NIS, GDPR and Cyber Security: Convergence of Cyber and Compliance Risk

Tony Drewitt – Head of Consultancy
IT Governance Ltd
www.itgovernance.co.uk

IT Governance Ltd: GRC One-Stop-Shop

Thought Leaders
Specialist publisher

Implementation toolkits

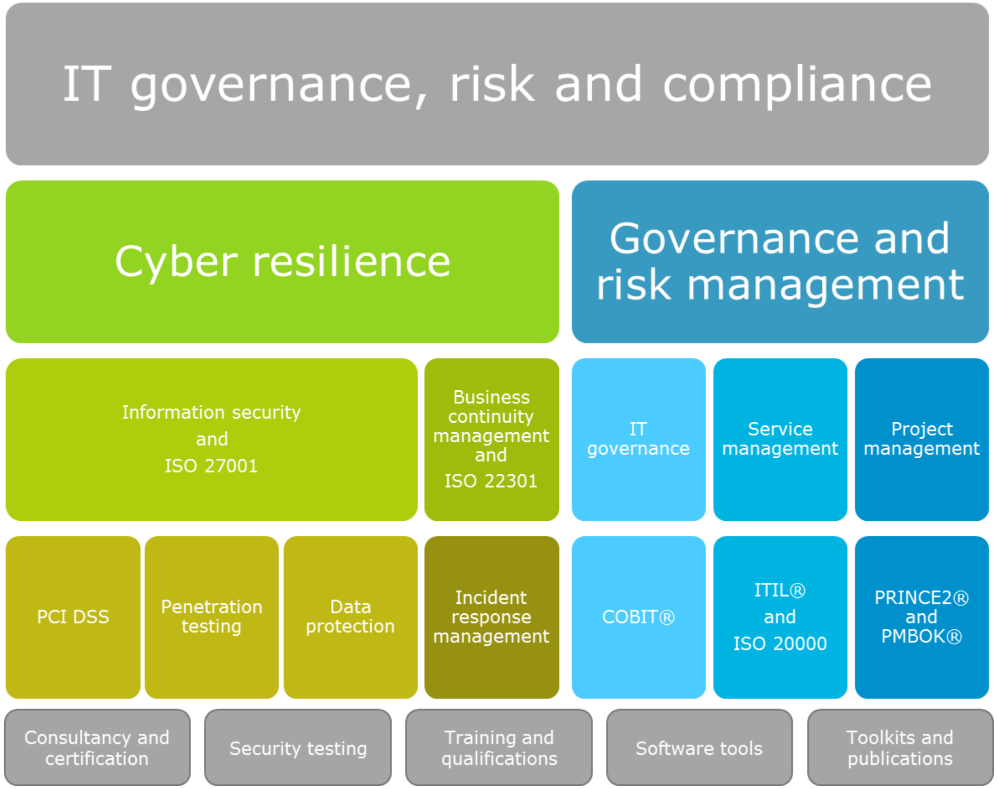
ATO

Consultants

Software and e-learning

IEC

Distribution



IT governance, risk and compliance

Cyber resilience

Governance and risk management

Information security and ISO 27001

Business continuity management and ISO 22301

IT governance

Service management

Project management

PCI DSS

Penetration testing

Data protection

Incident response management

COBIT®

ITIL® and ISO 20000

PRINCE2® and PMBOK®

Consultancy and certification

Security testing

Training and qualifications

Software tools

Toolkits and publications

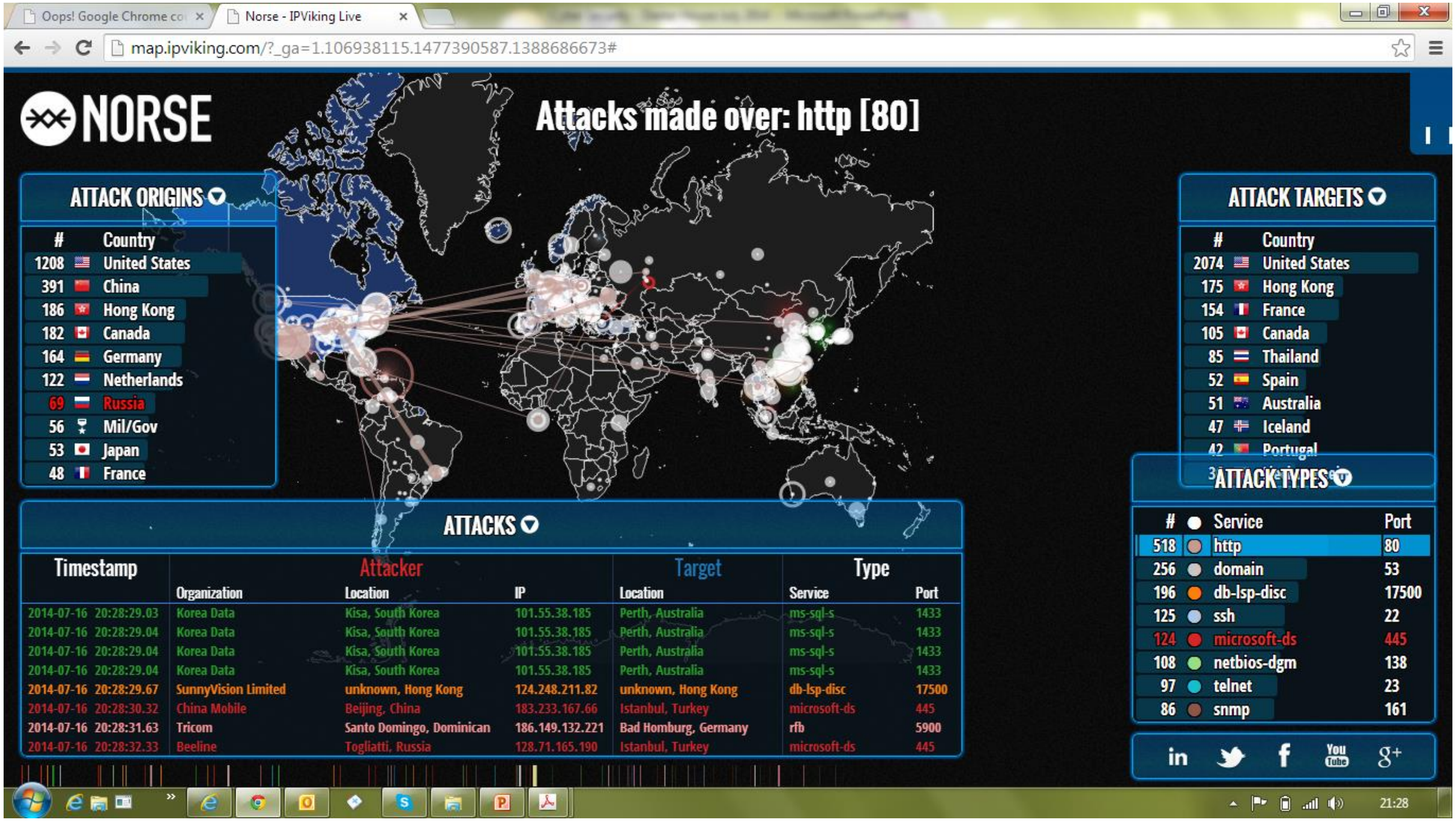
Point solutions that integrate……

APMG-International ISO/IEC 20000 · bcs The Chartered Institute for IT · IBITGQ Certifying Competence · CYBER ESSENTIALS · PCI Security Standards Council QUALIFIED SECURITY ASSESSOR · CREST · CYBER ESSENTIALS PLUS · ISO 9001 CERTIFICATION EUROPE · ISO 27001 CERTIFICATION EUROPE

Agenda

- Today’s cyber threat environment
- EU GDPR
- NIS
- Cyber Assurance

What’s Really Going On?



Attacks made over: http [80]

ATTACK ORIGINS

#	Country
1208	United States
391	China
186	Hong Kong
182	Canada
164	Germany
122	Netherlands
69	Russia
56	Mil/Gov
53	Japan
48	France

ATTACK TARGETS

#	Country
2074	United States
175	Hong Kong
154	France
105	Canada
85	Thailand
52	Spain
51	Australia
47	Iceland
42	Portugal

ATTACK TYPES

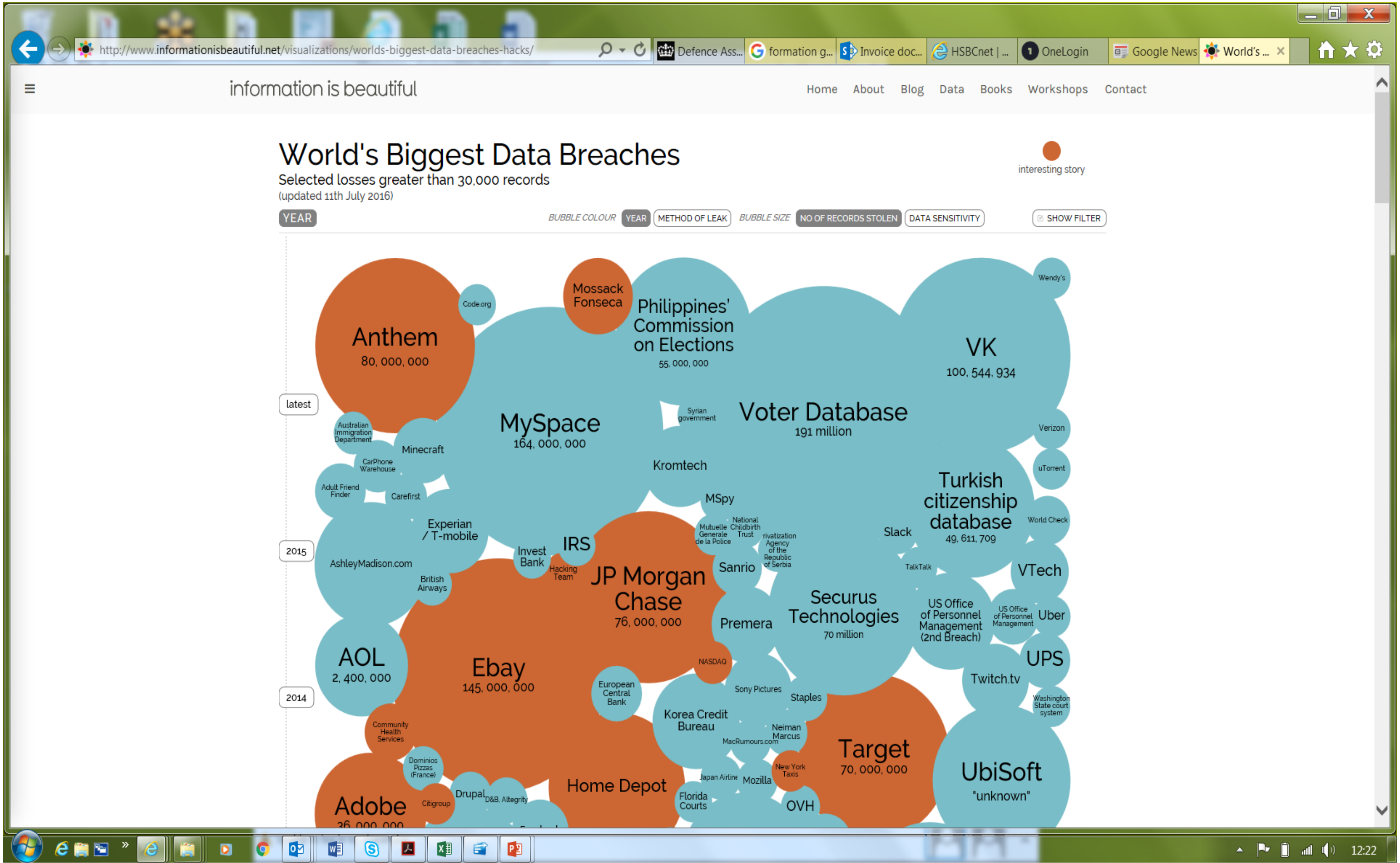
#	●	Service	Port
518	●	http	80
256	●	domain	53
196	●	db-lsp-disc	17500
125	●	ssh	22
124	●	microsoft-ds	445
108	●	netbios-dgm	138
97	●	telnet	23
86	●	snmp	161

ATTACKS

Timestamp	Attacker			Target	Type	
	Organization	Location	IP	Location	Service	Port
2014-07-16 20:28:29.03	Korea Data	Kisa, South Korea	101.55.38.185	Perth, Australia	ms-sql-s	1433
2014-07-16 20:28:29.04	Korea Data	Kisa, South Korea	101.55.38.185	Perth, Australia	ms-sql-s	1433
2014-07-16 20:28:29.04	Korea Data	Kisa, South Korea	101.55.38.185	Perth, Australia	ms-sql-s	1433
2014-07-16 20:28:29.04	Korea Data	Kisa, South Korea	101.55.38.185	Perth, Australia	ms-sql-s	1433
2014-07-16 20:28:29.67	SunnyVision Limited	unknown, Hong Kong	124.248.211.82	unknown, Hong Kong	db-lsp-disc	17500
2014-07-16 20:28:30.32	China Mobile	Beijing, China	183.233.167.66	Istanbul, Turkey	microsoft-ds	445
2014-07-16 20:28:31.63	Tricom	Santo Domingo, Dominican	186.149.132.221	Bad Homburg, Germany	rfb	5900
2014-07-16 20:28:32.33	Beeline	Togliatti, Russia	128.71.165.190	Istanbul, Turkey	microsoft-ds	445

Massive data breaches

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



information is beautiful

Home About Blog Data Books Workshops Contact

World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 11th July 2016)

Cyber Risks for all

- Digital Information is at the heart of cyber crime
  - Key assets at risk:
    - High Value Research – e.g. energy technology, biotechnology, advanced engineering
    - Politically/commercially sensitive data – eg product development, climate modelling, testing data
    - Sensitive internal information: e.g. 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

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

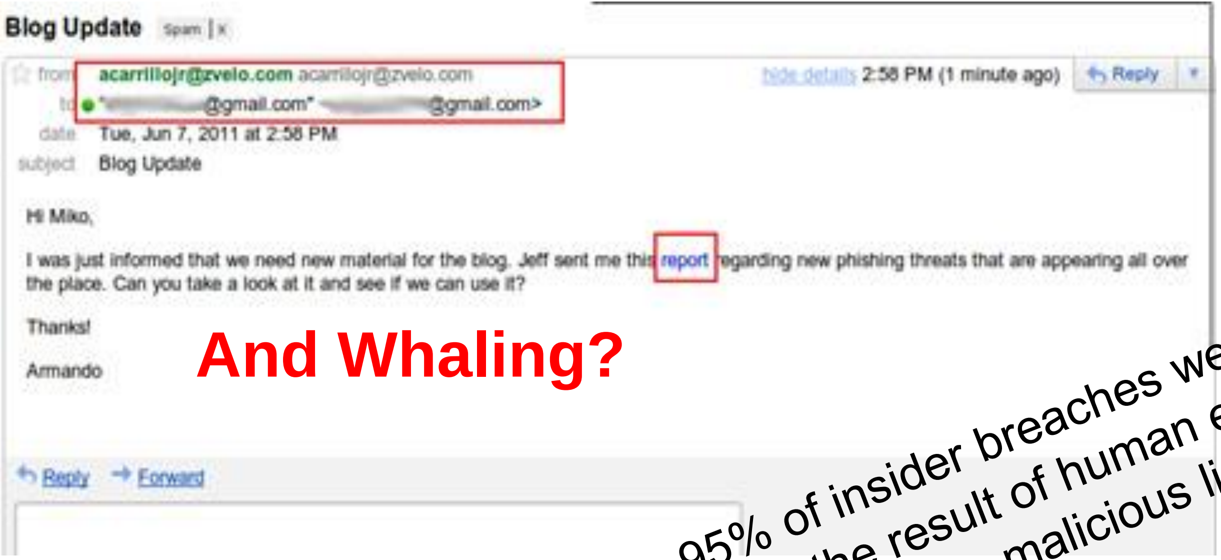
Cost of cyber crime is rising

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

Phishing, Spear Phishing



Blog Update Spam | x

from **acarrillojr@zvelo.com** acarrillojr@zvelo.com

to "[redacted]@gmail.com" [redacted]@gmail.com>

date Tue, Jun 7, 2011 at 2:58 PM

subject Blog Update

Hi Miko,

I was just informed that we need new material for the blog. Jeff sent me this report regarding new phishing threats that are appearing all over the place. Can you take a look at it and see if we can use it?

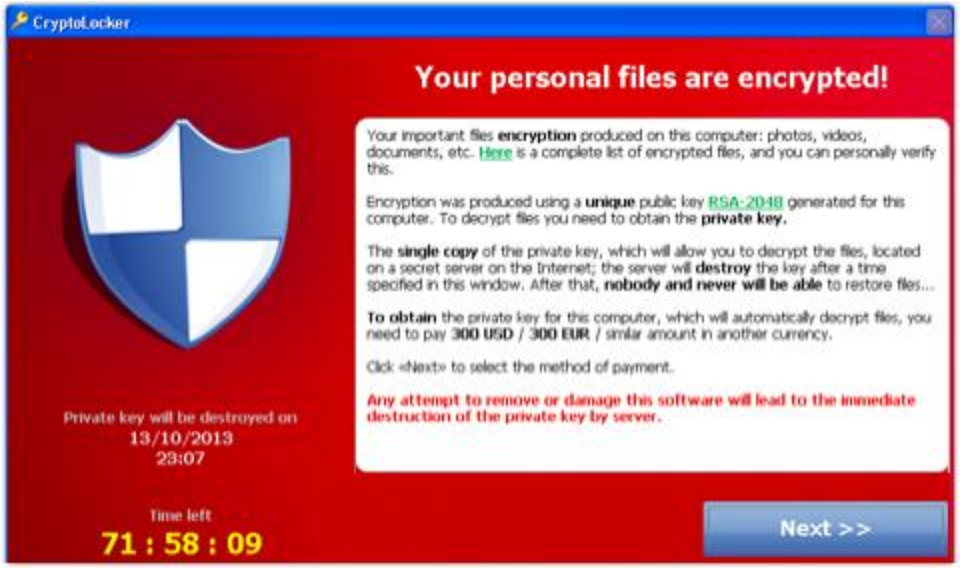
Thanks!

Armando

And Whaling?

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



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
13/10/2013
23:07

Time left
71 : 58 : 09

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

- Many are on shared servers - multiple potential access points for a hacker to exploit.
- Many 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.
- Often no internal security practices, so passwords and access are easily compromised.
- Websites are often built on common, open-source frameworks, popular amongst hackers

The Stakes Are High!

The potential impacts of cyber attack to a business:

- Direct financial loss from theft, fraud or loss of production
- 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

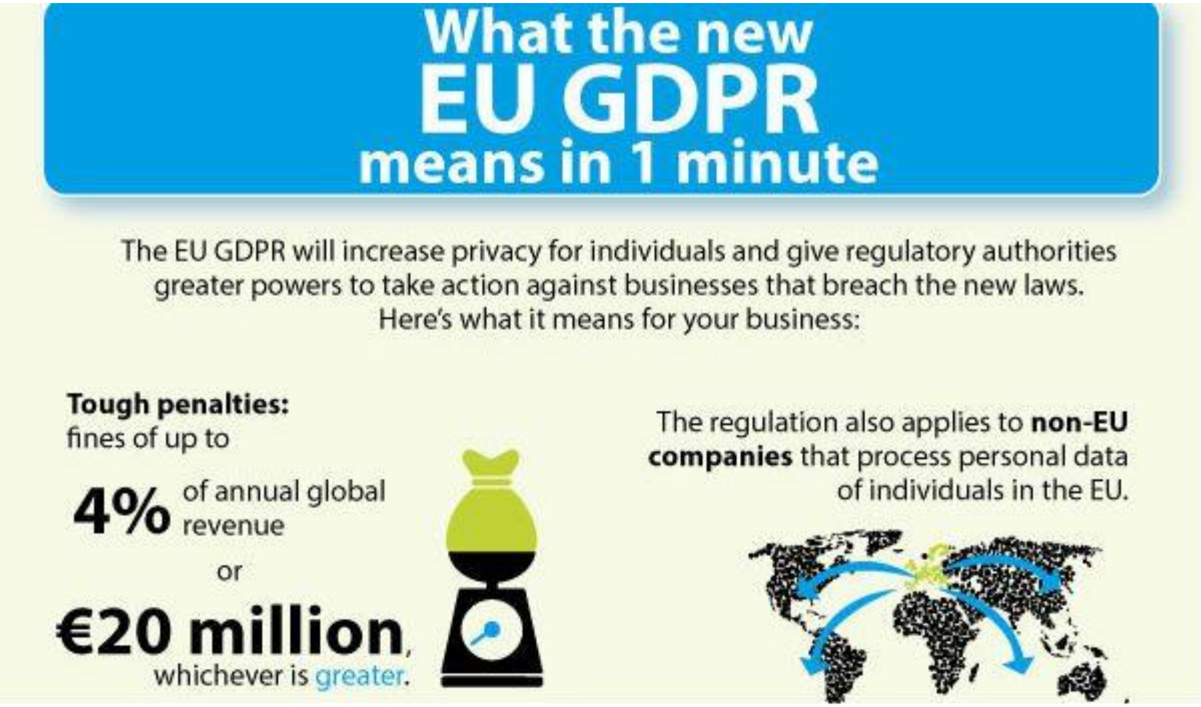
74%: customers prefer dealing with suppliers with proven cyber security credentials

50%: have been asked about information security measures by customers in the past 12 months

Cyber Security Strategy

- Key elements
  - Adopt technical and organizational measures appropriate to risk
  - Clear, centrally-defined security policies
    - With audit, 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
  - Effective incident & data breach response capability – tried and tested
  - Idea of business resilience
  - Use international standards to demonstrate credibility

EU GDPR



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.

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

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

- ***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

GDPR: Key statements

- Clear organizational policies for protection of personal data
- Board assurance provided by audit and monitoring processes
- Confidentiality, integrity and availability of personal information
- Adopt technical and organizational measures appropriate to risk
- Penalties for infringement must be ‘effective, proportionate and dissuasive’
- Organizations may use adherence to approved codes of conduct or management system certifications “as an element by which to demonstrate compliance with their obligations”

NIS: Network & Information Security Directive

- Applies to:
  - ‘Essential services’– eg CNI, Finance, Health, Utilities, Transport, Energy, Food etc
  - Digital Service Providers
- Translated into national law by May 2018
- Increase intra-EU cooperation, national CSIRT network
- Adopt technical and organizational measures appropriate to risk:
  - Ensure the security of systems and facilities
  - Processes for Incident handling
  - Business continuity management
  - Monitoring, auditing and testing
  - Compliance with international standards
- Penalties for infringement must be ‘effective, proportionate and dissuasive’.
- Member states shall…take into account…international standards

Digital Services

- Includes:
  - images or text, such as… and other digitised documents eg, pdf files
  - supplies of music, films and games… gambling…
  - online magazines
  - website supply or web hosting services
  - distance maintenance of programmes and equipment
  - supplies of software and software updates
  - advertising space on a website

HMRC web page 24/01/2017

NIS

- Legislation must be enacted by 9th May 2018 – before GDPR!
- Applies to enterprises with 50+ staff and T/O or balance sheet >€10 m
- Digital services - includes Electronically supplied services:

"…delivered over the internet…the nature of which renders their supply…impossible…in the absence of information technology"

What can you do to stay safe: Cyber Essentials Scheme

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.

Cyber Essentials vs Cyber Essentials Plus

Cyber Essentials:

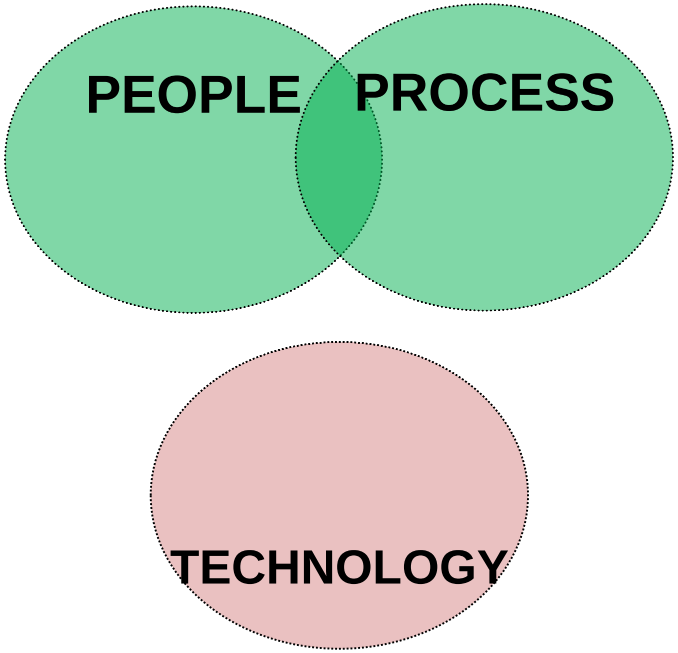
- *Self Assessment Questionnaire*
- *Attestation of Compliance*
- *External vulnerability scan*

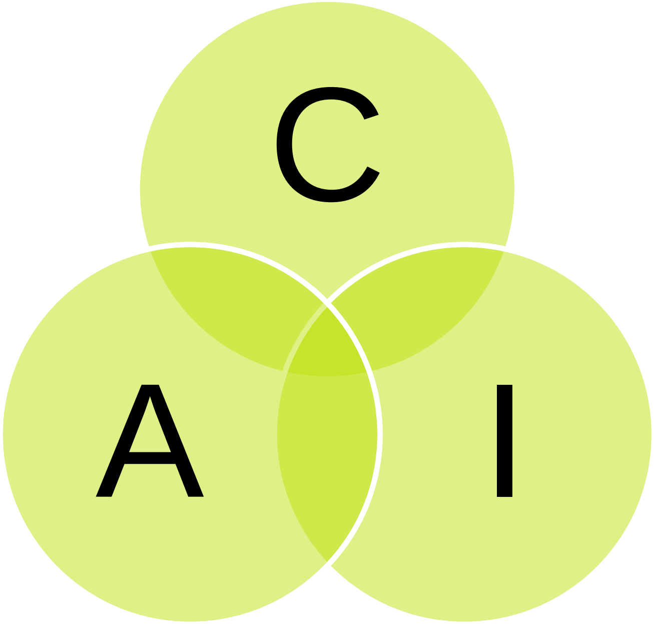
Cyber Essentials Plus

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

Independent Certification
CREST-accredited

Critical issues





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

Convergence: Cyber Security Assurance

- ISO/IEC 27001:2013
  - Is an international standard
  - already meets the “appropriate technical and organizational measures” requirement
  - Is widely recognised and adopted
- Provides assurance to the board that data security is being managed in accordance with business, contractual and regulatory requirements
  - Information security/data protection policies
  - Audit, monitoring and review
- Manage ALL information assets and all information security within the organization – protecting against ALL threats

Breach Recovery?

- Cyber security is about defence
  - Protect C, I, A
  - Respond to Incidents
  - Maintain security posture
- However – defences are being – and will be - breached…..
  - How should we respond, in what order?
    - Not part of ISO27001
    - Not part of traditional Information Security

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..”

Supporting Standards

- ISO/IEC 27031 - Guidelines for information and communication technology readiness for business continuity
- ISO/IEC 27032 – Guidelines for Cyber Security
- ISO/IEC 27035 - Information Security Incident Management
- ISO/IEC 27036-3 Information Security for Supplier Relationships
- ISO 22301 – Business Continuity Management System

7-Step Cyber-resilience Strategy

1. Governance, clear policies, leadership
2. Business, regulatory and contractual requirements
3. Integrated risk assessment, BIA, DPIA
   - Assets AND Processes
4. Secure the cyber perimeter & endpoints; defence in depth
5. Train all staff – skills, competence, awareness
6. Develop and test a security incident response and escalation plan
7. Audit, monitor, test, continually improve

Adopt and integrate ISO27001, ISO27031, ISO27035, ISO22301 tdrewitt@itgovernance.co.uk

0845 070 1750

www.itgovernance.co.uk