Safer working in local government: a layered approach

Jonathan Haddock

12th January 2018

About Jonathan

- Worked in IT for over 15 years, across a number of roles and organisations
- Recently moved to specialise in cyber security
- Previously worked with the BCS YPISG, talking at a number of *penetration testing training days*
- Now a *network and security engineer* working with 3 local government authorities

It‘s important to note that all roles have a part to play in securing the network.

I‘ve experienced various environments, from education, defence, medical and professional services.

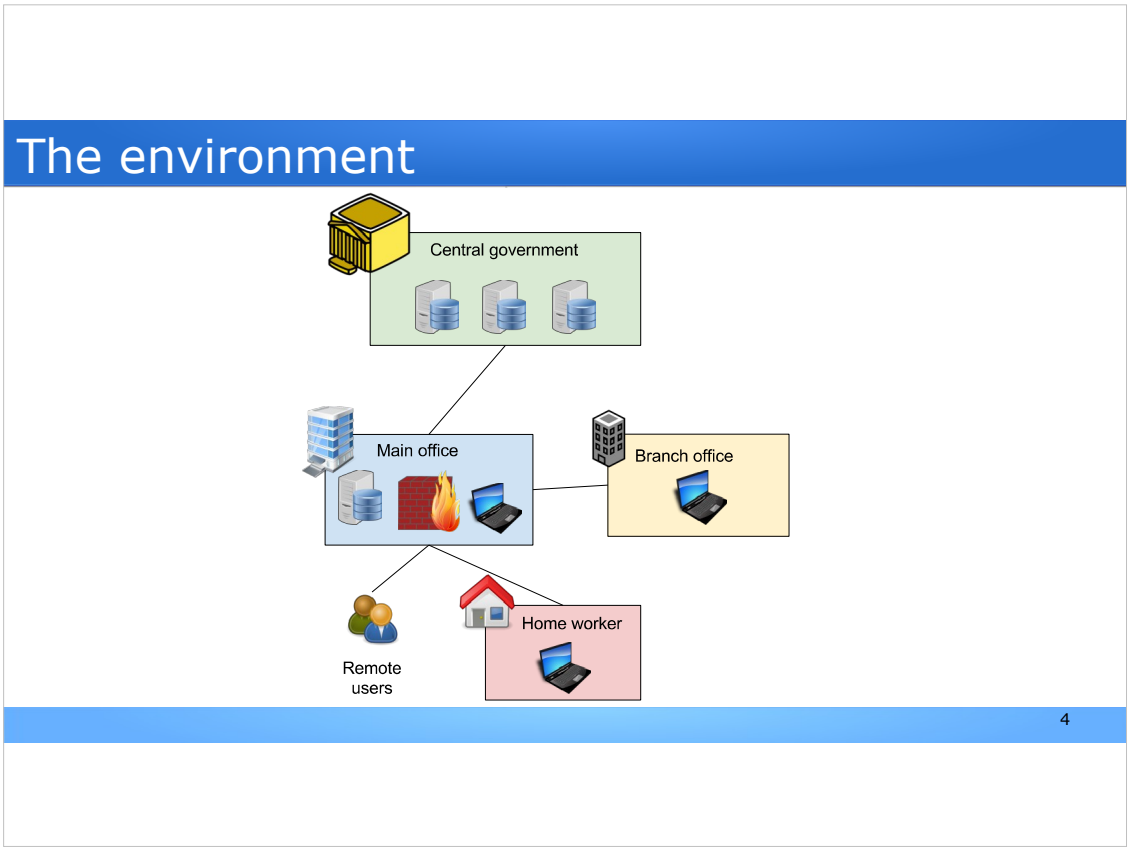
What is local government ?

- An organisation with responsibilities to members of the public
- Provider of numerous services – housing, refuse collection, planning, benefits
- Data processors and owners
- A large employer (approximately 1 million people in the UK[1])

[1] https://local.gov.uk/about/what-local-government

Until you've worked in local government you really don't appreciate how vast it is. Whereas a business may only have its Client Relationship Management software along with an email platform and file servers, local government may have similar systems for *each department*.

There are many applications to manage, with hundreds of users to consider.



Local government offices have a link to *central government* to access data from departments like the DWP.

The main *local government* office is generally where most of the infrastructure is.

Branch offices may have data that‘s not being supervised, and *home workers* potentially have printouts available to multiple house members. As a result it‘s a real challenge to keep track of, and protect, the data.

Challenges for local government

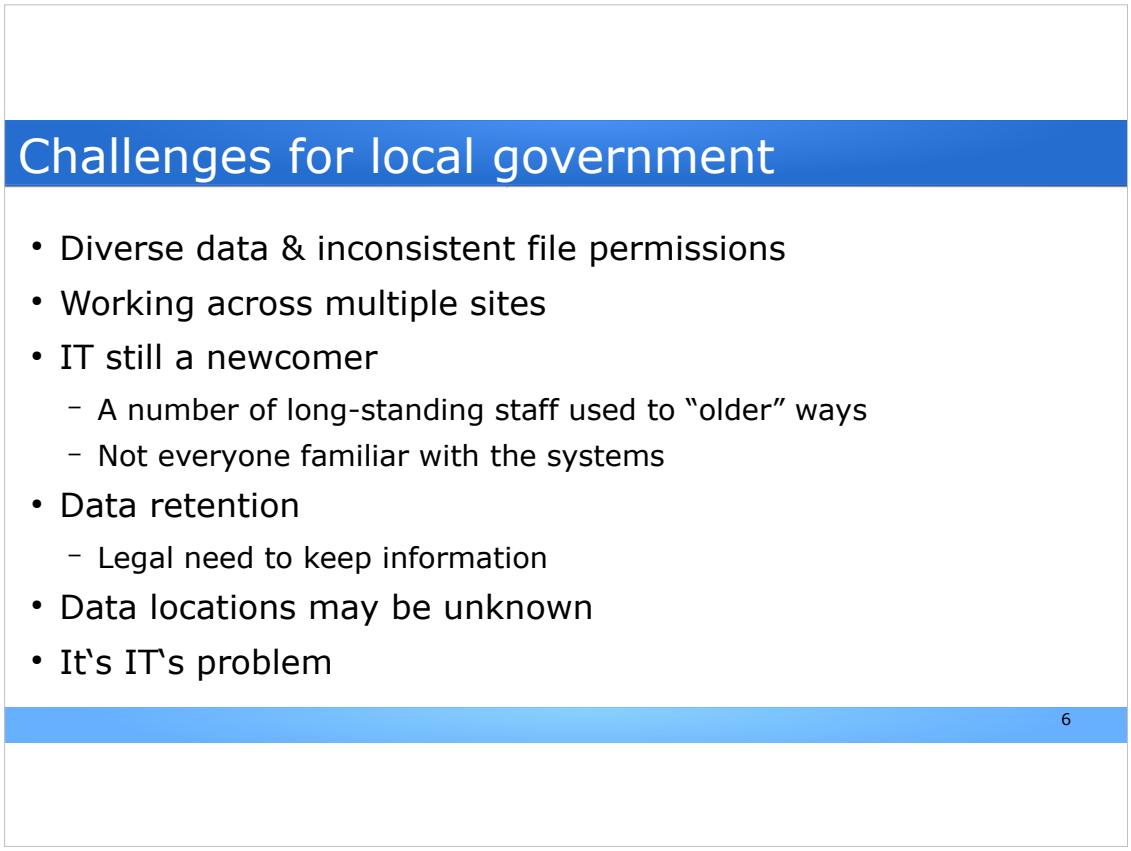
- The need for uptime (sometimes legally mandated)
- Public expectation
- Compliance with law and standards
  - Freedom of Information Act (2000)
  - Data Protection Act (1998)
  - General Data Protection Regulation (2016), from May 2018
  - Payment Card Industry Data Security Standard (PCI DSS)
- Interoperability with government
  - Involves connectivity to central government departments

5

Some local government provided services are legally mandated and have to be operational. This presents a challenge as systems may not be permitted to go offline without significant notice.

Members of the public, and businesses, expect to be able to contact local government whenever convenient, and there‘s a push towards 24x7 working.

Various laws and standards have to be adhered to in order to appropriately protect personal data.



Data is held on people of all ages and financial situations. Naturally this data is sensitive.

As departmental staff have changed, some being redeployed, there can be inconsistent permissions on file servers. Sometimes old access isn't revoked immediately.

Working across multiple sites is a challenge to apply protection in a uniform fashion. Sometimes data must be transported, potentially leading to loss.

There's a real culture of data protection being IT's problem. In reality everyone needs to play their part.

New systems

- Important to ask questions at the commissioning stage
  - What does the vendor do when a vulnerability is found?
  - Are there charges for security updates?
    - Who has to install them?
  - Can the supplier demonstrate their solution aims to be secure?
- Supplier surveys become part of the contract
- Survey questions have to be updated

New systems are subject to review by our technical architect, who'll provide the vendor with a survey covering a number of areas, including security.

There have been occasions where a vendor has stated they'll configure a system securely. When that hasn't happened, their survey has been used to highlight it should have been. This led to remedial work not costing the tax payer.

Keeping the survey updated is an important task.

Old systems

- Data not always migrated - cost
- Needed to access old data
- Often unsupported
- Have to be isolated when vulnerable
  - Can‘t patch
  - Can‘t decommission

Old systems may be required to provide access to legacy data – sometimes there are legal reasons to keep them available.

Cost can be a prohibitive factor to migrating data to a new system, or to upgrading the system in the first place.

Once a system is unsupported, it‘s often vulnerable. To mitigate this risk, unsupported systems get isolated from the network wherever possible.-

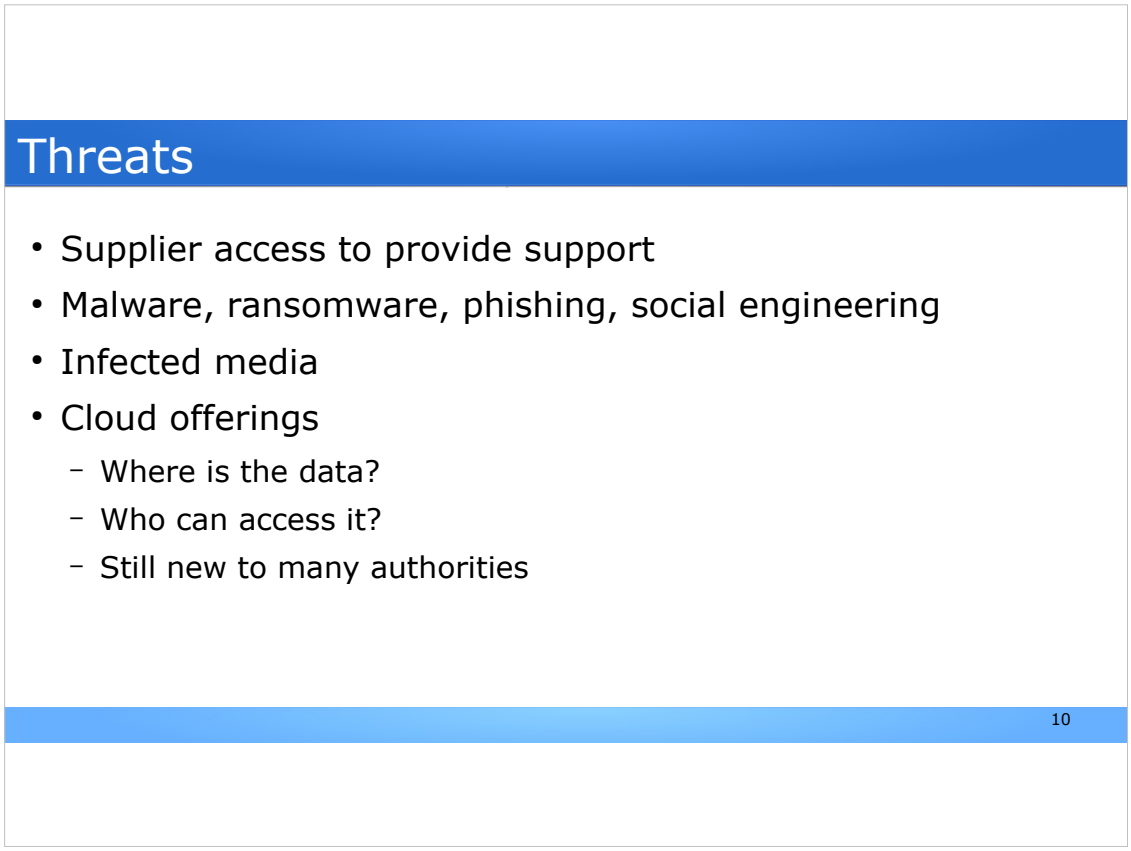
Threats

- Many are the same as faced by businesses
- Potential target due to volume of personal data
- Data theft
- Accidental breaches,e.g.:
  - Double enveloping
  - Sending information to the wrong email address
  - Public release of data (e.g. planning applications)

Confidentiality is important, and breaches can occur for multiple reasons – not all of the malicious intent. A few councils have been prosecuted recently for accidental data breaches.

Availability is also crucial, and ransomware is a persistent threat. We're using behavioural anti-virus, as well as signature based, to help protect our systems.

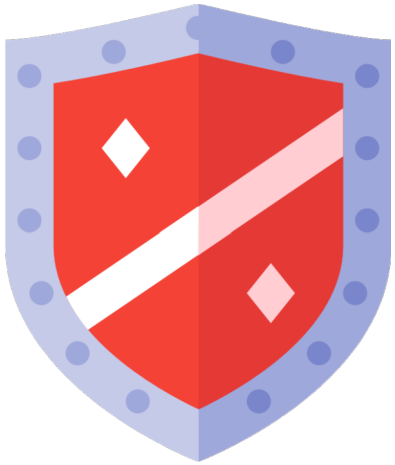
See links towards the end of the notes.



Suppliers need access in order to provide access. At the same time, we‘re required to know who has accessed a system, when (and why). This is controlled by enabling supplier access only as necessary.

There‘s still an expectation that people can just connect their memory stick, or phones, to our systems in order to transfer files. This isn‘t permitted and devices have to be scanned by ICT.

Defence



We have the usual things (firewalls, anti-virus etc.) but also look to provide a few extras too.

Not everything has a technical solution...

Firewalls

- Potentially a very basic mechanism to keep outsiders out
- Next generation firewalls apply further scanning
  - Anti-virus
  - SSL inspection
- Botnet and command & control protection
  - Often a subscription service
- Easily misconfigured
- Not the only answer

12

A firewall falls into the "usual things" bracket. We're using next generation firewalls so are able to scan the traffic coming in to the organisation for malware. Using SSL inspection (AKA SSL intercept) means it's also possible to check encrypted traffic for threats.

Additional subscription services are used to help us block access to addresses with a known bad reputation. The firewalls also act as a transparent proxy.

Updates

- Microsoft's *patch Tuesday*
- Adobe and Java patches, among others
- Scheduling of updates can be a nightmare
  - Push for 24/7 services
- Sometimes the latest version isn't compatible with a key business application
  - Java sometimes has to be maintained at a major version behind
- Cost of updates during austerity
  - Adobe Acrobat Professional, etc.

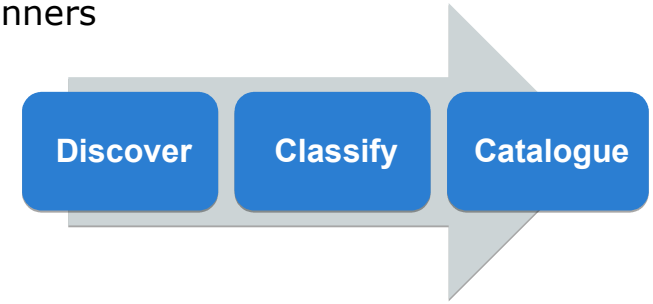
Updates are not always problem-free. Some have to be removed after issues are identified with test users.

More concerningly is when vendor provided applications aren't updated to make use of newer technologies. This leads to a legacy insecure dependency.

Updates are sometimes too costly, so the organisation may choose to bear the risk.

Vulnerability management

- Have to *know* about the vulnerabilities to *manage* them
- Plan to *fix*, *avoid, transfer* or *accept* the various risks
  - Organisation has to make that choice
- Use of vulnerability scanners
- Continual
- A whole talk in itself

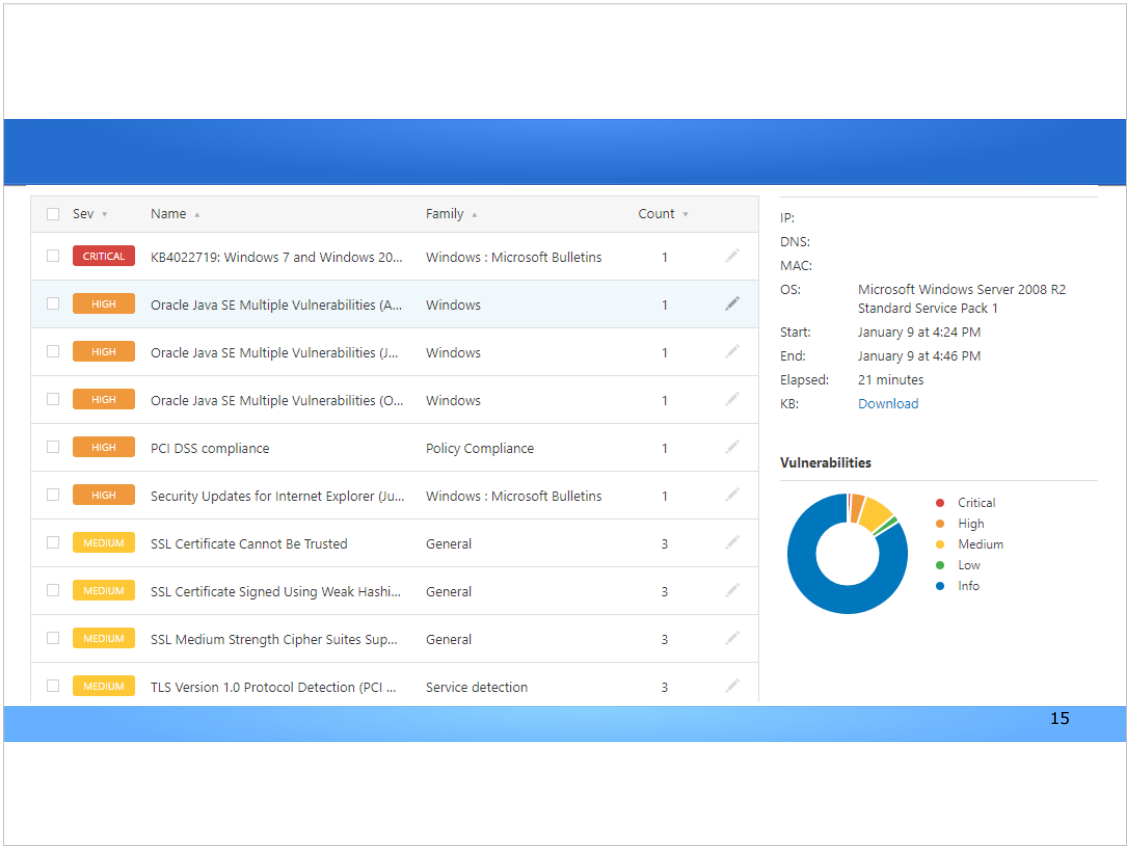


14

It‘s necessary to know the environment in order to be able to do this properly.

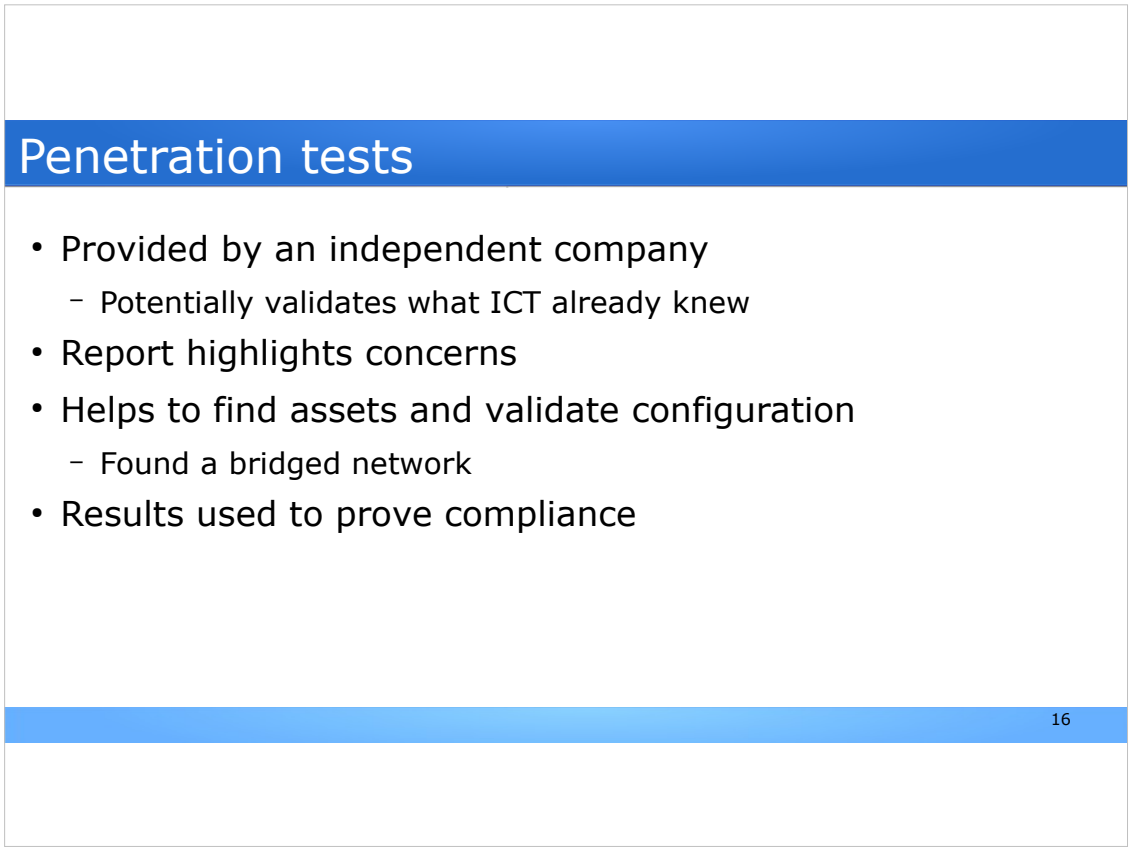
The environment changes, with new equipment perhaps being connected that isn‘t expected. As result this is a continuous process. New problems are also found regularly in existing setups.

If acction is to be taken to fix a problem, it‘s necessary to get any downtime approved. Other IT colleagues have to be available to patch their systems.



Sev	Name	Family	Count
CRITICAL	KB4022719: Windows 7 and Windows 20...	Windows : Microsoft Bulletins	1
HIGH	Oracle Java SE Multiple Vulnerabilities (A...	Windows	1
HIGH	Oracle Java SE Multiple Vulnerabilities (J...	Windows	1
HIGH	Oracle Java SE Multiple Vulnerabilities (O...	Windows	1
HIGH	PCI DSS compliance	Policy Compliance	1
HIGH	Security Updates for Internet Explorer (Ju...	Windows : Microsoft Bulletins	1
MEDIUM	SSL Certificate Cannot Be Trusted	General	3
MEDIUM	SSL Certificate Signed Using Weak Hashi...	General	3
MEDIUM	SSL Medium Strength Cipher Suites Sup...	General	3
MEDIUM	TLS Version 1.0 Protocol Detection (PCI ...	Service detection	3

An example report from the Tenable Nessus vulnerability scanner.



In order to access central government resources we‘re required to have a penetration test conducted each year.

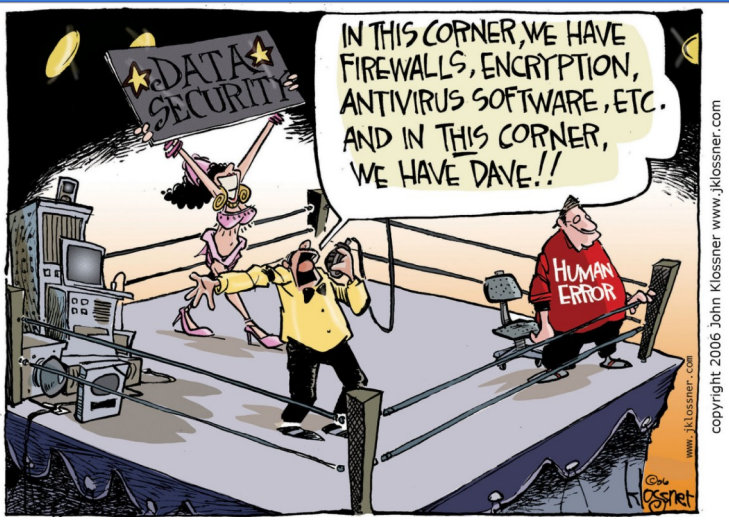
By running our own internal checks, including vulnerability management, we aim to stay on top of problems. This helps to reduce the findings of any penetration test.

Compliance

- A useful pursuader
- Organisations resist change where there's cost
  - Time
  - Financial
- If compliance with a standard is needed, changes become necessary
- Public Sector Network (PSN) and PCI DSS

Given the challenges of down time and cost, it can be a long time before a problem is resolved. Where it's necessary to gain compliance with a particular standard this can be the reason the organisation agrees to an upgrade / change.

What about Dave?



All the technical controls mentioned so far can be undone by a single person, here we call them Dave.

Users can often see security as IT‘s problem, or being for IT‘s benefit.

User training

- Staff are often an organisations *biggest* asset but also its *weakest* link
- Mandatory training
  - Freedom of Information Act (2000)
  - Data Protection Act (1998)
- Security training often an afterthought
  - Security is complicated and slows you down
  - Many managers aren't experts themselves
- Tailgating

Staff didn‘t take the job to worry about all this security stuff – to many of them that‘s something that should be there already. We have to change their thinking so they realise they‘re part of the solution. We‘ve had to explain to them how by being a bit more alert they save themselves time (and interactions with IT!).

It‘s crucial to avoid jargon during training. IT topics can be complicated, and users have varying experiences.

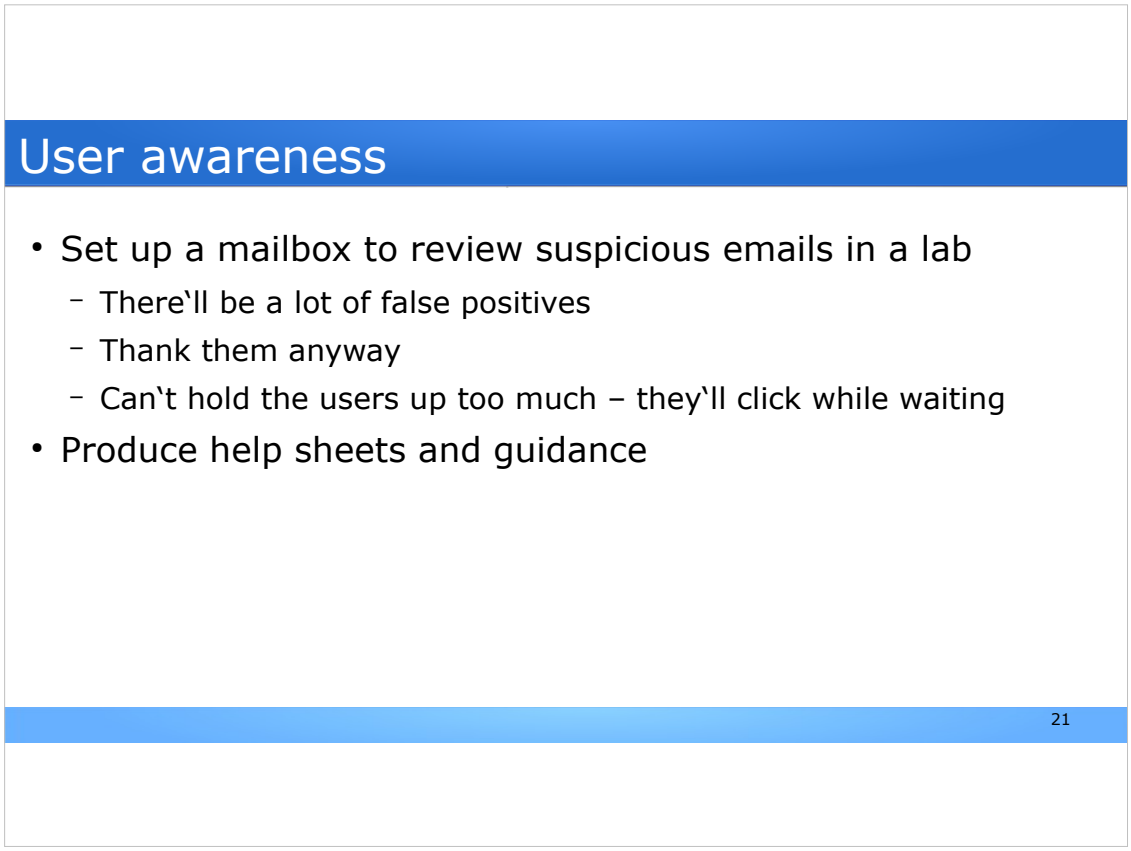
Tailgating is a real problem, despite staff knowing they have to ID anyone that follows them through the door. One of the authorities I work with ran a campaign about this, including a video where yours truly acted as the tailgater.

User awareness

- Once end-users know about the threat, you have to keep them engaged
- Mass-mailing warnings when malicious trends identified
- Criminals are clever, and look to trick the user
  - Can‘t always blame them
  - Sometimes only report to ICT once it‘s too late
- Users may assume a message on their screen is legitimate

We sometimes have to explain to users that filters can‘t catch everything, so aren‘t 100% protection. Many of our end users now treat emails with suspicion but we‘ll still send out warnings sometimes. A good example is around Christmas, when we‘ve seen many parcel waiting scam emails come through.

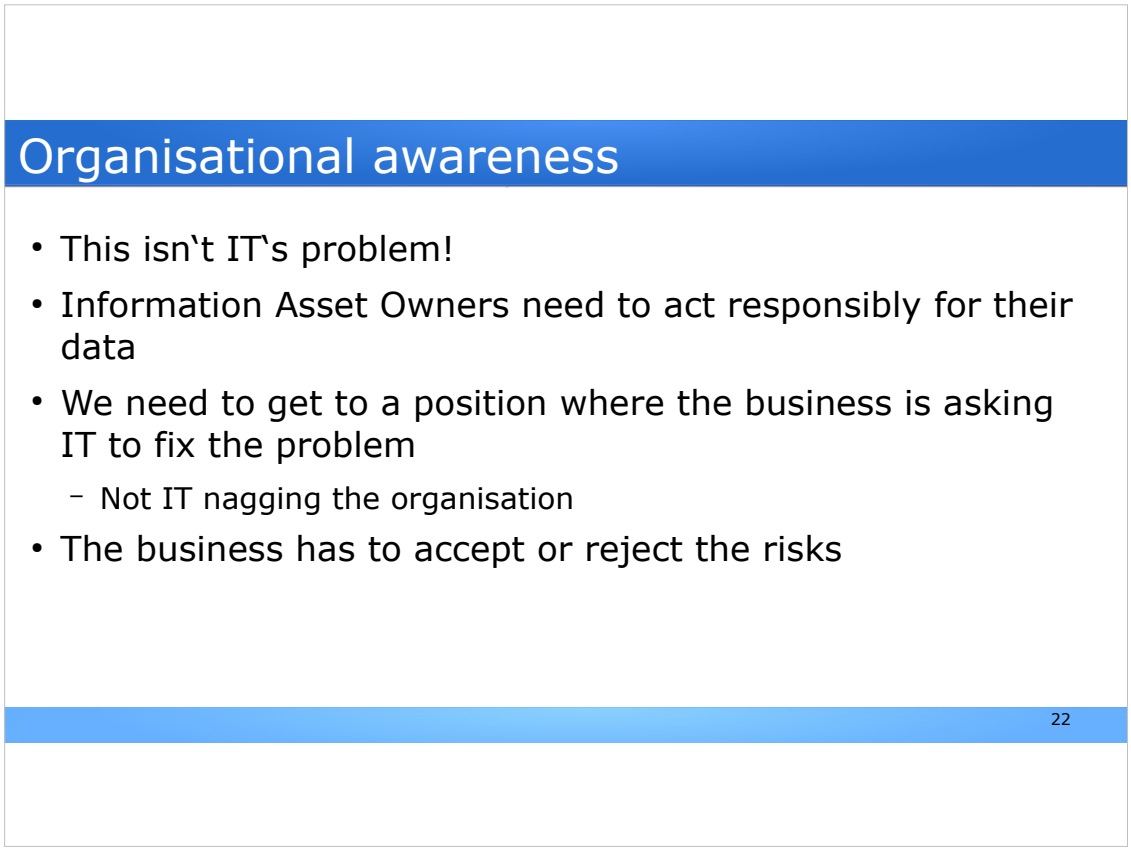
Use of legitimate encryption can confuse things, one user didn‘t contact IT because they thought the ransomware encrypting their files was a legitimate ICT tool.



A review mailbox has the benefit that cautious users will tip you off to a problem. Sometimes a suspicious email will have been received by several people, so knowing about it early can heavily reduce resolution times.

Not all emails sent for review will be an actual problem. Nonetheless, it's important to thank the sender anyway to ensure the mechanism isn't sent as pointless or scary.

Producing help sheets also helps people to help themselves, making them feel better about the whole process.

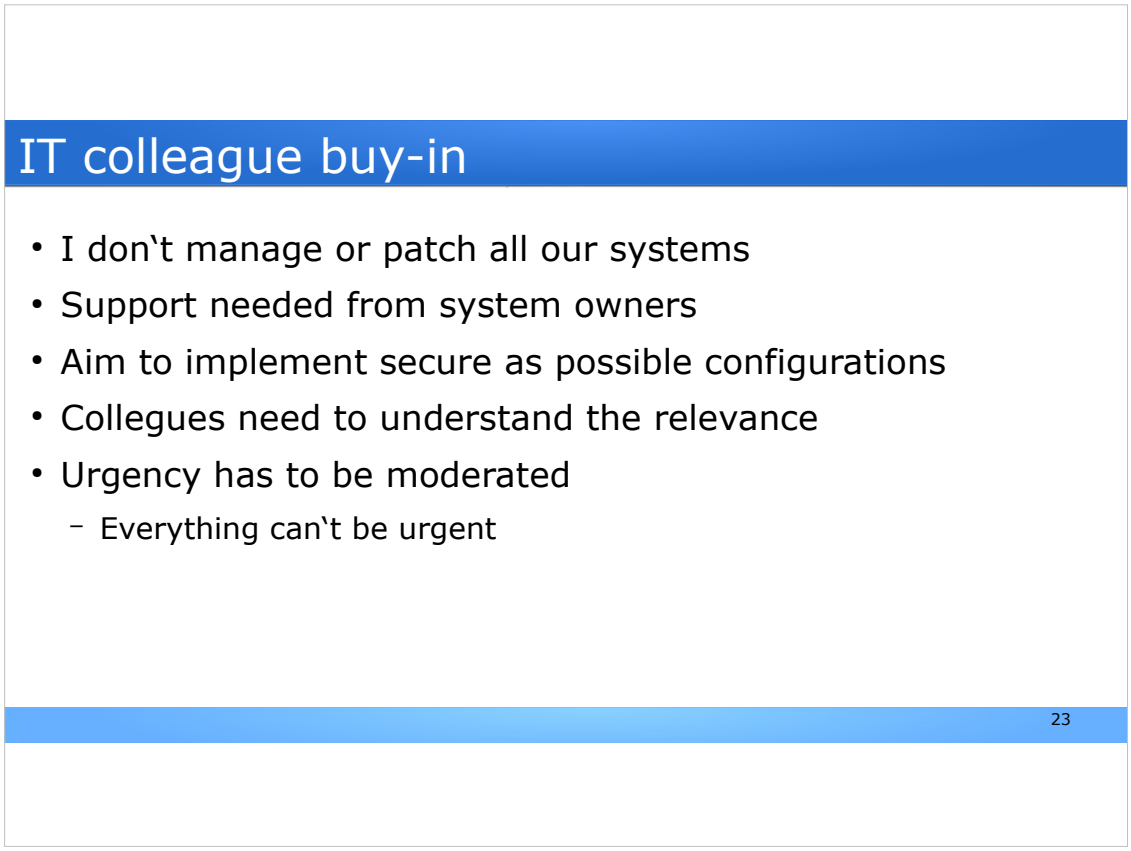


The organisation needs to realise this isn't IT's problem. Security applies to everyone, and at the end of the day its their risk and reputation.

Information Asset Owners have to be assigned to collections of data. They then have responsibility for approving, denying and removing access from colleagues. The request will still go to IT, but IT don't make the decissen.

The ideal position is where the business becomes aware of a problem and chases IT to fix it.

At the councils, we've set up a Corporate Information Governance Group that review policies and risks. Decisions are then made on how best to deal with them.



Fixing the problem often means liaising with IT colleagues. They‘ll be making a lot of the changes so it‘s important not to claim everything is an urgent priority.

Training IT colleagues to implement secure configurations from the outset will also save many hours of fixes later on. This means teaching them why the security measures help and how they‘ll have saved themselves time in the long run.

Summary

- No single solution
- Technology can‘t be successful on its own
- Bring management, colleagues and users on the journey – don‘t make them resent security
- Incidents: *when* not *if* – have a plan

Hopefully this presentation has shown how a layered approach is essential to the security of an organisation, not just local government.

At some point there will be an incident, so have a plan to help deal with it. By having worked with the end users, and other IT colleagues, incidents shouldn‘t be as drastic.

Thank you for listening

Additional links

- ICO fines Basildon Borough Council for planning application personal data leak:
  https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/05/essex-local-authority-fined-for-publishing-sensitive-personal-data-in-online-planning-documents/
- Sophos Shh/Updater-B
  https://nakedsecurity.sophos.com/2012/09/19/sshupdater-b-fsophos-anti-virus-products/
- Lincolnshire County Council hit by ransomware
  http://www.bbc.co.uk/news/uk-england-lincolnshire-35443434
- Carphone Warehouse 2018 breach
  http://www.bbc.co.uk/news/business-42637820

Clipart acknowledgments

- https://openclipart.org/detail/17394/building-1
- http://clipartx.info/detail/216806-office-building
- https://openclipart.org/detail/17308/administration
- https://openclipart.org/detail/30805/tango-go-home
- https://openclipart.org/detail/289639/defense
- https://openclipart.org/detail/36067/tango-application-certificate
-