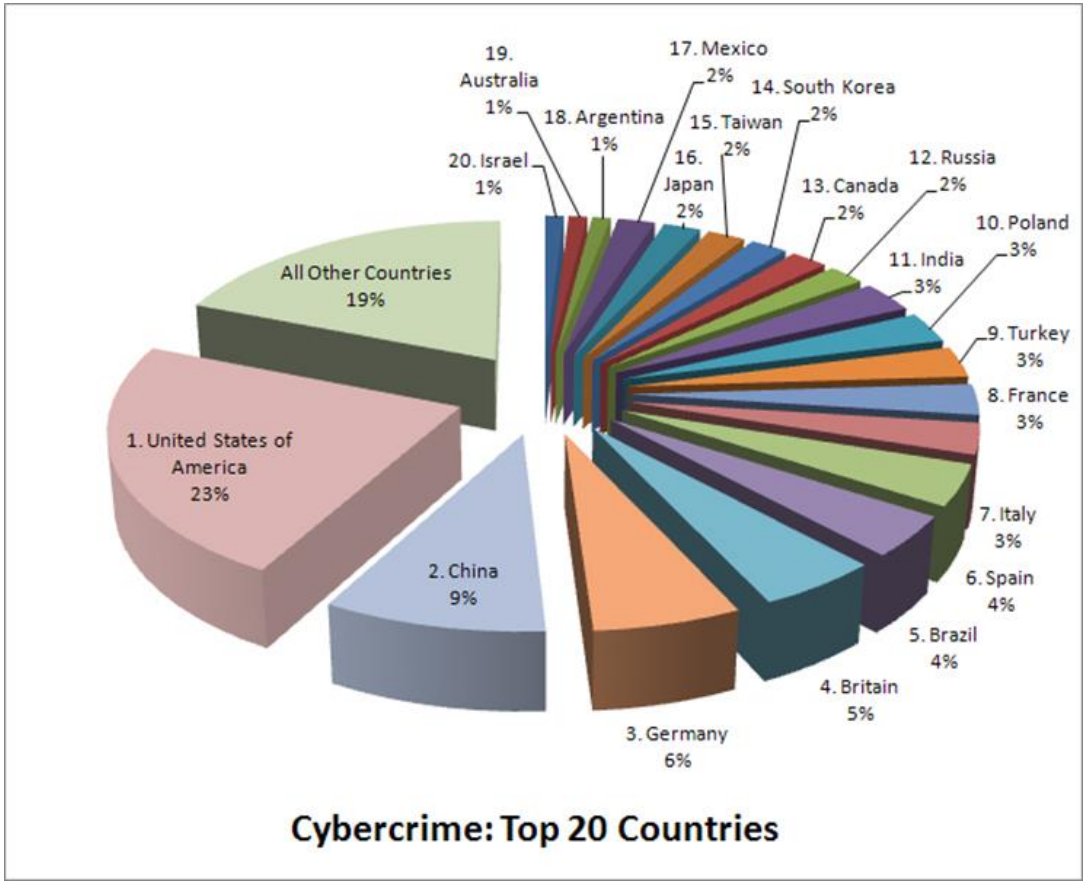
# Cyber resilience: the new normal

Alan Calder
Founder & Executive Chair
IT Governance Ltd
February 2014

www.itgovernance.co.uk

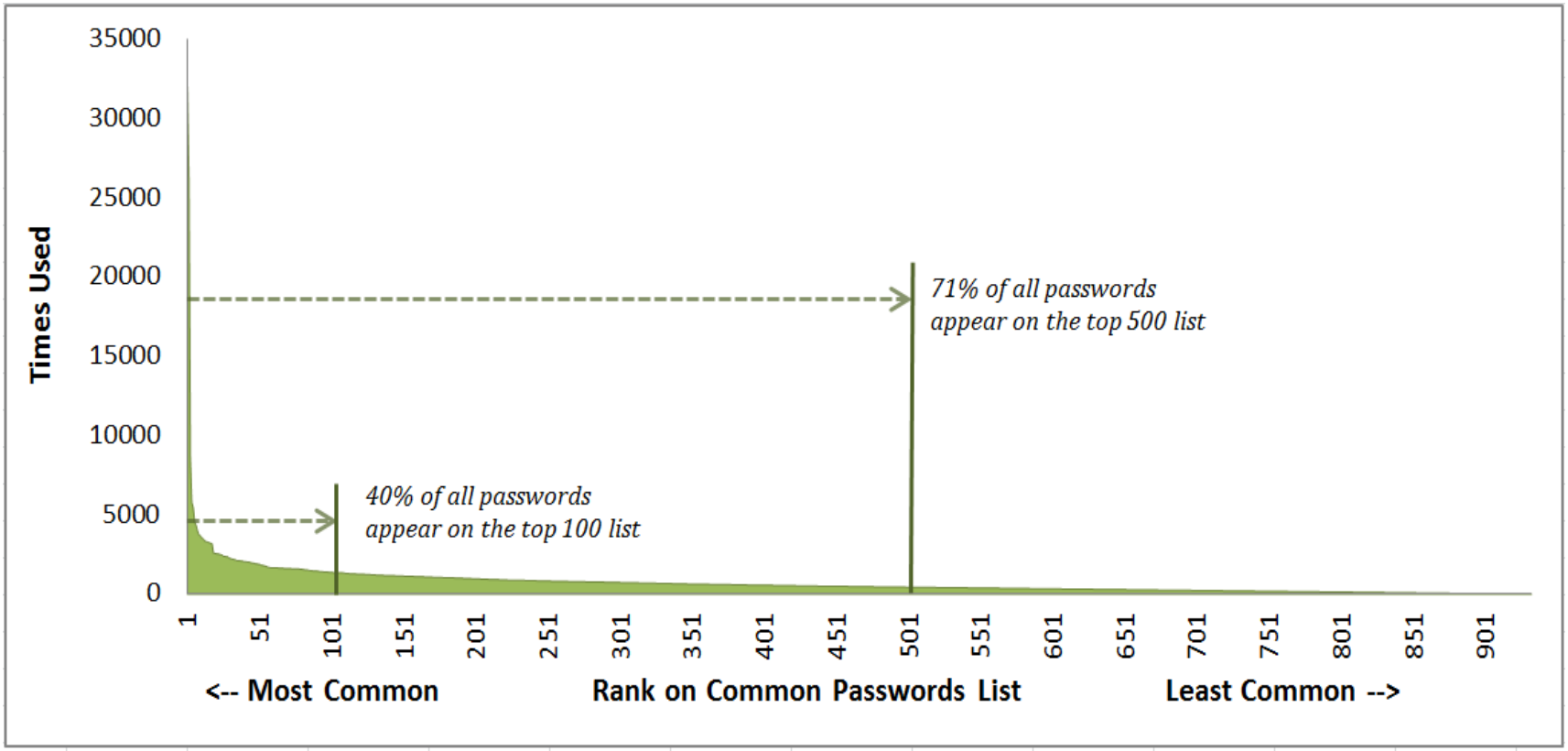
# On the Internet, where do we find security?

# Cyber crime: already widespread




**Source: BusinessWeek/Symantec**

# Passwords?




Source: https://xato.net/

# Serious Organised Crime

*"Serious organised crime groups are increasingly multi–commodity and poly-criminal in their activities, with extensive, diverse portfolios of business interests and significant collaborative activity" – Europol*

Cyber crime is:

- Lower level and more widespread than APTs
- Initially automated and indiscriminate, looking for vulnerabilities
- Sophisticated, multi-vectored
- Commercially professional – support, guarantees, etc
- Extra-territorial, extra-judicial

- Phishing, pharming, social engineering – and hacking

*PWC ISBS Breaches Survey 2012 confirms 'Cybercrime losses double in two years'*

# Assets Targeted

- Commercial information
  - Intellectual Property
  - Customer lists and related information
  - Business and commercial strategy
  - Financially sensitive information
- Data Assets
  - Banking information
  - Payment card details
  - PII (personally Identifiable Information)
  - Contact details (eg email, member lists)

***"The main loser [from cybercrime] – at a total estimated cost of £21bn – is UK business, which suffers from high levels of IP theft and industrial espionage."***

*UK Office of Cyber Security and Information Assurance - 2011*

# Computers aren't secure…

http://imediaincblog.com

- **25,000 Phones lost/stolen in London every week**
- **700,000 Handsets stolen in the UK last year**
- **Resale value of phones £10 - £60**
- **USA: 113 phones lost or stolen every minute**

# Penetrable networks & websites

Average numbers of vulnerabilities across our last 6 penetration tests

| Risk Rating Key | | |
|---|---|---|
| **Rating** | **Description** | **#** |
| **High** | The threat agent could gain full control over the system or application, or render it unusable to legitimate users. | 19 |
| **Medium** | The threat agent could gain some level of interactive control or access to data held on the system. | 26 |
| **Low** | The threat agent could gain information about the systems which could be used to facilitate further access. | 34 |
| **Info** | Informational issues. | 374 |

# Commercial Competitors?

- khalil says At 8:53:15 AM:
- i'm hacker  i stop it , because the competing other company pay me to make your site down , tell your manager now please to deal contact me on my email khalil_man1@yahoo.com
- khalil says At 8:53:25 AM:
- and check your site now i make it offline
- khalil says At 8:55:34 AM:
- or transfer me to your manager please
- Jo says At 8:57:07 AM:
- which competing company please?
- khalil says At 8:57:24 AM:
- deal with me to open your site and tell you name the other company
- Jo says At 8:57:43 AM:
- are you proud of the work you do, Khalil?
- khalil says At 8:58:02 AM:
- no

# Tutorials for Newbies:

- **Credit Card Hacking**
  CC (Credit Cards) can be hacked by two ways:
  Credit Card Scams ( usually used for earning money , some times for shopping )
  Credit Card Shopadmin Hacking ( just for fun, knowledge, shopping on internet )
  1. Shopadmin Hacking
  Shopadmins are of different companies, like: VP-ASP , X CART, etc. This tutorial is for hacking VP-ASP SHOP.
  I hope u seen whenever u try to buy some thing on internet with cc, they show u a well programmed form, very secure. They are carts, like vp-asp xcarts. Specific sites are not hacked, but carts are hacked.
  Below I'm posting tutorial to hack VP ASP cart. Now every site which use that cart can be hacked, and through their *mdb file u can get their clients 'creditcard details', and also login name and password of their admin area, and all other info of clients and comapny secrets.
  Lets start: Type: VP-ASP Shopping Cart Version: 5.00
  **How to find VP-ASP 5.00 sites?**
  Finding VP-ASP 5.00 sites is so simple...
  1. Go to google.com and type: VP-ASP Shopping Cart 5.00
  **2. You will find many websites with VP-ASP 5.00 cart software installed**
  Now let's go to the exploit..
  The page will be like this: ****://***.victim.com/shop/shopdisplaycategories.asp
  The exploit is: diag_dbtest.asp
  Now you need to do this: ****://***.victim.com/shop/diag_dbtest.asp

# Fraud as a Service

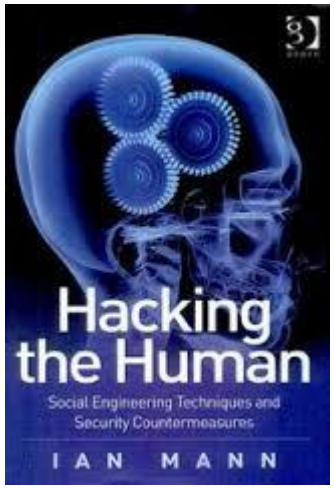
- “Citadel started as a Zeus v2 Trojan, deployed and tweaked by a crime gang using it for their own banking fraud operations, however once Citadel was released into the Russian-speaking underground in January 2012, it took on a life of its own being supported by a skillful, relentless development team.
- Today, Citadel is the most advanced crimeware tool money can buy and is the only crimeware of its grade being marketed to fraudsters in open underground venues. Comparable Trojans, like Sinowal, are all privately owned, but Citadel is taking the open market by storm and is continuing to evolve in sophistication. Since its release, Citadel has seen 4 major upgrades (including v1.3.4.5) that **addressed “customer”** concerns and fixed a long list of bugs originating in Zeus v2’s faulty mechanisms.
- An excellent example of a successful deployment of **a Fraud-as-a-Service (FaaS)** model, Citadel is the first ever crimeware to have its own **dedicated CRM** where dubious clientele can congregate, raise issues, get support and request new modules be implemented. The Citadel CRM is pushed as a compulsory part of using the Trojan, and demands a monthly fee be paid for the membership.”
- www.blogs.rsa.com

# Social Media


Source: Mombizcoach.com

*“WASHINGTON: Facebook users have demanded an apology from the social media giant for the reported leak of their email addresses and phone numbers due to a bug.”*
*(press report)*

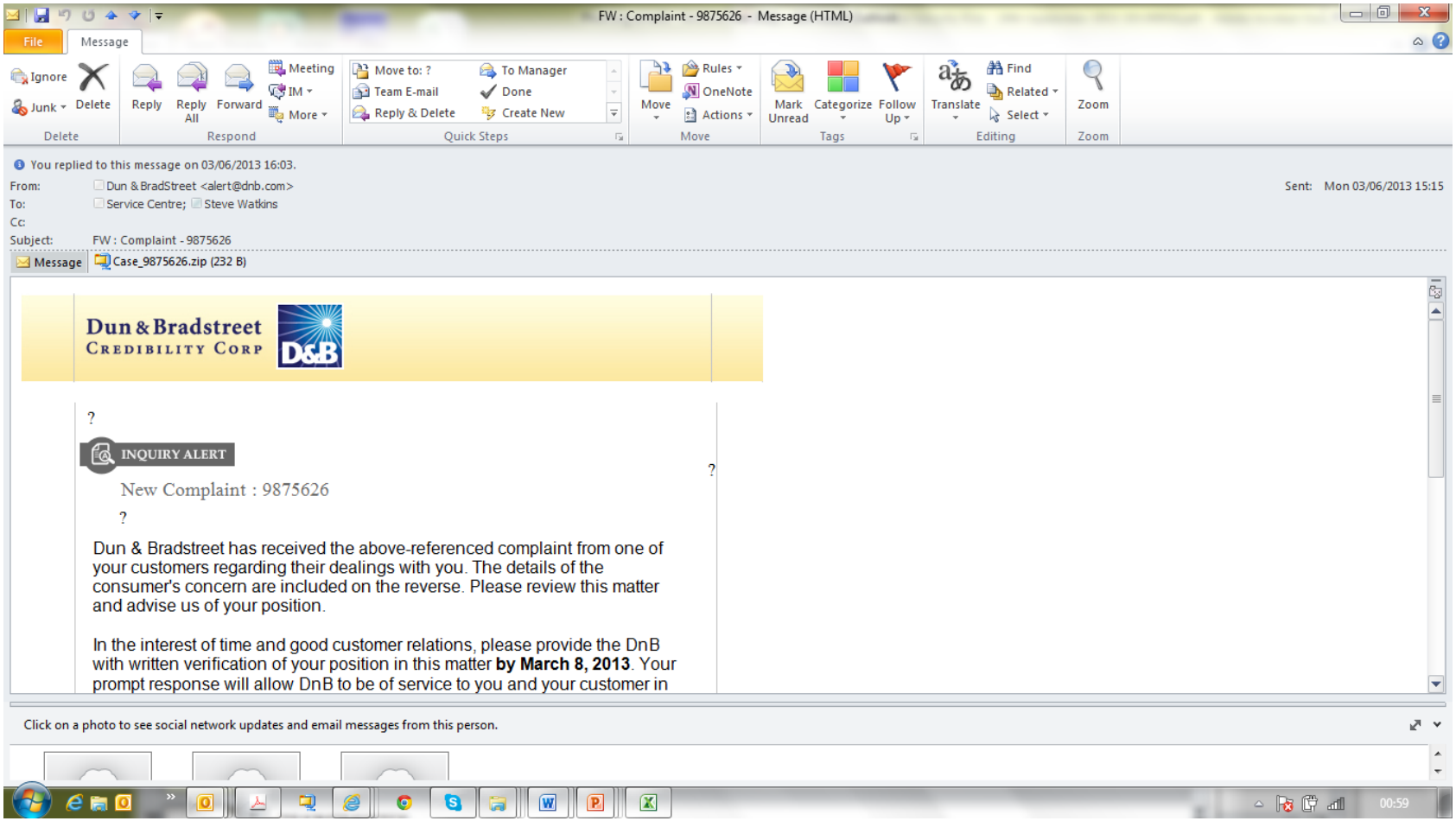
# Hacking the Human





www.trustedsec.com

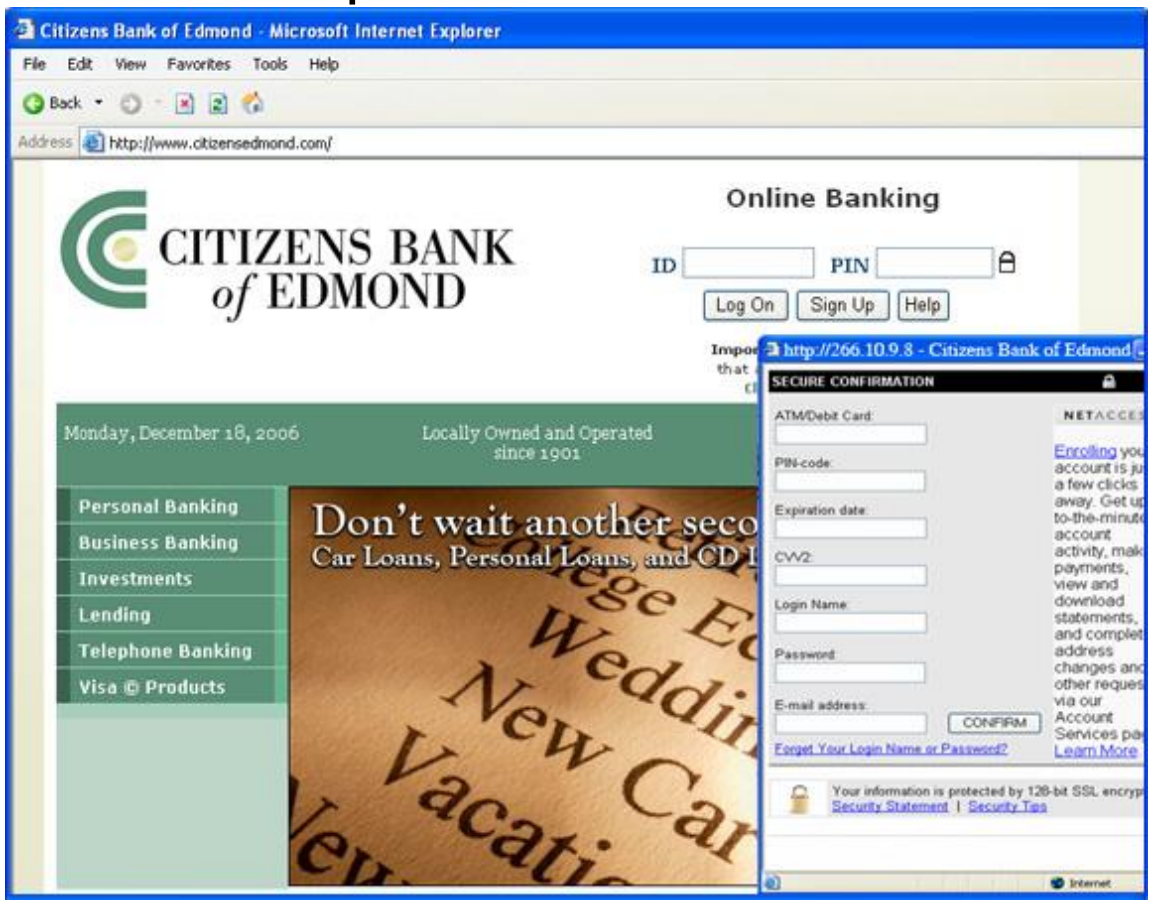
# Phishing



# Spear Phishing

# Pharming

- Malware infecting your computer
- Compromised host computer



# Cyber Insecurity

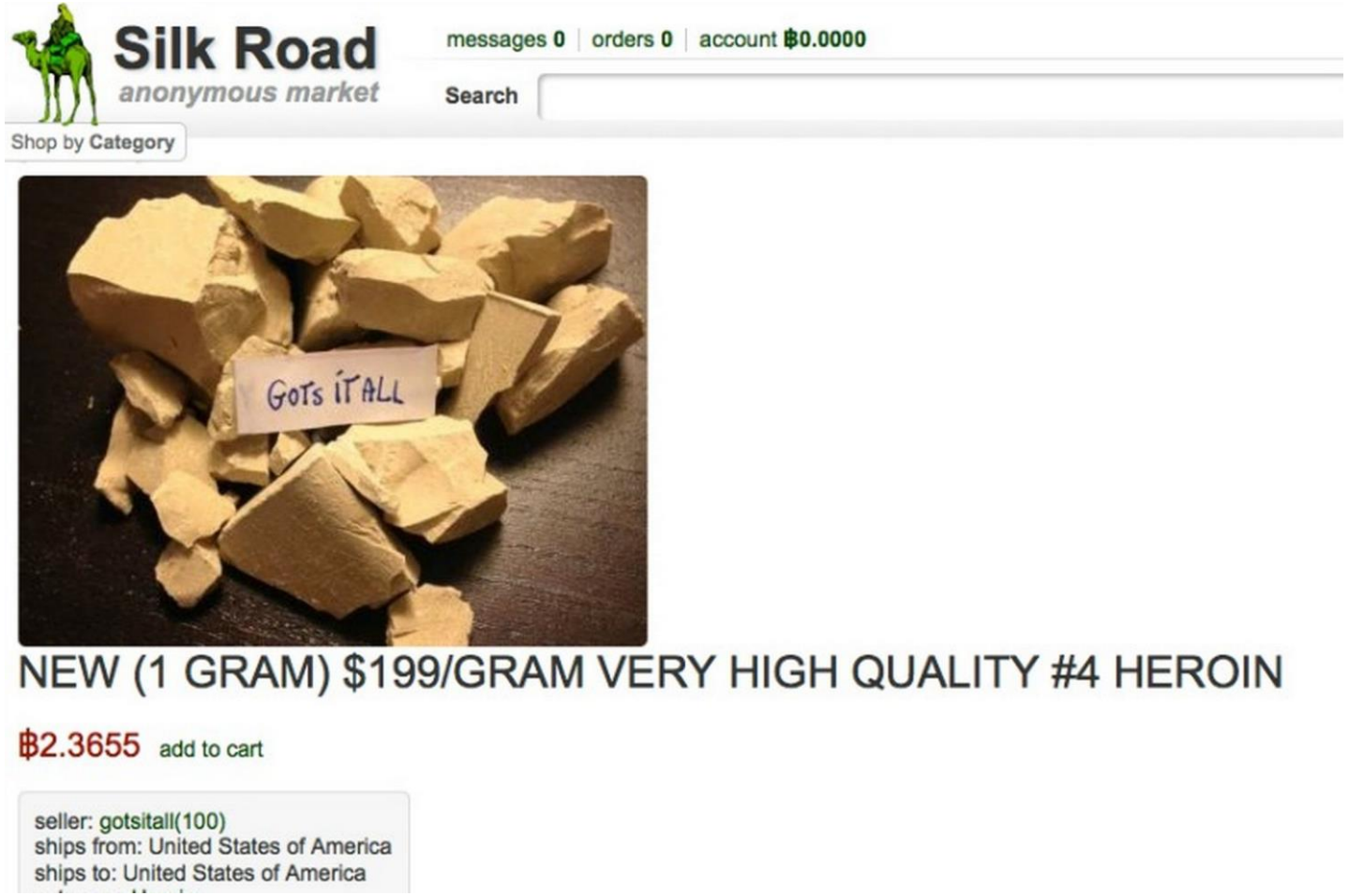
Cyberspace has no cyber cops…

- Hackers can get formal qualifications……
- Hacking, scanning, analysis, password recovery software and exploit code widely available
- Top software errors enumerated by SANS, CWE & OWASP
- And: The Internet of Things (the ‘IoT’)
  - Much greater attack surface
  - Less security
    - Home devices
    - Medical devices
    - Motor cars with 4G and Wi-fi

# Tor


https://www.torproject.org/
Tor Project: Anonymity Onl...
tor browser download
Search
Share
More
Sign In
Suggested Sites
Free Hotmail
Get more Add-ons
Customize Links
Dropbox - Files - Online b...
New PCI compliance stan...
New PCI compliance stan...
Home
About Tor
Documentation
Press
Blog
Store
Contact
Download
Volunteer
Donate
Anonymity Online
Protect your privacy. Defend yourself against network surveillance and traffic analysis.
Download Tor
Tor prevents people from learning your location or browsing habits.
Tor is for web browsers, instant messaging clients, and more.
Tor is free and open source for Windows, Mac, Linux/Unix, and Android
What is Tor?
Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.
Learn more about Tor »
Why Anonymity Matters
Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location.
Get involved with Tor »
Our Projects
Announcements
Sep 21
For most uses, Tor provides the best available protection against a well-resourced observer. It's an open question how much protection Tor (or any other existing anonymous communications tool) provides against the NSA's large-scale Internet surveillance. On its own, Tor can't protect against attacks against vulnerabilities on your computer or its software; Tor is not the only tool you need to be secure on the internet. We're working on writing clear explanations for the issues, and the state of the research field as it stands. In the meantime, Bruce Schneier's advice may be useful.
Sep 20
New Tor Browser Bundle packages with Firefox fixes. Learn what's new.
Sep 11
Tor, NSA, GCHQ, and QUICK ANT Speculation. Read our thoughts.
Cyber-thieves are behind a big leap in the number of computers connecting to the Tor anonymous web browsing system – Aug 13
Speed up browsing by disabling add-ons.
Choose add-ons
Ask me later
USB Device Not Recognized
One of the USB devices attached to this computer has malfunctioned, and Windows does not recognize it.
For assistance in solving this problem, click this
90%
00:28

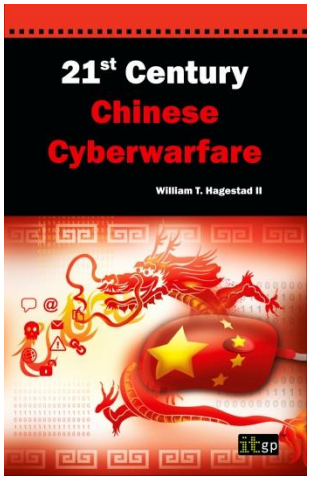
# Darknet sites



# On the Internet….

# 21st Century Chinese Cyberwarfare

- Doctrine of War Without Limits, Unrestricted Warfare
- Various cyber attacks: GhostNet, Night Dragon, Aurora, ShadyRAT




- US, UK and other industrial countries are military and commercial targets

# Why is Cyber Attack a Tier 1 Risk?

- Government and Military depend on cyber systems
- Information on which our responses to any national incident depend is stored electronically
- Critical National Infrastructure (CNI) increasingly dependent on computers, ICS and SCADA systems,
- Advanced Persistent Threats posed by state level entities
- International conflict likely to include cyberattack:
  - Stuxnet worm - US/Iran – June 2010
  - Titan Rain – China on US, multi-year from 2003
  - Cyber attacks on Estonia Russia – 2007 (Web War 1)
  - Georgia cyber attack – 2008 South Ossetia

# Advanced Persistent Threat

Co-ordinated cyber activities of state-level entities and criminals, usually with unofficial state protection, targeted on large corporations and foreign governments with the objective of stealing information or compromising information systems.

- *Advanced: sophisticated, combining multiple targeting methods, an advanced range of tools, technologies and techniques, and a wide range of channels*
- *Persistent: stealthy, continuing, multi-targeted*
- *Threat: stealing information, compromising systems and defences*

- **RSA Washington DC APT Summit 2011**

*'plan and act as though you've already been breached'*

# HMG Cyber Security Strategy

- UK National Security Strategy 2010:
  - Four high priority (Tier 1) risks:
    - International Terrorism
    - ***Cyber Attack***

- UK National Cyber Security Strategy 2011
  1. Making the UK one of the most secure places in the world to do business in cyberspace
  2. Making the UK more resilient to cyber attack and better able to protect our interests in cyberspace
  3. Helping shape an open, vibrant and stable cyberspace that supports open societies
  4. Building the UK's cyber security knowledge, skills and capability.

# EU Cyber Security Strategy

- Cyber Security Strategy of the EU: *An Open, Safe and Secure Cyberspace* (published Feb 2013)
- 5 Strategic Priorities
  - Achieve cyber resilience
  - Drastically reduce cyber crime
  - Develop cyber defence capabilities
  - Develop technical and industrial cyber security resources
  - Establish a coherent EU-wide cyberspace policy
- Proposed EU legislation to force member countries to:
  - Create national CERTs
  - Adopt a national Network and Information Security plan
  - Require key sectors to achieve minimum levels of cyber security
  - *"In particular, industry should …. make CEOs and Boards more accountable for ensuring cybersecurity."*

# We appear to be losing:

- UK – per NAO, Feb 2013:
  - 44 million cyber attacks in 2011
  - £18bn - £27 bn annual cost of cybercrime
  - ***80% could be prevented through basic security 'hygiene'***

- The PwC Information Security Breaches Survey (2012) found that
  - 93% of large corporations, and
  - 76% of small businesses had a cyber security breach in 2012.
  - The cost was estimated between £110,000-250,000 for large businesses and £15,000-30,000 for smaller

# Internationally, as well

- Verizon 2012 Data Breach Investigations Report
  - Worldwide – 855 Incidents, 174 million compromised records
    - 98% involved external agents
    - 58% of all data theft tied to activist groups
    - 81% of breaches involved hacking
    - 69% incorporated malware
    - 79% were victims of opportunity
    - 96% of attacks were not highly difficult
    - 85% of breaches took weeks to discover
    - 92% of incidents were discovered by third parties
- McAfee: Global Cyber crime cost is $300 Bn.

# The Stakes Are High!

The potential impacts of cyber attack to a business:

- Direct financial loss from theft or fraud.
- Indirect loss from recovery & remediation costs
- Loss of customer information or Intellectual Property.
- Possible fines from legal and regulatory bodies (e.g. FSA, Information Commissioner).
- Loss of reputation through ‘word of mouth’ and adverse press coverage.
- Survival of the organisation itself.

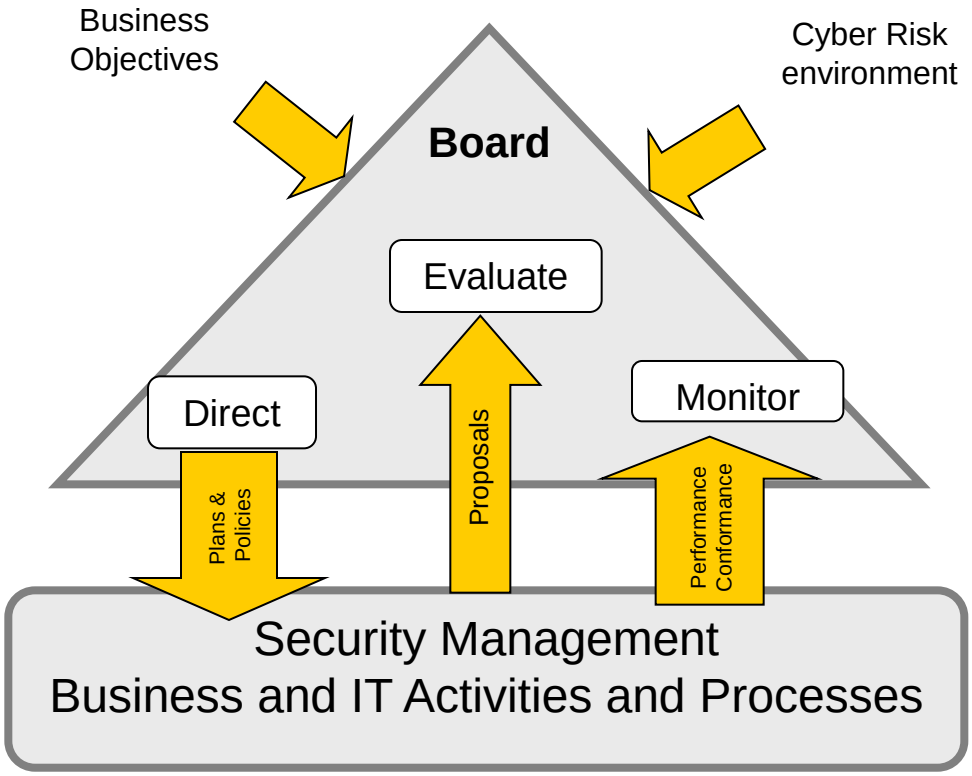
**Demands for assurance**

74% of respondents say their customers prefer dealing with suppliers with proven cyber security credentials, while 50% say their company has been asked about its information security measures by customers in the past 12 months.

# How should Chairs/CEOs respond?

## Governance of Cyber Security

"Corporate governance consists of the set of processes, customs, policies, laws and institutions affecting the way people direct, administer or control a corporation." (Wikipedia)




Management "is the act of getting people together to accomplish desired goals and objectives using available resources efficiently and effectively." (Wikipedia)

Governance ≠ Management

# Cyber resilience

- Resilience:
  - " the ability to rapidly adapt, protect assets and respond to risks…"
- Business Resilience:
  - "the ability to rapidly adapt, protect business assets, respond to business disruptions and maintain continuous business operations.."
  - Contains both BCM and DR
  - Implies mitigation capability
- Cyber-resilience
  - "the ability to repel cyber attacks while protecting critical business assets, rapidly adapting and responding to business disruptions and maintaining continuous business operations.."

# Cyber Resilience Framework

Effective cyber security depends on resilience: co-ordinated, integrated preparations for rebuffing, responding to and recovering from a wide range of possible attacks.

- A strategy is essential.
- A management system is fundamental.
- Defence, continuity, and recovery must each be provided for.
- No single stand-alone solution is sufficient.

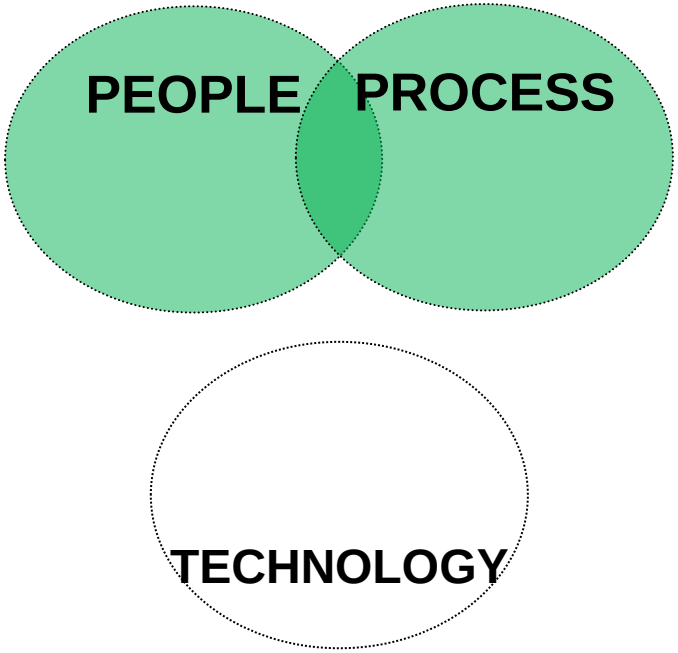
- Money will be required

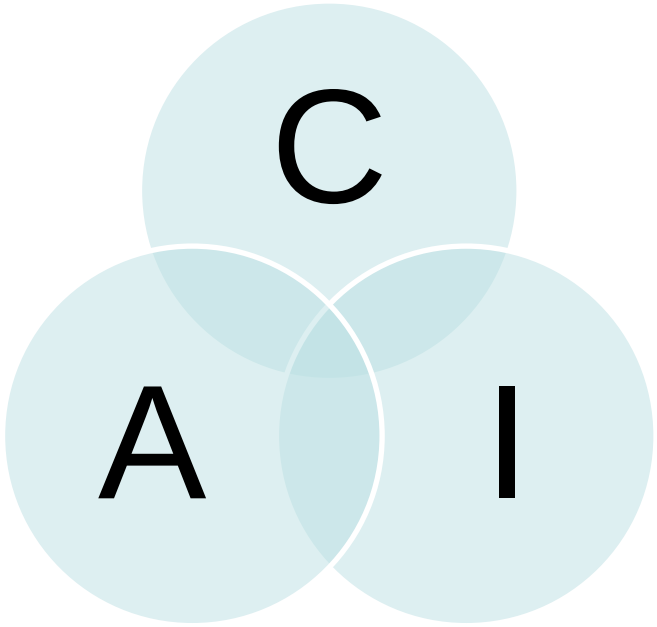
- ***80% of breaches could be prevented through basic security 'hygiene'***

# HMG & Cyber security standards

- BIS Commissioned PwC – Report Nov 2013:
  - Identified all the standards which touch in some way on cyber security
    - Organisation, Product, Personnel, Process
    - International Reach
    - Nothing excluded
- 52% of organisations implement a standard to some level
- 7/10 was average level of importance of cyber security certification
- 48% of organisations implemented new cyber security policies
- 35% of organisations plan to increase cyber security spending
- 34% of organisations plan to implement an ISMS
- 39% plan to seek external certification ‘soon’
- *“The greatest volume of support from industry was in favour of the ISO27000-series of standards, which offers a management framework for managing information security risk and is well-established, relatively widely used and internationally recognised.”*
- *CISSP, CIS LI and CIS LA qualifications most widely useful*

# Critical framework aspects




- Management–driven
- Business-focused
- Risk appetite-based
- Enterprise-orientated
- Continual improvement

# ISO27001 The Cyber Security Standard

ISO/IEC 27001, together with the international code of practice, ISO/IEC 27002, provide a globally recognised standard and best-practice framework for addressing the entire range of cyber risks

# Cyber-resilience Standards

International Best Practice Standards:

***Security defences WILL BE BREACHED, so prepare!***

- ISO/IEC 27035 - Information Security Incident Management
- ISO/IEC 27031 - Guidelines for information and communication technology readiness for business continuity
- ISO22301 – BCMS Requirements (Business Continuity Management)
- ISO/IEC 24762 – Disaster Recovery Services
- Digital Forensics Capability
- www.itgovernance.co.uk/cybersecurity-standards.aspx.

# 7 – Step Cyber-resilience Strategy

1. Integrated risk assessment, BIA
   - Assets AND Processes
2. Secure the cyber perimeter (fixed and mobile)
3. 20 Critical Security Controls
4. Train all staff – skills, competence, awareness
5. Develop and test a security incident response plan
6. Determine and test RTO capability
7. Develop and test seriously remote DR facilities

Adopt and integrate IS027001, ISO27031, ISO27035, ISO22301, ISO24762

# Secure the cyber perimeter

- Fixed:
  - Lock down server & device configurations
  - Regular vulnerability scans (network and website)
  - Regular penetration tests (internal & external)
- Mobile (including BYOD):
  - Mobile device encryption
  - Central policy control
  - Mobile VPN
- Review ISO/IEC 27032 – Guidelines for Cybersecurity

# 20 Critical Security Controls SANS: CSIS

- Critical Control 1: Inventory of Authorized and Unauthorized Devices
- Critical Control 2: Inventory of Authorized and Unauthorized Software
- Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Critical Control 4: Continuous Vulnerability Assessment and Remediation
- Critical Control 5: Malware Defenses
- Critical Control 6: Application Software Security
- Critical Control 7: Wireless Device Control
- Critical Control 8: Data Recovery Capability
- Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
- Critical Control 12: Controlled Use of Administrative Privileges
- Critical Control 13: Boundary Defense
- Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
- Critical Control 15: Controlled Access Based on the Need to Know
- Critical Control 16: Account Monitoring and Control
- Critical Control 17: Data Loss Prevention
- Critical Control 18: Incident Response and Management
- Critical Control 19: Secure Network Engineering
- Critical Control 20: Penetration Tests and Red Team Exercises
- www.itgovernance.co.uk/20-critical-controls-consensus-audit-guidelines.aspx

# Incident Management

- Integrate cyber incident management with helpdesk event & incident management
- Robust, tested processes and assigned responsibilities
  - Detect, report and assess cyber security incidents
  - Respond to and manage cyber security incidents
  - Detect, assess and manage cyber vulnerabilities
  - Continuously improve cyber incident management through testing and learning
- Review ISO/IEC 27035 - Information Security Incident Management

# ICT Continuity

- BIA must consider
  - Zero hour attacks
  - internal skills and competences when responding to an outage
  - Linked system dependencies
  - Dynamic nature of data
  - Real costs of disruption – time, reputation, customers, investors
  - Cloud-based dependencies
- RTOs – Recovery Time Objectives
  - Rehearsal and testing essential
  - Regular reviews and updates – changes to technology, skills, threats, vulnerabilities
- Simultaneous physical disruptions

# Cloud Discontinuity

- Cloud can provide solutions – but can also create its own problems>
  - "Amazon EC2 has experienced a couple of outages form the same datacenter, "…one, in late June, was sparked by a violent thunderstorm which cut power, setting up a chain of events that put many Amazon customers offline for hours." A lightning strike, or any other sort of weather event, should NOT take out a datacenter." www.zdnet.com
  - "*We are experiencing an availability issue in the West Europe sub-region, which impacts access to hosted services in this region. We are actively investigating this issue and working to resolve it as soon as possible. Further updates will be published to keep you apprised of the situation. We apologize for any inconvenience this causes our customers."* Microsoft Windows Azure, quoted by www.zdnet.com
- Other hosted providers also have outages
- Your cyber-continuity plans must take account of this
  - Supplier certifications
  - Alternative hosting options/failover

# Business Continuity

- Integrate digital and analogue continuity planning
- ISO22301 the international specification
- Certification scheme
- What about your supply chain?

# What will it cost?

The average global cost of a data breach was **$136 (£90) per record** in 2012 [Ponemon Institute / Symantec].

Data breach costs were estimated at between £110,000-250,000 for large businesses and £15,000-30,000 for smaller – per breach (PwC Survey 2012)

**What damage will you suffer in 2013?**

**What would it be worth investing to protect the organisation?**

# Investment required

- Average company spends 6% of IT budget on IT security
- The benchmark: 13%
- 2010 Cyber Security Watch Survey
  - CSO Magazine, US Secret Service, CERT, Deloitte's Security Centre
  - Increase in number of incidents but decline in severity
    - 42% increase in IT security spending
    - 86% increase in corporate/physical security spending
- ESG Survey 2011
  - APTs will cause increases in security expenditure of between 6% and more than 10%.

# Cyber Health Check: Building the Case for Cyber Health

- Two day basic health check – on site and remote
- Four steps: Identify, Audit, Analyse, Recommend

# Identify Cyber Risks

1. Identify
   - Risks (likelihood and impact)
     - Key digital assets, including PII
     - Key, relevant (primarily cyber) risks
     - Risk Stance (cautious……aggressive)
     - Legal, regulatory, contractual issues (incl privacy and DPA)
   - Planned response
     - Policies (reference ISO27001/27002 and other standards)
     - Competences
     - Business requirements for ISM

# Heath Check – Audit & Analyse

2. Audit
   - Policy deployment
   - Wireless security
   - Remote vulnerability scans – websites and Internet connections
   - Online staff questionnaire
3. Analyse
   - Gaps between targeted risk mitigation and reality
     - Processes
     - People
     - Technology

# Health Check – Prioritised Recommendations

4. Prioritise
   - Prioritised action list
   - High level cost-benefit analysis
   - Contextualised for ISO27001
   - Next steps

   - For an SMB (Small or Medium Business) up to 500 staff: only £2.5k for the Cyber Health Check.

# Questions and Answers

acalder@itgovernance.co.uk

**0845 070 1750**

www.itgovernance.co.uk

www.itgovernanceusa.com

www.itgovernance.eu

www.itgovernance.asia

www.itgovernance.in

# Question & Answer
# WORKSHOP