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

IT Matters Forum July 2017

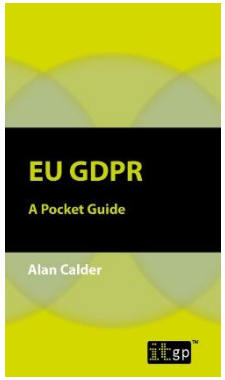
Alan Calder
Founder & Executive Chairman
IT Governance Ltd

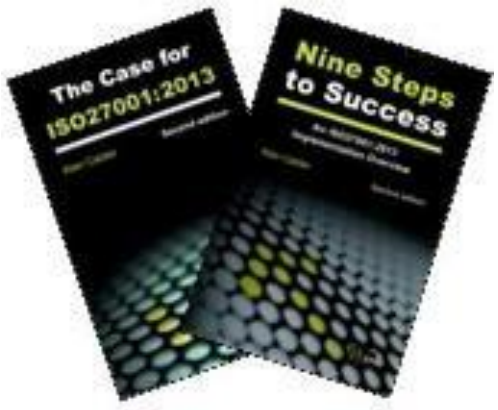
www.itgovernance.co.uk

Introduction

www.itgovernance.co.uk

- Alan Calder
- Founder – IT Governance Ltd
- World leaders in Information Security Management Systems, cyber risk management and GDPR compliance.
- *IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002, 6th Edition* (Open University textbook)
- *www.itgovernance.co.uk (also sites in USA, EU, Asia Pacific, South Africa)*
-





IT Governance Ltd: GRC One-Stop-Shop

www.itgovernance.co.uk

Thought Leaders
Specialist publisher

Implementation toolkits

ATO

Consultants

Software and e-learning

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……

Agenda

www.itgovernance.co.uk

- UK backdrop: cyber denial
- EU GDPR
- NIS
- Cyber resilience maturity model
- Immediate actions

Cyber disconnect

www.itgovernance.co.uk

- Most organizations are ‘confident’ in their cyber defences
- 70% of organizations say:
  - Cyber security completely embedded in their processes
  - Cyber security a board-level concern, with top executive focus
- However:
  - Organizations face 100+ targeted attacks per year
  - 1/3 are successful – that’s 2 or 3 per month!
  - Most breaches are discovered by outsiders!

(Accenture: Facing the Cybersecurity Conundrum 2016)

Cyber Health Check example

www.itgovernance.co.uk

- National health organisation, founded in 1960s, established across UK, nearly 4000 staff
- Cyber Heath Check
  - 14 Critical Internet-facing vulnerabilities
  - 175 medium level vulnerabilities
  - Uncertainty over roles and responsibilities
  - Uncertainty over cyber insurance
  - No risk management process, no risk assessment in last 3 years
  - No data inventory but 1000's of boxes of paper records and millions of electronic personal records
  - No data classification, no retention policy
  - 2 competing versions of a data protection policy
  - Other documents, where they exist, up to 7 years old
  - No BCMS, ISMS, or incident response process
  - No formal staff training and awareness
  - Physical security - internal and external – highly vulnerable
  - Windows operating systems – 2003, 2008 and 2012
  - SQL server versions outdated, patching on average 18 months old
  - Rogue devices will be assigned a network IP address
  - 60 remote sites connect to the main network – 50 of which are running end-of-life hardware and software
  - Servers and mobile devices unencrypted
  - No restrictions on data exports or file sharing
  - PCI compliance status unclear
  - Had some reported minor breaches

Data breaches in the UK

www.itgovernance.co.uk

- January to March 2016 - 448 new cases
- Data Breaches by Sector
  - Health (184)
  - Local Government (43)
  - Education (36)
  - General Business (36)
  - Finance, Insurance & Credit (25)
  - Legal (25)
  - Charitable & Voluntary (23)
  - Justice (18)
  - Land or Property Services (17)
  - Other (41)
- NB: Mandatory reporting only for public sector, not private/not-for-profit
- How will these stats change after May 2018?

Source: UK Information Commissioner's Office 2016

Cyber risk – an overview

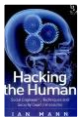
www.itgovernance.co.uk

Attackers


Hacktivists


Terrorists


Opportunists



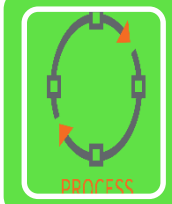
Criminals


Competitors


Enemies

Weaknesses


People



Process


Technology

Assets

IP

Card data

PII

Money

Reputation

Commercial Info

Security breach levels are rising

www.itgovernance.co.uk

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

- Hacked organizations continue struggling for years afterwards
  - Target, Yahoo, Talk Talk

Cyber security, accountability & compliance

www.itgovernance.co.uk

"The biggest vulnerability remediation rates have been achieved when boards of directors and executive management have been accountable for breaches. Interestingly, when breach accountability was with security departments, the lowest remediation rates have been achieved.
It is worth noticing that the largest remediation rates of vulnerabilities are achieved when compliance is the driver, while vulnerability remediation due to a risk-oriented posture is delivering lowest remediation rates." *ENISA Threat Report,* 2015

ICO on accountability

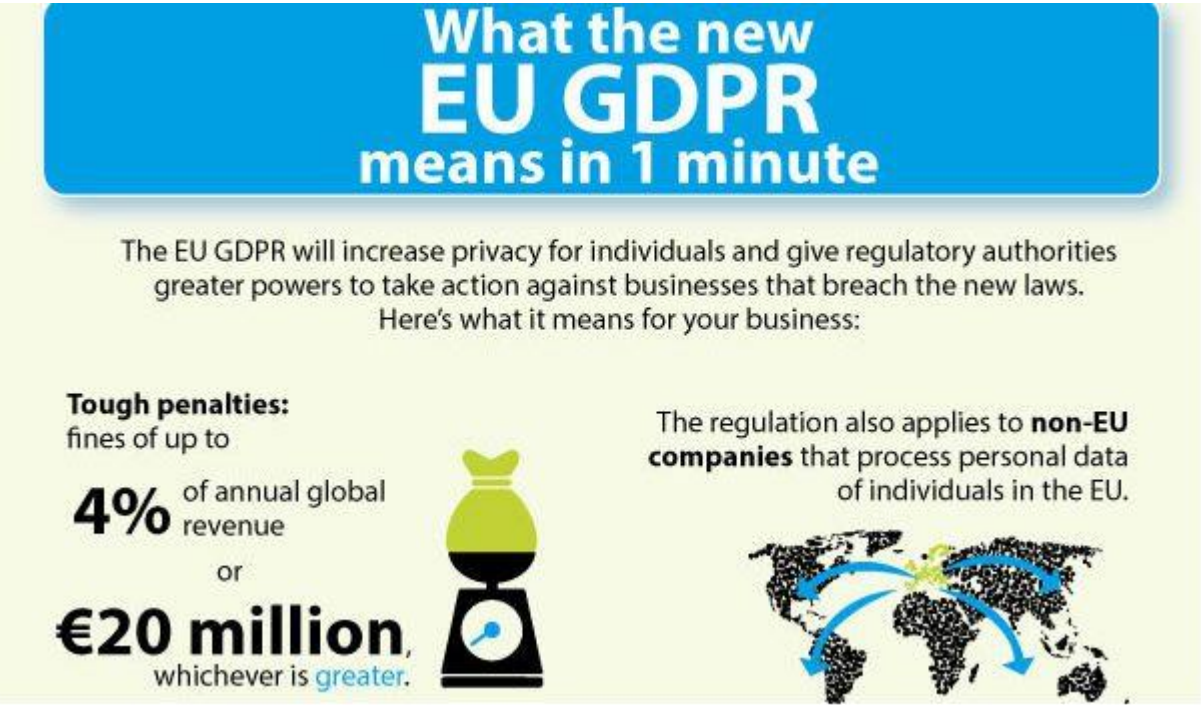
www.itgovernance.co.uk

- “The new legislation creates an onus on companies to understand the risks that they create for others, and to mitigate those risks. It’s about moving away from seeing the law as a box ticking exercise, and instead to work on a framework that can be used to build a culture of privacy that pervades an entire organisation.”
- “The GDPR mandates organisations to put into place comprehensive but proportionate governance measures.”
- “It means a change to the culture of an organisation. That isn’t an easy thing to do, and it’s certainly true that accountability cannot be bolted on: it needs to be a *part of the company’s overall systems approach* to how it manages and processes personal data.”

- Speech to ICAEW 17 January 2017

EU GDPR

www.itgovernance.co.uk



Complete overhaul of data protection framework
All forms of personal data, including biometric, genetic and location data
Applies across all member states of the EU
In force on 25 May May 2018

The GDPR: Data subject actions

www.itgovernance.co.uk

- Article 77: Right to lodge a complaint with a supervisory authority
- Article 78: Right to an effective judicial remedy against a supervisory authority
- Article 79: Right to an effective judicial remedy against a controller or processor
- Article 80: Right to mandate a consumer protection agency
  - Represent them, bring claims on their behalf
- Article 82: Right to compensation
  - Any person who has suffered “material or non-material damage”
  - No upper limit

The GDPR: Data breaches

www.itgovernance.co.uk

- ***Mandatory data breach reporting – within 72 hours***
  - Processors must report to controllers “without undue delay”
  - Controllers must report to supervisory authority within 72 hours
  - Describe actions being taken to
    - Address the breach
    - Mitigate the consequences
  - Data subjects must be contacted “without undue delay”
    - Unless no risk to their data
- Failure to report within 72 hours must be explained

NIS: Network & Information Security Directive

www.itgovernance.co.uk

- Applies to:
  - 'Essential services'– eg CNI, Finance, Health, Utilities, Transport, Energy, Food, Marine 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'.

Cyber health check example: breach consequences after 25 May 2018

www.itgovernance.co.uk

- Report breach to ICO – if they know about it, if they know how to report
- Investigation – will reveal what my be described as ‘sustained negligence’
- Is likely to trigger monetary penalties in the upper bracket – for multiple breaches of the data protection principles
- PCI compliance breach – investigation and fines
- NIS breach – penalties similar to GDPR
- Multiple individual court actions for non-material damage
- Reputation damage, funding problems
- Will tie up directors and senior managers for years
- Will not help avoid the necessary cyber security investment
  - Enhanced by clean-up and emergency costs

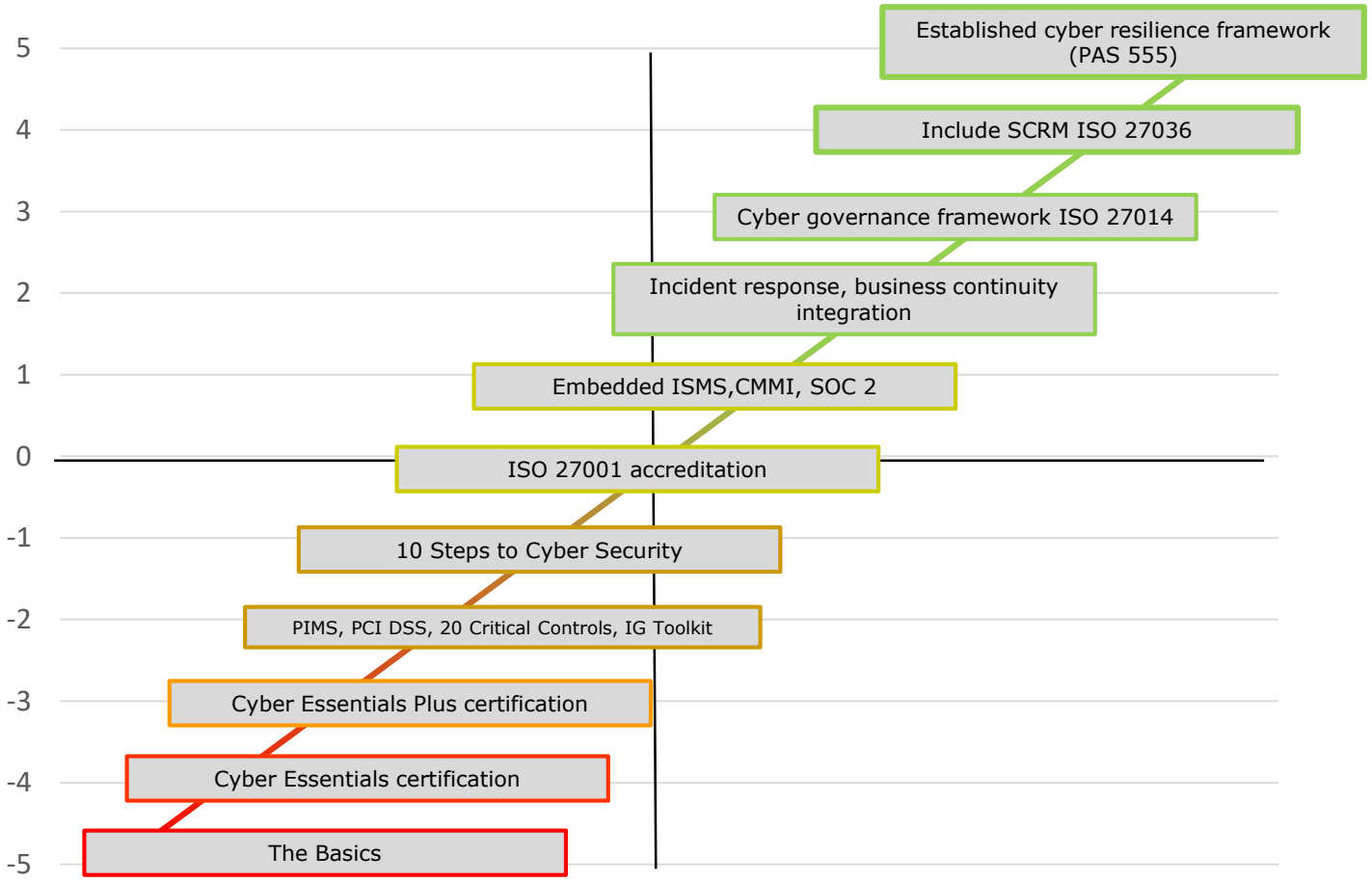
Convergence: cyber security assurance

www.itgovernance.co.uk

- GDPR Article 32: “Adherence to an approved code of conduct…or an approved certification mechanism….. may be used as an element by which to demonstrate compliance with the requirements….of this Article.”
- ISO/IEC 27001:2013
  - Is an international standard
  - 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

Cyber resilience maturity model

www.itgovernance.co.uk



Key, immediate steps

www.itgovernance.co.uk

- Board involvement
- Clear roles and responsibilities – cyber security, data protection
- Budget – for people, support and technology
- Update and patch – systematically and comprehensively
- Penetration test – then remediate
- Encrypt mobile devices, databases and email
- Inventory personal data – delete/destroy old data, secure what you keep
- Prepare and test an incident response and data breach reporting process
- Initiate GDPR and NIS compliance plans
- In parallel – cyber essentials and start climbing the maturity ladder as fast as possible
-

Questions?

acalder@itgovernance.co.uk

0845 070 1750

www.itgovernance.co.uk