- On Friday 11/11/11 the FBI Admins let the DNSSEC signature expire on a sever
- Thus for those that checked they could not get the fbi.gov domain addresses resolved

Source : http://isc.sans.edu/ Storm Centre Diary

http://isc.sans.edu/diary/Details+About+the+fbi+gov+DNSSEC+Configuration+Issue+/12013

Aaargh!! I mentioned VPN

- Why do I hate VPN?
- Simple… it's a pipe for Rats!

JERICHO FORUM

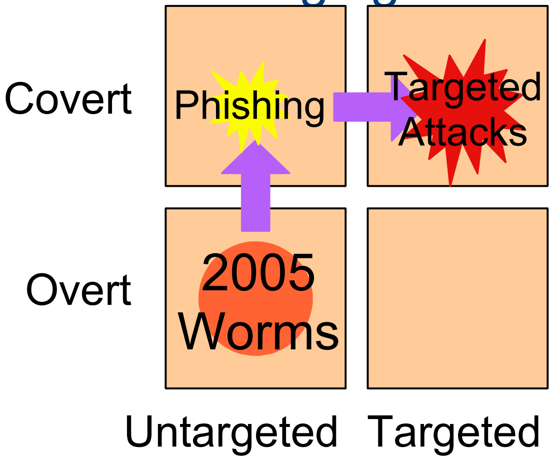
Read the Jericho Forum Commandments and the paper on Secure End to End Communications

Why Worry?: AFS 2005

Security Environment 2005 > 2009

Aalesund University College

- Changing Threats



Covert

Overt

Phishing

Targeted Attacks

2005 Worms

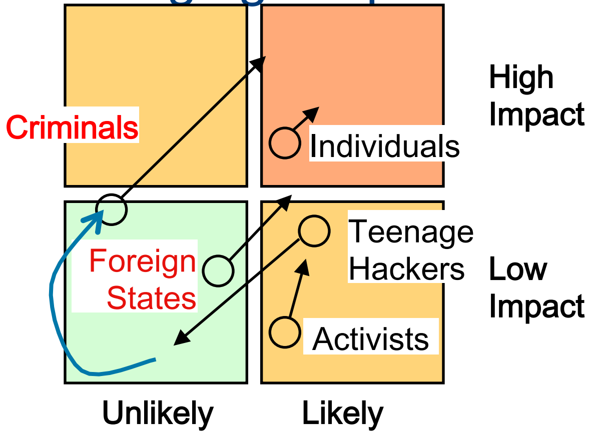
Untargeted

Targeted

< Creates Loss

< Created Noise

Changing Perpetrators



Criminals

Individuals

Foreign States

Teenage Hackers

Activists

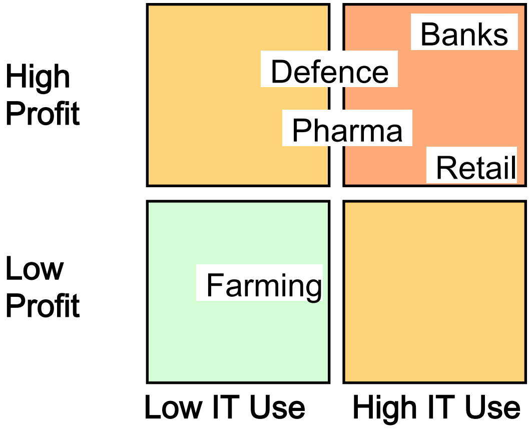
High Impact

Low Impact

Unlikely

Likely

Target Industries



High Profit

Low Profit

Banks

Defence

Pharma

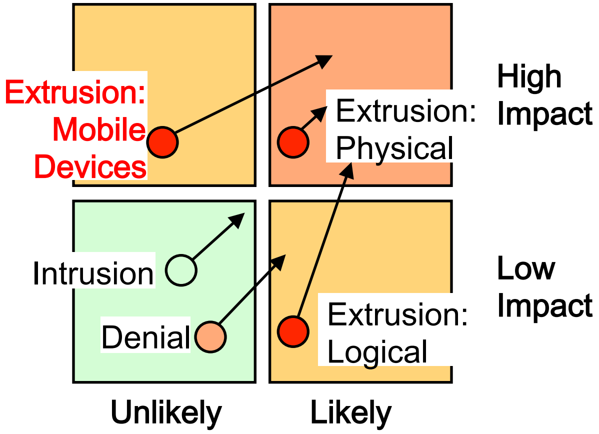
Retail

Farming

Low IT Use

High IT Use

Changing Means



Extrusion: Mobile Devices

Extrusion: Physical

Intrusion

Denial

Extrusion: Logical

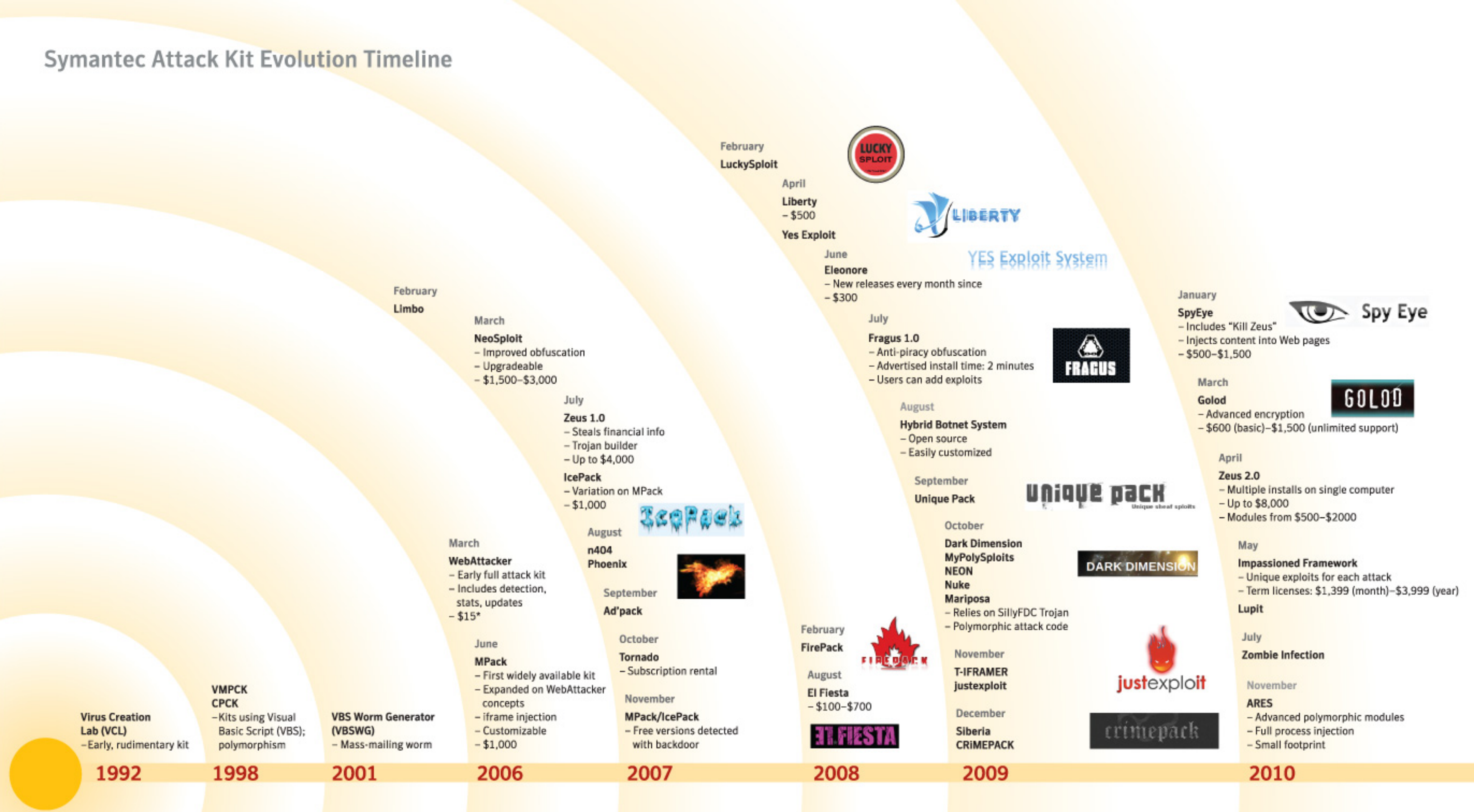
High Impact

Low Impact

Unlikely

Likely

Attack Kit Evolution



Symantec Attack Kit Evolution Timeline

1992

Virus Creation Lab (VCL)
– Early, rudimentary kit

1998

VMPCK
CPCK
– Kits using Visual Basic Script (VBS); polymorphism

2001

VBS Worm Generator (VBSWG)
– Mass-mailing worm

2006

February
Limbo

March
NeoSploit
– Improved obfuscation
– Upgradeable
– $1,500–$3,000

March
WebAttacker
– Early full attack kit
– Includes detection, stats, updates
– $15*

June
MPack
– First widely available kit
– Expanded on WebAttacker concepts
– iframe injection
– Customizable
– $1,000

July
Zeus 1.0
– Steals financial info
– Trojan builder
– Up to $4,000

IcePack
– Variation on MPack
– $1,000

August
n404
Phoenix

September
Ad'pack

2007

October
Tornado
– Subscription rental

November
MPack/IcePack
– Free versions detected with backdoor

February
LuckySploit

April
Liberty
– $500

Yes Exploit

June
Eleonore
– New releases every month since
– $300

July
Fragus 1.0
– Anti-piracy obfuscation
– Advertised install time: 2 minutes
– Users can add exploits

August
Hybrid Botnet System
– Open source
– Easily customized

September
Unique Pack

2008

February
FirePack

August
El Fiesta
– $100–$700

2009

October
Dark Dimension
MyPolySploits
NEON
Nuke
Mariposa
– Relies on SillyFDC Trojan
– Polymorphic attack code

November
T-IFRAMER
justexploit

December
Siberia
CRIMEPACK

2010

January
SpyEye
– Includes "Kill Zeus"
– Injects content into Web pages
– $500–$1,500

March
Golod
– Advanced encryption
– $600 (basic)–$1,500 (unlimited support)

April
Zeus 2.0
– Multiple installs on single computer
– Up to $8,000
– Modules from $500–$2000

May
Impassioned Framework
– Unique exploits for each attack
– Term licenses: $1,399 (month)–$3,999 (year)

Lupit

July
Zombie Infection

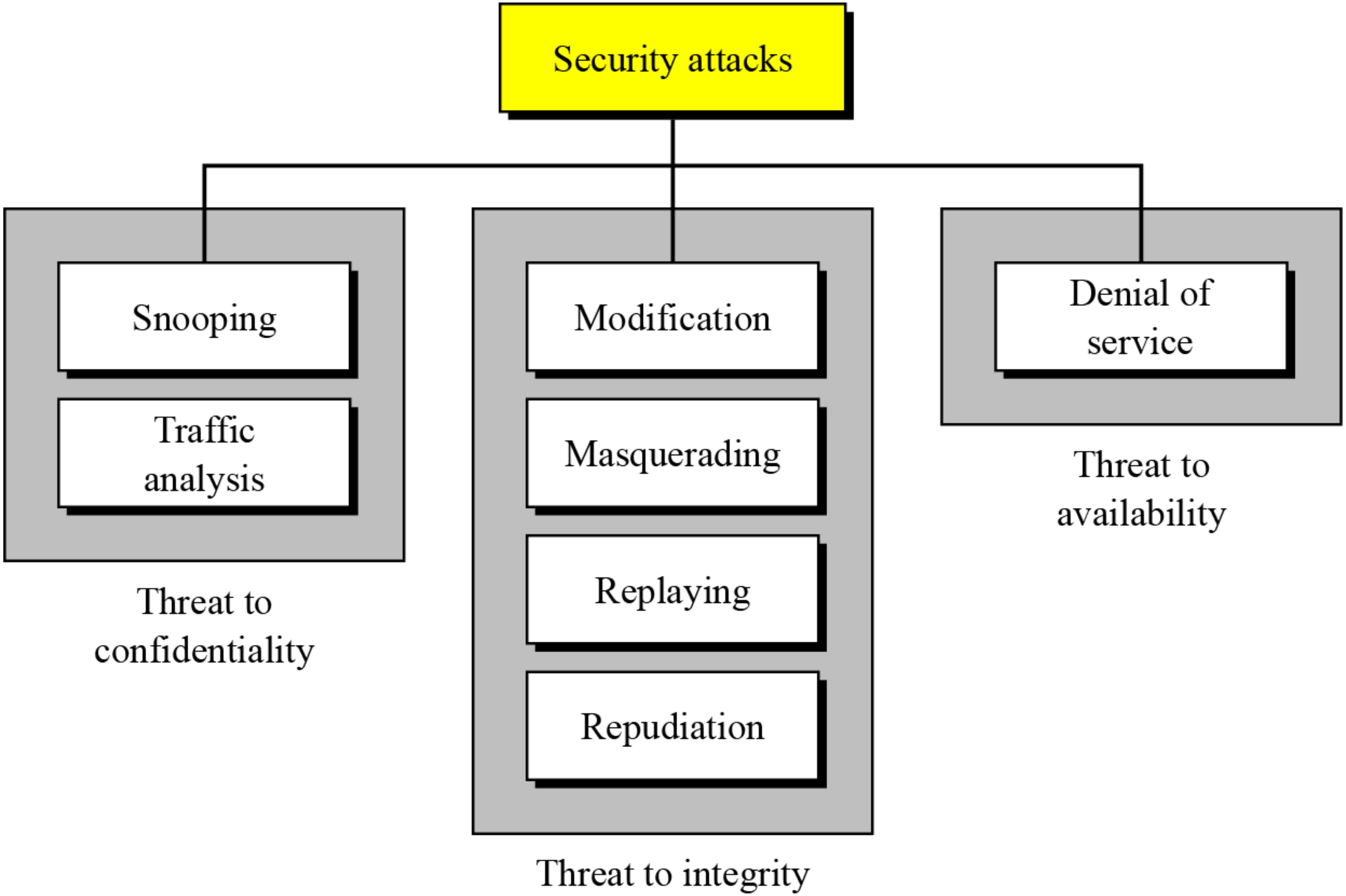
November
ARES
– Advanced polymorphic modules
– Full process injection
– Small footprint

Source: http://www.symantec.com/business/popup.jsp?popupid=attack_kit_evolution_timeline

Symantec Videos

- Attack Kits
- Botnets
- CyberCrime Underground

Types of Attacks on CIA



ISMS Implementation

Steps	Products
Define the scope	ISMS Scope Document
Define an ISMS Policy	ISMS Policy
Define the Risk Assessment Approach	Documented Risk Assessment Approach
Identify Risks and their Components	Risk Register, including List of Threats, Vulnerabilities and Impacts
Undertake Enterprise Risk Assessment	Report on potential Business Impacts of Risks and their likelihoods.
Evaluate Risk Treatment Options	Risk Treatment Plan
Define Control Objectives & Select Controls	Documented Controls & Objectives
Gain approval for Residual Risks	Record of Approved Residual Risks
Gain approval for implementing the ISMS	ISMS Authorisation
Prepare Statement of Applicability	Statement of Applicability

ISO 27000 Series

ISO/IEC **27000** - will provide an overview/introduction to the ISO27k standards as a whole plus the specialist vocabulary used in ISO27k.

ISO/IEC **27001**:2005 is the ISMS requirements standard (specification) against which around 5,000 organizations have been certified compliant.

ISO/IEC **27002**:2005 is the code of practice for information security management describing a comprehensive set of information security control objectives and a set of generally accepted good practice security controls.

ISO/IEC **27003** provides implementation guidance for ISO/IEC 27001

ISO/IEC **27004** will be an information security management measurement standard suggesting metrics to help improve the effectiveness of an ISMS.

ISO/IEC **27005**:2008 is a new information security risk management standard

ISO/IEC **27006**:2007 is a guide to the certification or registration process for accredited ISMS certification or registration bodies.

ISO/IEC **27007** is a guideline for auditing ISMS

ISO/IEC TR 27008 will provide guidance on auditing information security controls.

ISO/IEC 27010 will provide guidance on information security management for sector-to-sector communications.

Original Source: http://www.berr.gov.uk/whatwedo/sectors/infosec/infosecadvice
Now a dead link

ISO 27000 Series

ISO/IEC 27011 will be information security management guidelines for telecommunications (also known as X.1051) and will be released soon.

ISO/IEC 27012 will provide information security management systems guidance for e-government.

ISO/IEC 27013 will provide guidance on the integrated implementation of ISO/IEC 20000-1 (ITIL) and ISO/IEC 27001 (ISMS) Page added Jan 15th

ISO/IEC 27014 will cover information security governance. Updated Jan 15

ISO/IEC 27015 will provide information security management systems guidance for financial services organizations. Updated Jan 15

ISO/IEC 27031 will be an ICT-focused standard on business continuity.

ISO/IEC 27032 will provide guidelines for cyber security.

ISO/IEC 27033 will replace the multi-part ISO/IEC 18028 standard on IT network security. Updated Dec 21

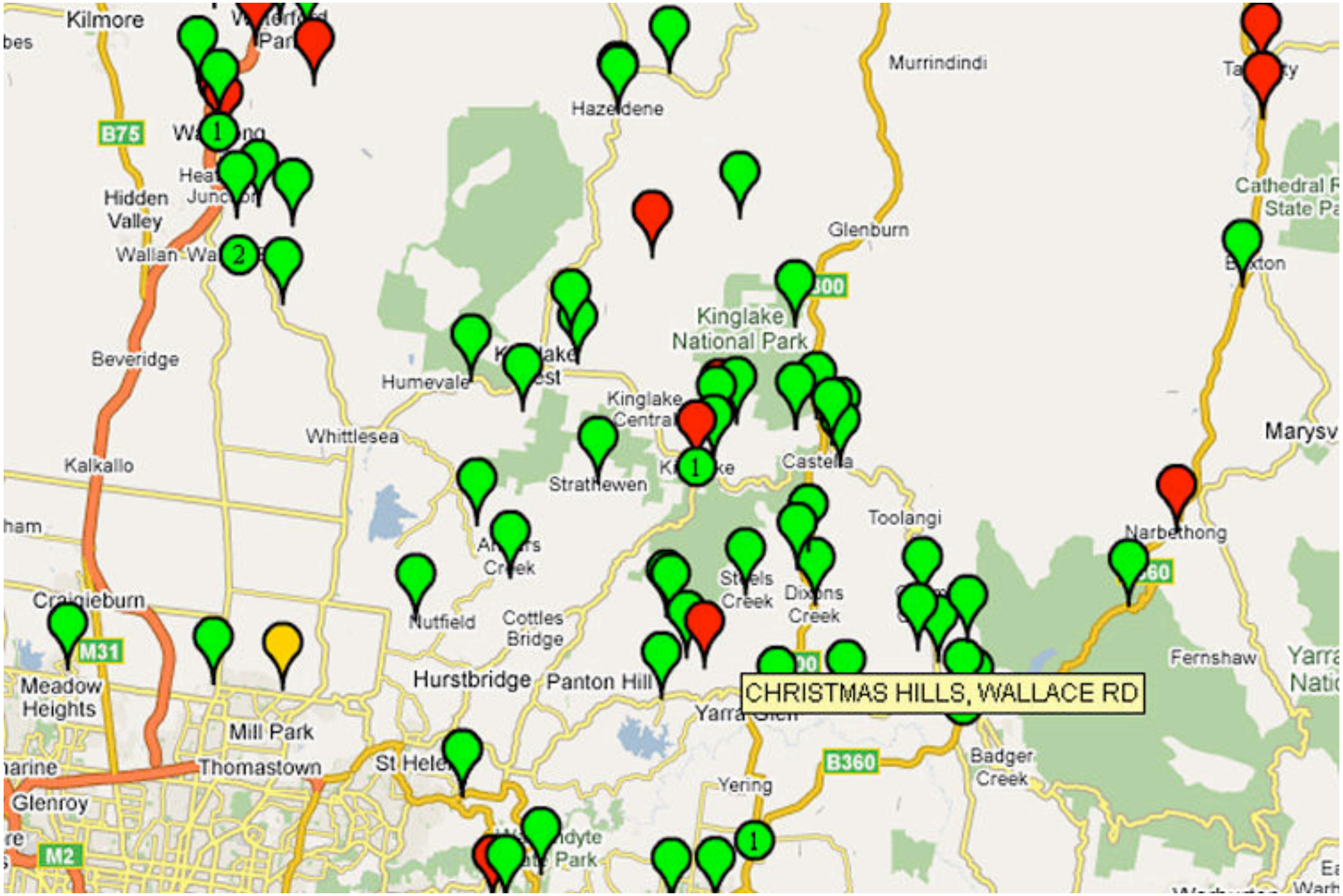
ISO/IEC 27034 will provide guidelines for application security.

ISO/IEC 27035 will replace ISO TR 18044 on security incident management.

Original Source: http://www.berr.gov.uk/whatwedo/sectors/infosec/infosecadvice
Now a dead link

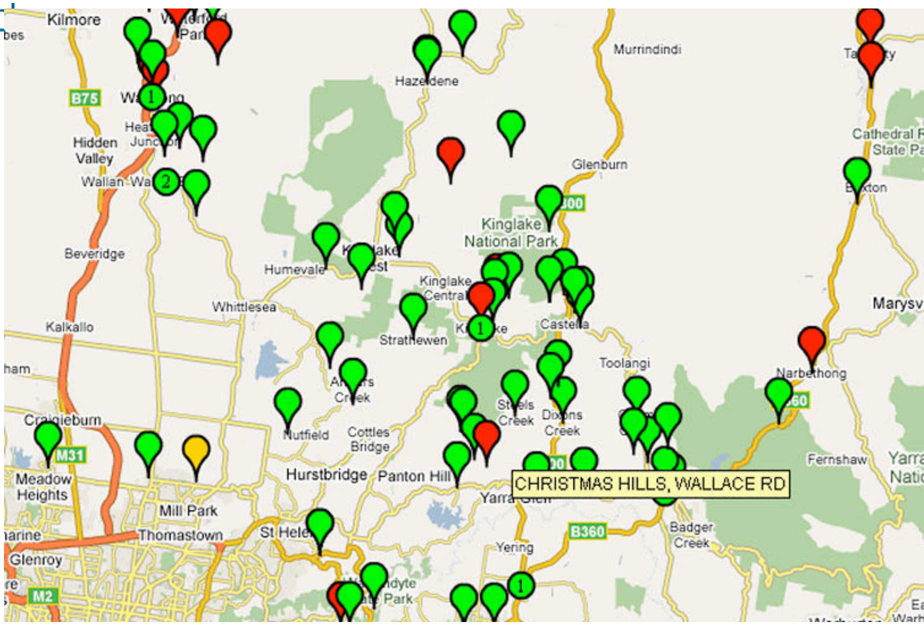
Aalesund
University
College

Best Homes to Rob!



Transparency Good or Bad?

- Thanks to Google technology, you can use the satellite feature and zoom in on the layout of campaign donors' land and access the quickest route through their neighborhoods.
- After combing this map, activists encouraged by gay rights Web sites have been harassing individuals who have donated to the Prop 8 campaign. Death threats, physical violence, vandalism and harassing phone calls have been reported.
- Source: http://media.www.guilfordian.com/media/storage/paper281/news/2009/01/30/Forum/Google.Map.Outs.Donors.To.Proposition.8-3605264.shtml
- Actually this was a real time map of the Australian Bushfires…



But I want Control!

- Selective Transparency
- Privacy “I” control

- I call this Data Primacy

	Not Private	Private
Transparent	🟥	?
Not Transparent	🟧	🟦

Data Protection Principles

1. Processed fairly and lawfully
2. Processed only for specified lawful purpose(s)
3. Adequate, relevant and not excessive in regard to the specified purpose(s)
4. Accurate and up-to-date
5. Maintained no longer than necessary with regard to the specified purpose(s)
6. Processed in a way that meets the rights of the individual (i.e. the person to whom the data refers)
7. Protected by appropriate controls
8. Not transferred outside the EU unless reciprocal legislation and practices exist in the recipient country

Source:http://www.berr.gov.uk/whatwedo/sectors/infosec/infosecadvice/legislationpolicystandards/legislation/dataprotectionact/page33364.html

Safe Harbour Principles

1. Notice
   Individuals must be informed that their data is being collected and about how it will be used.
2. Choice
   Individuals must have the ability to opt out of the collection and forward transfer of the data to third parties.
3. Onward Transfer
   Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.

Safe Harbour Principles

4. Security

   Reasonable efforts must be made to prevent loss of collected information.

5. Data Integrity

   Data must be relevant and reliable for the purpose it was collected.

6. Access

   Individuals must be able to access information held about them, and correct or delete it if it is inaccurate.

7. Enforcement

   There must be effective means of enforcing these rules.

Safe Harbour Principles

1. NOTICE
   An organization must inform individuals about the purposes for which it collects information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or discloses it to a third party.

Safe Harbour Principles

2. CHOICE

An organization must offer individuals the opportunity to choose (opt out) whether and how personal information they provide is used or disclosed to third parties (where such use is incompatible with the purpose for which it was originally collected or with any other purpose disclosed to the individual in a notice). They must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise this option. For sensitive information, such as medical and health information, information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information concerning the sex life of the individual they must be given affirmative or explicit (opt in) choice.(4)

Safe Harbour Principles

3. ONWARD TRANSFER

An organization may only disclose personal information to third parties consistent with the principles of notice and choice. Where an organization has not provided choice because a use is compatible with the purpose for which the data was originally collected or which was disclosed in a notice and the organization wishes to transfer the data to a third party, it may do so if it first either ascertains that the third party subscribes to the safe harbor principles or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant safe harbor principles.(5)

Safe Harbour Principles

4. SECURITY

Organizations creating, maintaining, using or disseminating personal information must take reasonable measures to assure its reliability for its intended use and reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

Safe Harbour Principles

5. DATA INTEGRITY

Consistent with these principles, an organization may only process personal information relevant to the purposes for which it has been gathered. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is accurate, complete, and current.

Safe Harbour Principles

6. ACCESS
   Individuals must have [reasonable] access to personal information about them that an organization holds and be able to correct or amend that information where it is inaccurate. [Reasonableness of access depends on the nature and sensitivity of the information collected, its intended uses, and the expense and difficulty of providing the individual with access to the information.](6)

Safe Harbour Principles

7. ENFORCEMENT

Effective privacy protection must include mechanisms for assuring compliance with the safe harbor principles, recourse for individuals to whom the data relate affected by non-compliance with the principles, and consequences for the organization when the principles are not followed.

At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which an individual’s complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with these principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

Exercise Two: Regulations

- In your Groups:
- Compare Data Protection Principles with Safe Harbour Principles
- Be ready to describe the linkages when asked
- (20 Mins)

Sensitive Personal Information

- Racial or ethnic origin
- Criminal records
- Certain elements of employment records e.g. “**Trade Union memberships**”
- Medical records
- Political opinions
- Religion
- Sexual orientation

Aims of Records Management

- What does a Records Retention Program actually do?
- What is Toxic Data?
- How long should documents be kept?
- Is that different for electronic data?

- Should we have a right to be virtually forgotten?

COBIT Information Criteria

Effectiveness deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.

Efficiency concerns the provision of information through the optimal (most productive and economical) use of resources.

Confidentiality concerns the protection of sensitive information from unauthorised disclosure.

Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.

Availability relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

Compliance deals with complying with the laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria as well as internal policies.

Reliability relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities.

Source: http://www.isaca.org/Template.cfm?Section=COBIT6&CONTENTID=8981&TEMPLATE=/ContentManagement/ContentDisplay.cfm

What was bad about this?

- Hacking gang breaks into Breiviks email

Aalesund
University
College

What links these?

- Svalbard
- 2nd People Liberation Army
- US Satellites

- Answer URLs
- http://theforeigner.no/pages/news-in-brief/norway-in-chinese-american-hacking-attacks/
- http://theforeigner.no/pages/news-in-brief/norway-satellite-security-may-be-outdated/

Amber Alert

Final Quiz: What are these?

- $C1 = 11 - (3x1 + 7x2 + 6x3 + x4 + 8x5 + 9x6 + 4i1 + 5i2 + 2i3) \text{mod} 11$
- $C2 = 11 - (5x1 + 4x2 + 3x3 + 2x4 + 7x5 + 6x6 + 5i1 + 4i2 + 3i3 + 2c1)$ $\text{mod} 11$

- Clue $x1$, $x2$, $x3$, $x4$, $x5$ & $x6$ relate to your birthdays

Some Useful Reading

http://delicious.com/adrius42/IAMkeytext

Related to:

Information Assets

ISO 27000

ITIL

COBIT