

Q3 – 2016 ‘Security Matters’ Forum



Cyber Security and Data Protection: Huge Penalties, Nowhere to Hide

Alan Calder
Founder & Executive Chair
IT Governance Ltd
July 2016



© IT Governance Ltd 2014

Introduction

- Alan Calder
- Founder – IT Governance Ltd
- *IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002, 6th Edition* (Open University textbook)
- www.itgovernance.co.uk/shop/p-772-it-governance-an-international-guide-to-data-security-and-iso27001iso27002.aspx

IT Governance Ltd: GRC One-Stop-Shop



© IT Governance Ltd 2014



www.itgovernance.co.uk

Agenda



© IT Governance Ltd 2014

- Today's cyber threat environment
- EU GDPR
- Cyber Assurance

What's Really Going On?

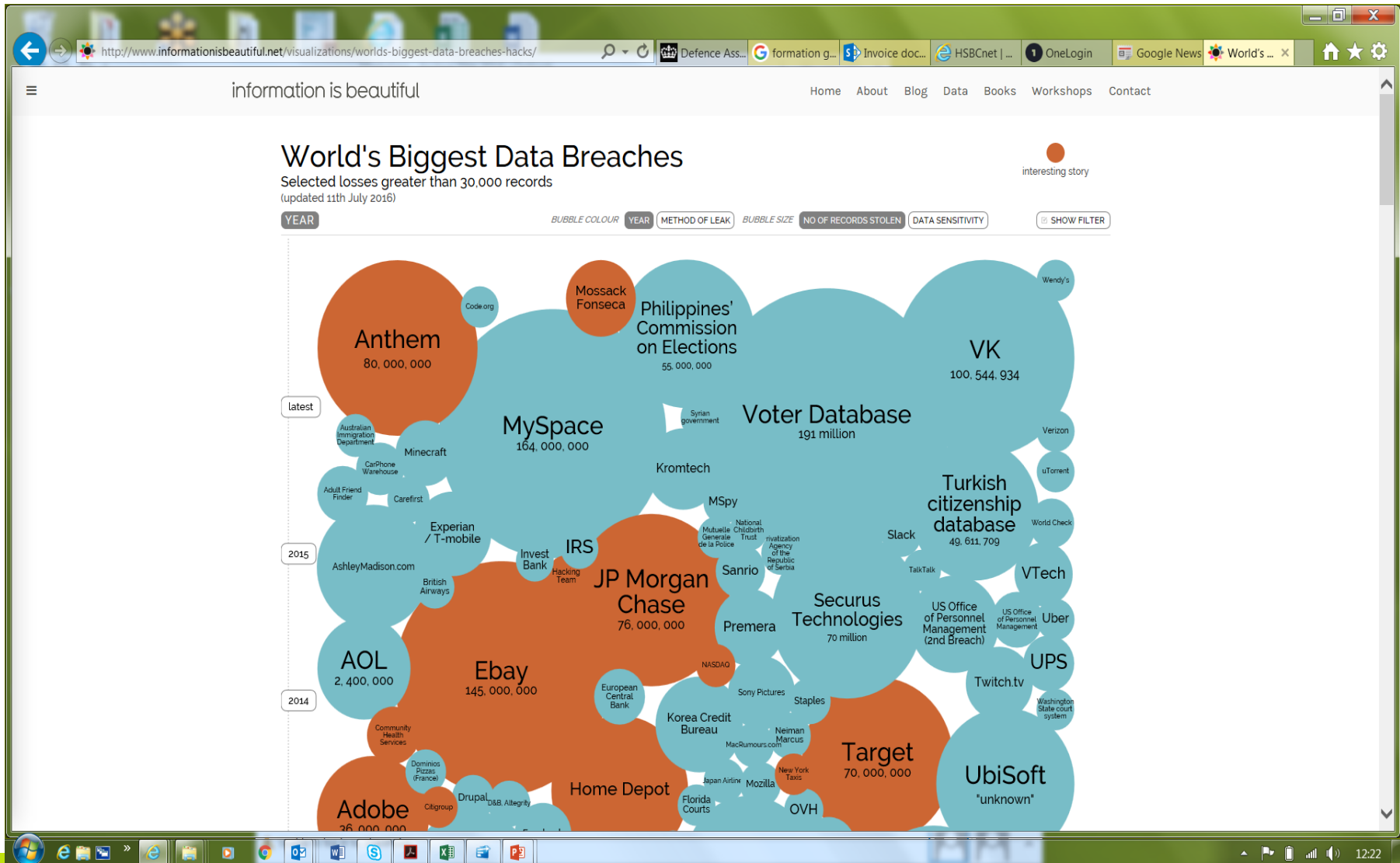


© IT Governance Ltd 2014



Massive data breaches

- www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



Cyber Risks for all



© IT Governance Ltd 2014

- Digital Information is at the heart of cyber crime
 - Key assets at risk:
 - High Value Research – eg energy technology, biotechnology, advanced engineering
 - Politically/commercially sensitive data – eg product development, climate modelling, testing data
 - Sensitive internal information: eg PII (customers and staff), financial data (eg bank accounts, payment card data, identity theft)
 - Key challenges:
 - Balancing openness with security
 - Devolved data management responsibilities
 - Multiple, mobile and remote access connection requirements
 - Complex data lifecycles
 - Rapid technology evolution

Security breach levels are rising



© IT Governance Ltd 2014

Security breach levels continue to rise. Last year in the UK:

- 90% of large organisations reported suffering a security breach, up from 81% a year before.
- 74% of small businesses had a security breach, up from 60% a year before.

Source: BIS/PwC 2015 Information Security Breaches Survey

Cost of cyber crime is rising



© IT Governance Ltd 2014

The average cost of a data breach for businesses in the UK is £2.37 million.

Source: IBM/Ponemon Institute 2015 Cost of Data Breach Study: United Kingdom

Hacking the Human



© IT Governance Ltd 2014

Phishing, Spear Phishing



95% of insider breaches were found to be the result of human error, such as clicking on malicious links in phishing emails.

Cryptolocker & Ransom-ware



© IT Governance Ltd 2014



Self-installs

- Phishing emails
- Compromised websites
- Existing malware

Can Encrypt:

- shared network drives,
- USB drives,
- external hard drives,
- network file shares,
- some cloud storage drives

Cost of Decryption Key: €300 – or 2 Bitcoins

Cryptolocker – 240,000 infected computers since Oct 2013
£16 million in ransoms.....

GameOverZeus – steals online banking passwords
\$100 million of income...

Small Businesses are Popular with Hackers



© IT Governance Ltd 2014

- Many small businesses are on shared servers. This multiplies the potential access points for a hacker to exploit.
- Small to mid-size businesses usually don't have an IT department that keeps server hardware and software up-to-date.
- Website versions and plug-ins are often out-of-date and easily hacked.
- Small to mid-size companies usually don't have internal security practices, so passwords and access are easily compromised.
- Small business websites are often built on common, open-source frameworks. These frameworks are popular to hackers because there are so many and the same weaknesses can be exploited across all of them.
- (Executionists Blog)

The Stakes Are High!



© IT Governance Ltd 2014

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.

Cyber Security Strategy

- Devolved cyber risk model, with appropriate board oversight
- Clear, centrally-defined security policies
 - With monitoring and oversight
 - And budgets
- Segmented networks
- Risk-based approach to mobile and remote access options
- Risk-based approach to technology deployments
- Good cyber security practices
 - Access control policies – and technology infrastructure
 - Cyber security awareness training
 - Rapid vulnerability patching
 - Perimeter and end-point security
- Integrated security and compliance management systems
- Data breach response capability – tried and tested

What can you do to stay safe: Cyber Essentials Scheme



© IT Governance Ltd 2014

1. Boundary Firewalls & Internet Gateways
2. Secure Configuration
3. Access Control
4. Malware Protection
5. Patch Management

These are the five basic controls that any organization should implement to mitigate the risk from common internet-borne threats.

ONLY £300



Cyber Essentials vs Cyber Essentials Plus



© IT Governance Ltd 2014

Cyber Essentials:

- *Self Assessment Questionnaire*
- *Attestation of Compliance*
- *External vulnerability scan*

Cyber Essentials Plus

- *As for Cyber Essentials, plus*
- *Onsite test of device configurations*

Independent Certification
CREST-accredited





© IT Governance Ltd 2014

Cyber Essentials Benefits

- Increase your resistance to cyber threats
- Focus on core business objectives, knowing that you're protected from the vast majority of common cyber attacks
- Drive business efficiency, save money and improve productivity through the streamlining of processes
- Reduce insurance premiums
- Demonstrate to clients, insurers, investors and other interested parties that you have taken the precautions necessary to reduce common cyber risks
- Work within supply chain information security risk management expectations
- Meet UK Government requirements that involve the handling of personal and sensitive information

EU GDPR




© IT Governance Ltd 2014

**What the new
EU GDPR
means in 1 minute**


The EU GDPR will increase privacy for individuals and give regulatory authorities greater powers to take action against businesses that breach the new laws.
Here's what it means for your business:

Tough penalties:
fines of up to

4% of annual global revenue
or
€20 million,
whichever is **greater.**

A black silhouette of a scale with a green bag on top, representing the financial penalties of the GDPR.

The regulation also applies to **non-EU companies** that process personal data of individuals in the EU.

A world map with blue arrows indicating data flow between continents, representing the global reach of the regulation.

Complete overhaul of data protection framework

Covers all forms of PII, including biometric, genetic and location data

Applies across all member states of the EU

In force from May 2018

GDPR – Data Breaches



© IT Governance Ltd 2014

- ***Mandatory data breach reporting – within 72 hours***
 - Describe actions being taken to
 - Address the breach
 - Mitigate the consequences
 - Data subjects contacted ‘without undue delay’
 - Unnecessary if appropriate protection is already in place
 - Consider encryption for all mobile devices, for all databases, and for email
 - Penetration testing to identify potential attack vectors should be standard
- Failure to report within 72 hours must be explained

Cyber Security Assurance



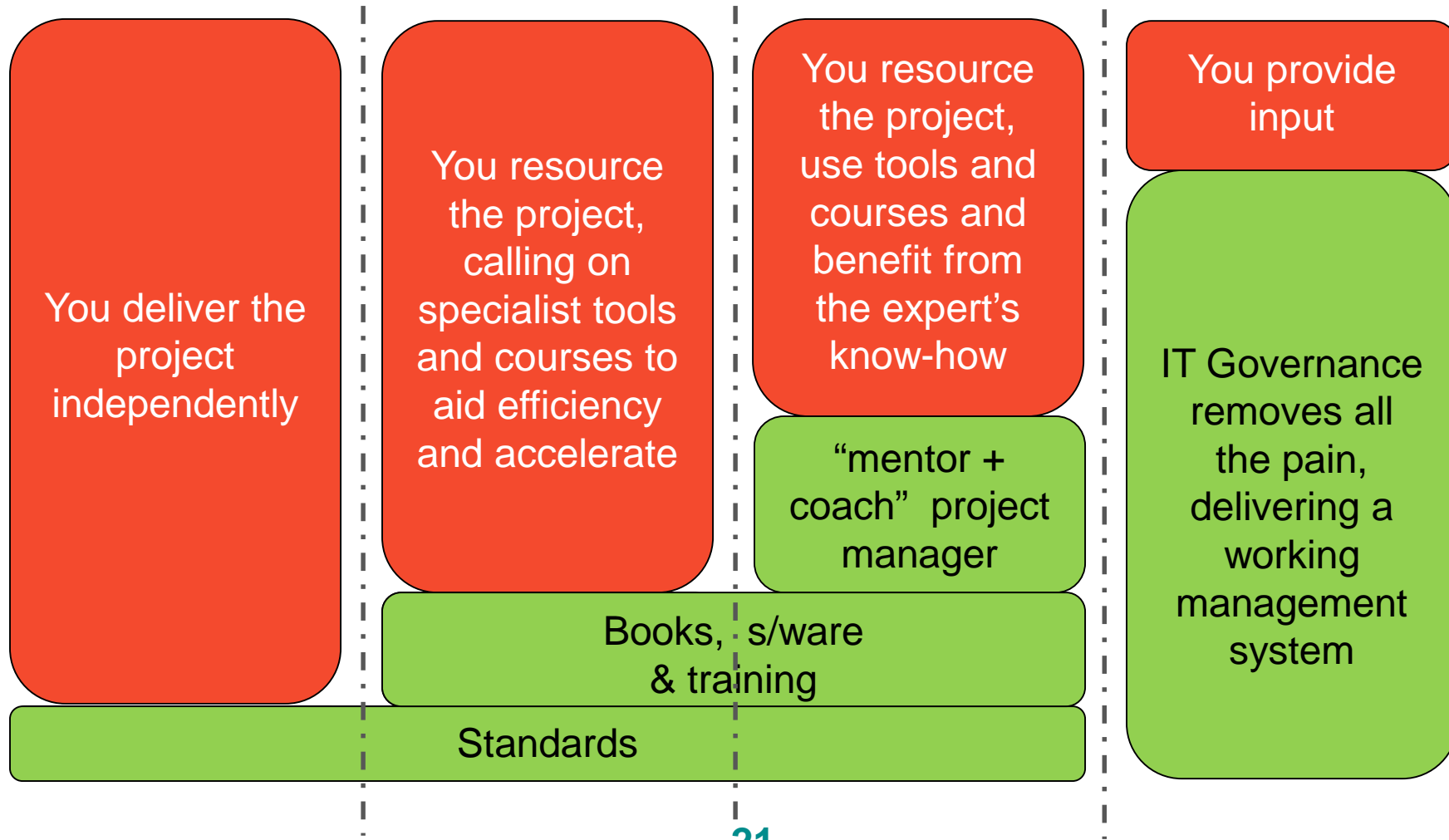
© IT Governance Ltd 2014

- GDPR requirement - data controllers must implement:
 - *“appropriate technical and organizational measures to ensure and to be able to demonstrate that the processing is performed in accordance with the regulation.”*
 - Must include appropriate data protection policies
 - Organizations may use adherence to approved codes of conduct or management system certifications “as an element by which to demonstrate compliance with their obligations”
- ISO 27001 already meets the “appropriate technical and organizational measures” requirement
- It provides assurance to the board that data security is being managed in accordance with the regulation
- It helps manage ALL information assets and all information security within the organization – protecting against ALL threats

Cyber Security Support Options



© IT Governance Ltd 2014



IT Governance: One-Stop-Shop

- Cyber Essentials
 - Cyber Essentials certification packages: DIY, Get a Little Help, Get a Lot of Help
 - Cyber Health Check
- GDPR
 - Pocket Guide and implementation manual
 - Documentation Toolkits
 - Certified Foundation & DPO training – managers and DPOs, & online awareness
 - Consultancy – Transition, data audits and DPIAs
- Penetration Testing
 - Internal, external, wireless security
- ISO 27001 Packages – fixed price and bespoke,
- All accessible via www.itgovernance.co.uk



© IT Governance Ltd 2014

Questions?

acalder@itgovernance.co.uk

0845 070 1750

www.itgovernance.co.uk