Managing IT Risk

Risk - combination of the probability of an event and its consequence

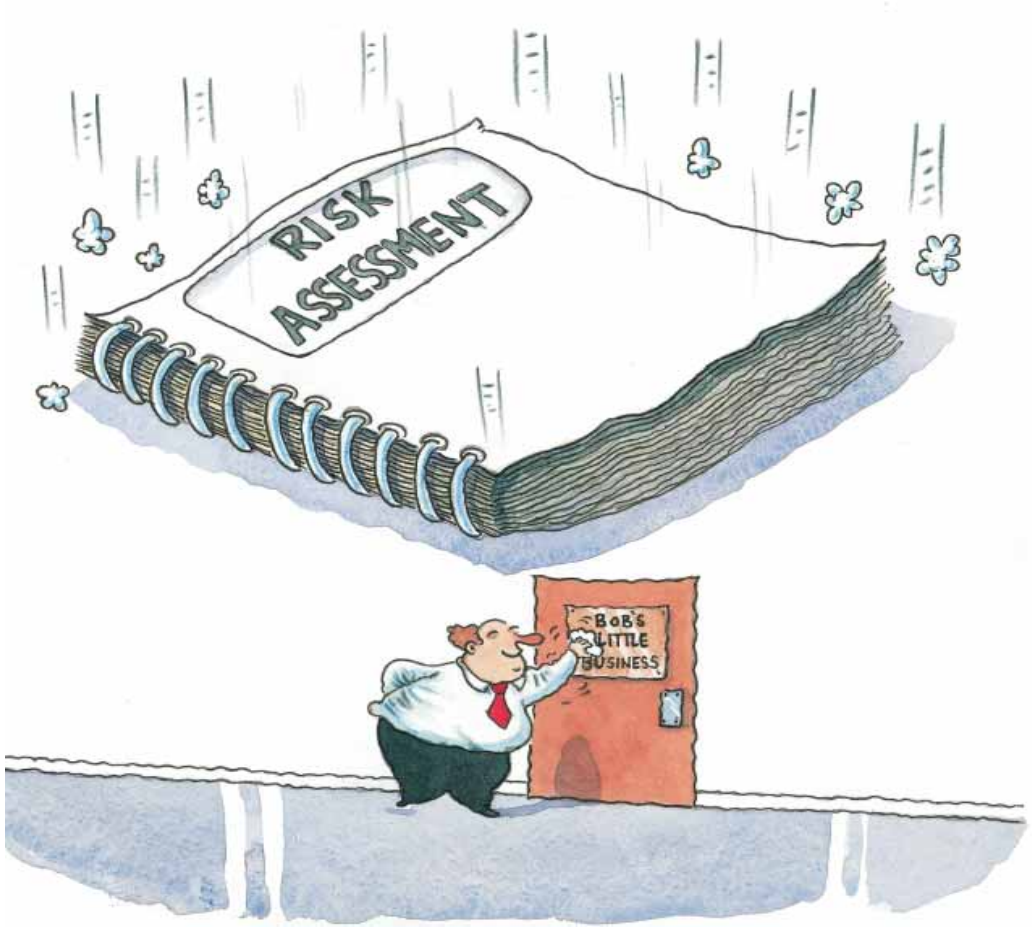
Tom Anstey
tom.anstey@imm.ox.ac.uk

Managing risk

Technology has enabled us to work in remote locations, away from the office and at any hour. This puts at risk data that we work with on laptop computers and portable storage devices because they can be stolen or misplaced.

We cannot change these realities, so we must do a far better job of protecting data contained on the devices.

A Statement from the NIH Director,
Elias A. Zerhouni, M.D.,
on Encryption and Data Security



If there is genuinely no significant risk, nothing needs to be written down. If a written assessment is needed – keep it fit for purpose, and crucially, act on it.

Paperwork without action does no one any good.

Management support is essential

Effective information security governance requires senior management commitment and an overall culture conducive to information security at the executive and operational levels. Too often management determines that it is easier to buy a solution than to change a culture. The result is all too often an ad hoc collection of poorly integrated tactical point solutions that are increasingly difficult to manage and invariably leave gaps in protection.

Management support is essential

Education and training in the operation of information security processes are often overlooked as well. However management should consider that even the most secure system, if operated by ill-informed, untrained, careless of indifferent personnel, will not achieve a significant degree of security.

ISACA Information Security Governance

Guidance for Information Security Managers

Identify the hazards

The data itself obviously isn't hazardous

Personally identifiable data – in UK, Data Protection Act 1998

- Any information that links one or more identifiable living person with private information about them
- Any source of information about 1000 identifiable individuals or more other than information sourced from the public domain

Identify the hazards

The data itself obviously isn't hazardous

- Emails and the contacts stored in an email system count as personal data
- Research data
- Locations, research methods, staffing data
- Examination results
- Intellectual Property – what might it be worth?

Who might be at risk and how?

The University or College

Fines by the Information Commissioner's Office (ICO) – up to £500,000

Bad publicity

Loss of possible funding and public goodwill

Release of Intellectual Property

Who might be at risk and how?

Funding bodies (including parents?)

The Media is probably the biggest problem

Staff, students, their families and colleagues

Private information, user names, contact details, research methods (a CV/resumé/job application could easily count as “Personal Data”)

Evaluate the risk, looking at the type of data stored..

Is there an Information Asset Register?

Does the Risk Register extend to information/data?

Is there sensitive data in places where it may easily be physically removed – laptops, external hard drives, USB keys, PDAs, mobile 'phones, iPads?

Do you understand your colleagues' work?

Are you even interested? Is it your job?

Evaluate the risk, looking at where the data is stored..

Is there sensitive data in places where it may easily be physically removed – laptops, external hard drives, USB keys, mobile 'phones, iPads etc.?

Are the rooms locked, laptops tethered, and is there CCTV and door access control?

Is equipment labelled and on the inventory? Is there frosted glass on windows in public viewable areas?

Evaluate the risk

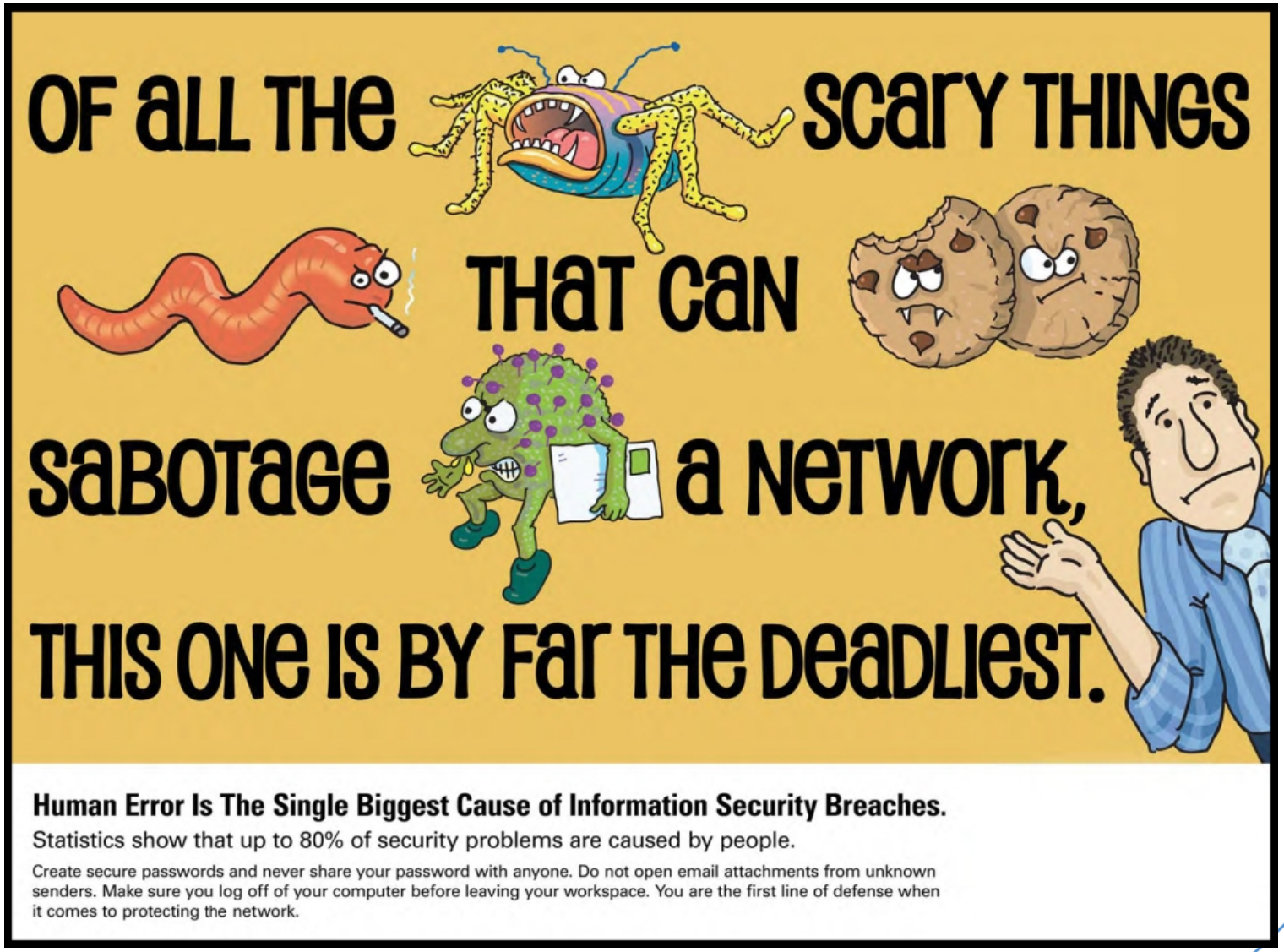
Electronic security

Are you using encryption? Is all accessible data anonymised? Remote wipe facilities on smartphones? Are there limits to shared data areas? Are the firewall rules too lax?

Security -vs- Convenience

Humans are the greatest risk! From inside and outside!

Have you vetted all staff & contractors in particularly sensitive areas?
Do staff know what they may say and to whom?


OF ALL THE
SCARY THINGS
THAT CAN
SABOTAGE
A NETWORK,
THIS ONE IS BY FAR THE DEADLIEST.
Human Error Is The Single Biggest Cause of Information Security Breaches.
Statistics show that up to 80% of security problems are caused by people.
Create secure passwords and never share your password with anyone. Do not open email attachments from unknown senders. Make sure you log off of your computer before leaving your workspace. You are the first line of defense when it comes to protecting the network.

Mitigate the risk

- Consider encryption – it's not a cure-all, but makes the ICO happy!

"That's our CIO. He's encrypted for security purposes."

Mitigate the risk - physical

- Lock rooms, tether laptops
- CCTV and (logged) access door controls - a lock isn’t enough!
- Equipment labelling lowers re-sale value
- Put frosted glass on windows in areas visible to the public

Mitigate the risk

- Electronic security – firewalls, A/V etc
- Encrypt if needed, anonymise data, limit access to shared data
- Humans are the greatest risk
- Mandate the wearing of ID cards?
- Encourage the challenging of unknown people
- Don’t allow tailgating through access routes

Take precautions and prevent loss!

Ban camera-phones and iPads? Disable USB ports on workstations? Force encryption of USB storage?

Lock rooms and laptops, CCTV, equipment labelling and inventory, access controls

Electronic security eg. encryption, remote backup, anonymised data, limits to shared data areas, remote wipe of portable devices.

However, go too far, and users will become evasive!

Personal ID Security

Check the identity of anyone requesting confidential data

Take up references for potential staff and students & perform security checks if needed (assess risk!).

Personal ID Security

Advise your users to choose passwords that are unique mixtures of letters & numbers and other characters, or a selection of words (although password policies may dictate what you enter).

The longer the password, the ~~more secure~~ less insecure it is likely to be!

Remember to change them regularly and do not use identical usernames and passwords on different systems

Two-factor authentication?

Personal ID Security

Think very carefully before submitting any personal or work information online – including on Facebook and LinkedIn

Check the privacy policy of any website where you submit personal data – if it doesn't have a clear and comprehensive policy, don't submit it

Dispose of data securely, whether in paper or electronic form (especially back-up files & hard drives)

Encrypt sensitive data on portable devices

Sensible risk management

- Have you got an Information Security Policy?
- Individuals need to understand that as well as the right to protection, they also have to exercise responsibility
- So, we need to identify the users and the data being held
- Who owns the laptop/USB device?
- Who owns the data stored on it?
- Who is responsible for possible loss of data?

Good practice

- Create an InfoSec Policy – copy [read first] & paste is OK!
- Manage your workstations – require individual authentication
- Make an inventory and assess risk of data – particularly on mobile devices. Does it really need to be there?
- Use an enterprise encryption solution
- Read and manage your log files
- Monitor your network – but be aware of users' rights to privacy

Got your head in the cloud?

So, what about DropBox, SkyDrive, iCloud or Amazon?

Should the sensitive data be leaving the University or College to somewhere that you have no legal control?

Are you happy that you know and trust all the keepers of your data?

US Safe Harbor scheme – are you content with that? Different legal jurisdictions? DPA?

http://www.adam-hart-davis.org/

Provide understandable guidance

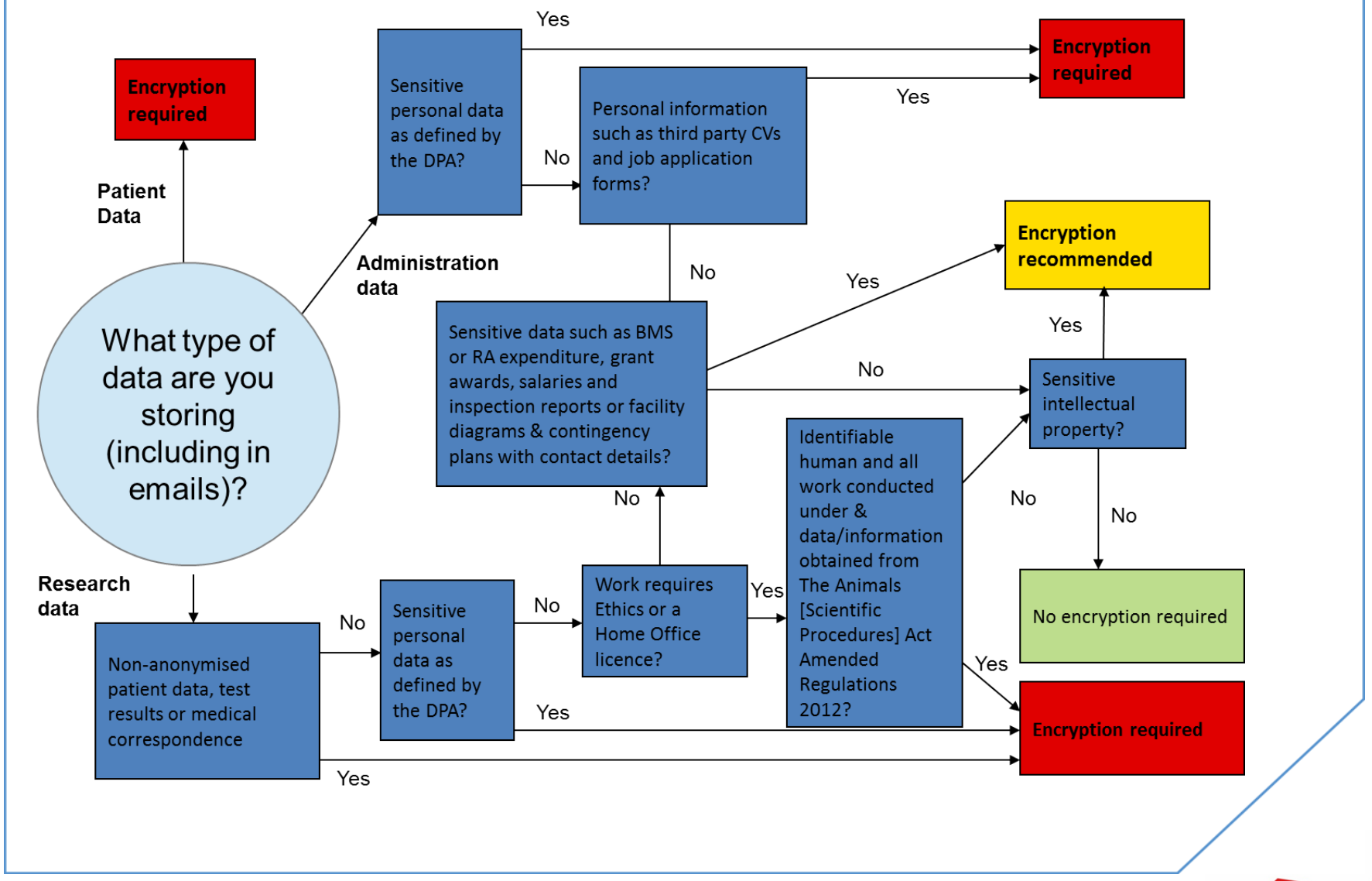
"People mostly want to be good. Rather than tell them not to do stuff, tell them the right way to do things. Secure behaviour needs to be the default, not the bolt-on. Security awareness is a use it or lose it mindset. You have to stay engaged. People follow examples, especially their bosses'. If you can get the boss talking and behaving in a way that shows that security is everyone's responsibility, the message is that much more vibrant."

Chris Burgess
Cisco

Provide understandable guidance

- Keep “geek-speak” out of users’ lives. They don’t want or need it! They probably don’t need to know whether it’s 2048 or 4096-bit encryption nor the hash and salting methods.
- Standardise operating procedures when/where possible, but be flexible.
- Make the difference between “Must” and “Should” very clear!
- All local policies must be at least as stringent as the University Information Security Policy.

When do you need to encrypt a mobile device in the WIMM?




YOUR VIGILANCE
YOUR DETERMINATION
YOUR RESPONSIBILITY
WILL BRING
US SECURITY
Copyright 2010 MindfulSecurity.com The Awareness Resource All Rights Reserved.
KEEP
PATCHING
AND
STAY
SECURE
Copyright 2010 MindfulSecurity.com The Awareness Resource All Rights Reserved.

What to do when it goes wrong

- Don’t bury your head
- Inform Unit Head + OxCERT / University Data Protection Office / Police & University Security
- Be honest! Mea culpa (if needs be) and helpful attitude please
- Learn from your (and others’) mistakes
- Don’t speak to the press – go via the Press Office
- Maintain confidentiality and privacy
- Prepare colleagues and give advice to students

Weatherall Institute of Molecular Medicine

UNIVERSITY OF OXFORD

The MRC Weatherall Institute of Molecular Medicine is a strategic alliance between the Medical Research Council and the University of Oxford

MRC Medical Research Council