# Data Breaches and the EU GDPR

Adrian Ross LLB (Hons), MBA
GRC Consultant
IT Governance Ltd
30 June 2016

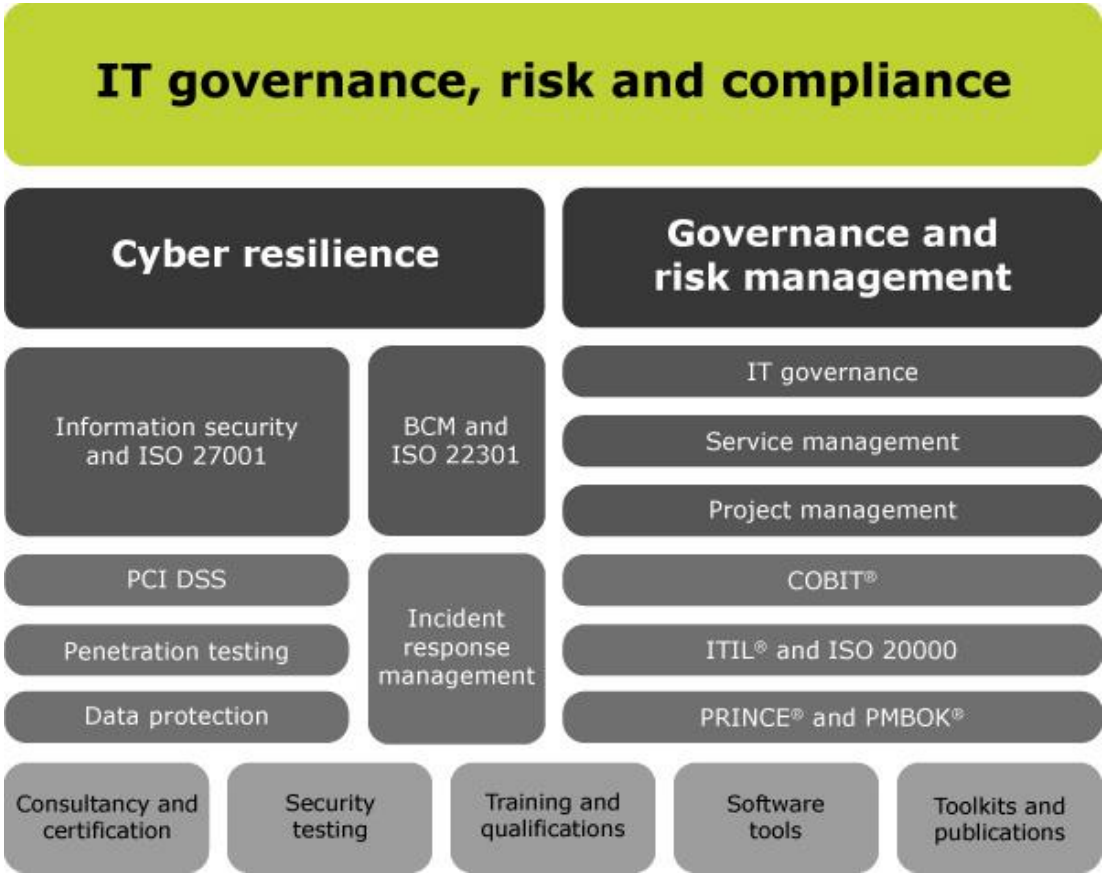
# Introduction



- Adrian Ross
- GRC Consultant
  - Infrastructure Services
  - Business Process Re-engineering
  - Business Intelligence
  - Business Architecture
  - Intellectual Property
  - Legal Compliance
  - Data Protection & Information Security
  - Enterprise Risk Management

# IT Governance Ltd: GRC One-Stop-Shop






All verticals, all sectors, all organizational sizes

# Agenda



- An overview of the regulatory landscape
- Territorial scope
- Remedies, Liabilities and Penalties
- Principles of the EU GDPR
- Data Breaches
- Notification rules
- Supervisory Authorities
- EU Data Protection Board

# The nature of European law



- Two main types of legislation:
  - Directives
    - Require individual implementation in each Member State
    - Implemented by the creation of national laws approved by the parliaments of each Member State
    - European Directive 95/46/EC is a Directive
    - UK Data Protection Act 1998
  - Regulations
    - Immediately applicable in each Member State
    - Require no local implementing legislation
    - EU GDPR is a Regulation

# *Article 99: Entry into force and application*



This Regulation shall be binding in its entirety and directly applicable in all Member States.

**KEY DATES**

- On 8 April 2016 the Council adopted the Regulation.
- On 14 April 2016 the Regulation was adopted by the European Parliament.
- On 4 May 2016, the official text of the Regulation was published in the EU Official Journal in all the official languages.
- The **Regulation** entered into force on 24 May 2016, and applies from **25 May 2018**.
- http://ec.europa.eu/justice/data-protection/reform/index_en.htm

Final Text of the Directive: http://data.consilium.europa.eu/doc/document/ST-5419-2016-REV-1/en/pdf

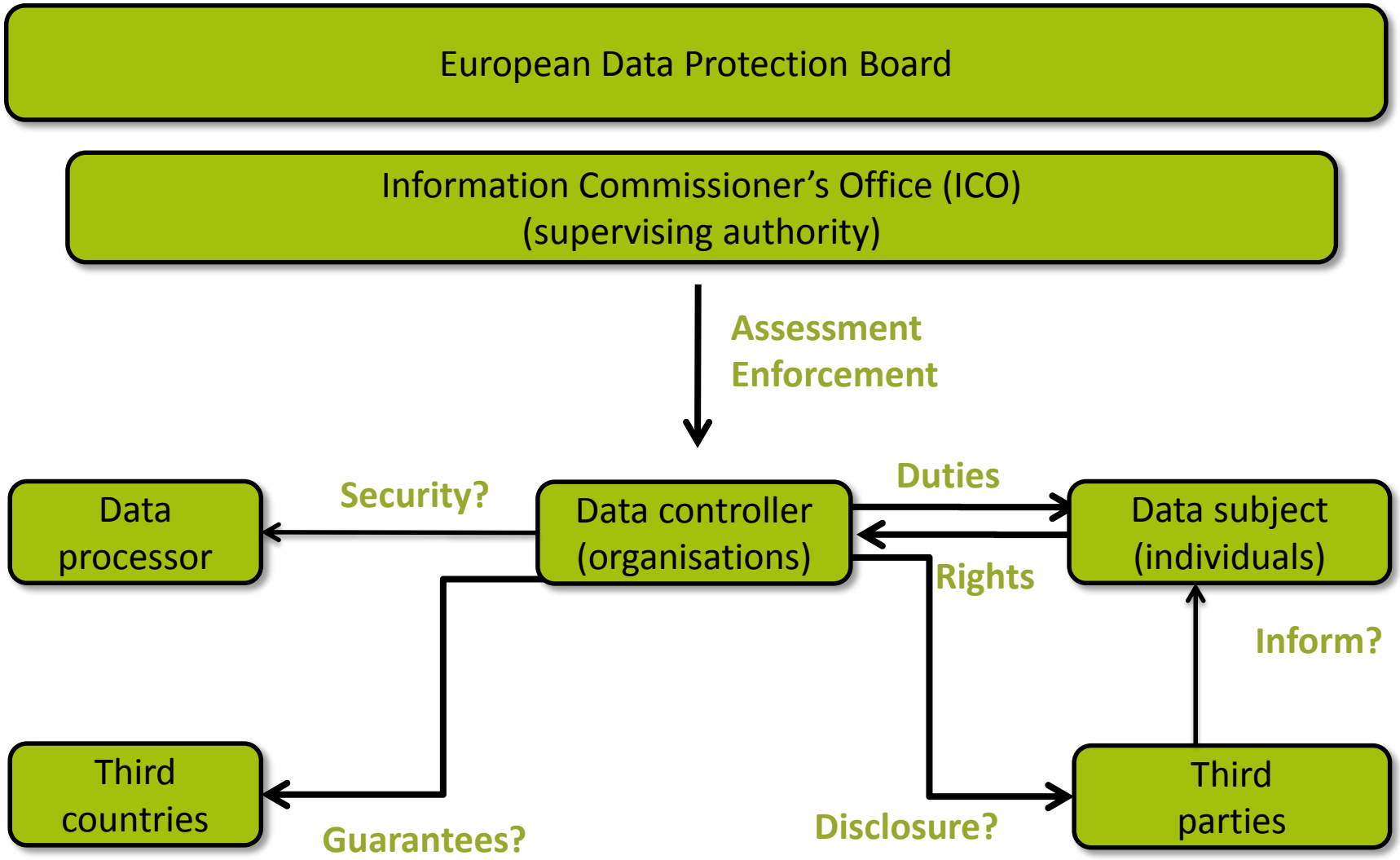
# GDPR



The GDPR has eleven chapters:

1. • Chapter I General Provisions: Articles 1 - 4
2. • Chapter II Principles: Articles 5 - 11
3. • Chapter III Rights of the Data Subject: Articles 12 - 23
4. • Chapter IV Controller and Processor: Articles 24 - 43
5. • Chapter V Transfer of Personal Data to Third Countries: Articles 44 - 50
6. • Chapter VI Independent Supervisory Authorities: Articles 51 - 59
7. • Chapter VII Cooperation and Consistency: Articles 60 - 76
8. • Chapter VIII Remedies Liabilities and Penalties: Articles 77 - 84
9. • Chapter IX Provisions Relating to Specific Processing Situations: Articles 85 - 91

# Data protection model under GDPR



# *Articles 1 – 3: Who, and where?*



- Natural person = a living individual
- Natural persons have rights associated with:
  - The protection of personal data
  - The protection of the processing personal data
  - The unrestricted movement of personal data within the EU
- In material scope:
  - Personal data that is processed wholly or partly by automated means;
  - Personal data that is part of a filing system, or intended to be.
- The Regulation applies to controllers and processors in the EU irrespective of where processing takes place.
- It applies to controllers not in the EU

# Remedies, liabilities and penalties



- ***Article 79: Right to an effective judicial remedy against a controller or processor***
  - Judicial remedy where their rights have been infringed as a result of the processing of personal data.
    - In the courts of the Member State where the controller or processor has an establishment.
    - In the courts of the Member State where the data subject habitually resides.
- ***Article 82: Right to compensation and liability***
  - Any person who has suffered material, or non-material, damage shall have the right to receive compensation from the controller or processor.
  - Controller involved in processing shall be liable for damage caused by processing.
- ***Article 83: General conditions for imposing administrative fines***
  - Imposition of administrative fines will in each case be effective, proportionate, and dissuasive
    - taking into account technical and organisational measures implemented;
  - € 20,000,000 or, in case of an undertaking, 4% total worldwide annual turnover in the preceding financial year (whichever is higher)

# Article 5: Principles - Personal data shall be:



1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary
4. Accurate and, where necessary kept up to date
5. Retained only for as long as necessary
6. Processed in an appropriate manner to maintain security
7. Accountability

# Article 5 & 6: Lawfulness



- Secure against accidental loss, destruction or damage
- Processing must be lawful – which means, inter alia:
  - Data subject must give consent for specific purposes
  - Other specific circumstances where consent is not required
    - So that controller can comply with legal obligations etc
- One month to respond to Subject Access Requests – & no charges
- Controllers and processors clearly distinguished
  - Clearly identified obligations
  - Controllers responsible for ensuring processors comply with contractual terms for processing information
  - Processors must operate under a legally binding contract
    - And note issues around extra-territoriality

# Article 32: Security of Personal Data



- A requirement for data controllers and data processors to implement a level of security appropriate to the risk, including:
  - pseudonymisation and encryption of personal data;
  - ensure the ongoing confidentiality, integrity and availability of systems;
  - a process for regularly testing, assessing and evaluating the effectiveness of security measures;
  - security measures taken need to comply with the concept of privacy by design;

# Key facts about cyber breaches



Which organisations suffered data breaches in 2015?

- 69 % of large organisations
- 38 % of small organisation

What was the median number of breaches per company?

- Large organisations: 14
- Small organisations: 4

What was the average cost of the worst single breach?

- Large organisations: £1.46 - £3.14m
- Small organisations: £75k - £311k

What will happen next year?

- 59% of respondents expect more breaches this year than last

- *PwC and BIS: 2015 ISBS Survey*

**60% of breached small organisations close down within 6 months – National Cyber Security Alliance**

# What sorts of breaches?



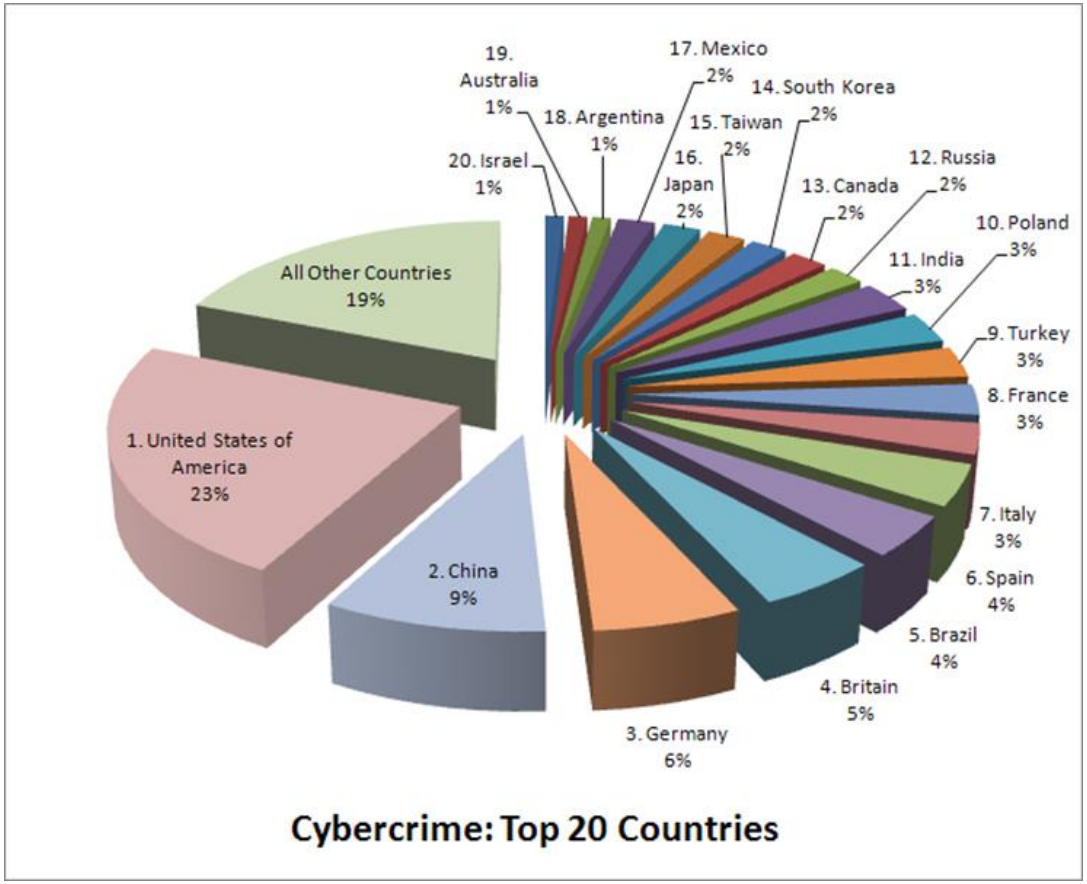
Of Large Organisations:

- External attack – 69%
- Malware or viruses – 84%
- Denial of Service – 37%
- Network penetration (detected) – 37%
  - (if you don't think you've been breached, you're not looking hard enough)
- Know they've suffered IP theft – 19%
- Staff-related security breaches – 75%
- Breaches caused by inadvertent human error – 50%

*PwC and BIS: 2015 ISBS Survey*

# Cyber crime: widespread






**Source: BusinessWeek/Symantec**

# Breach Landscape



- Not if, but when
- Being prepared is key
- Develop the resilience to respond
- Don’t wait until after the event
- 72 hour window to respond
- How and when you respond goes towards mitigation
- Incident response mandated in ISO27001, ISO 22301, PCI DSS

# CREST - Three Phases of a Cyber Attack



- **Stage 1**

- **Reconnaissance**
  - Identify target
  - Look for vulnerabilities

- **Countermeasures:**
  - Monitoring and logging
  - Situational awareness
  - Collaboration

# CREST - Three Phases of Cyber Attack



- **Stage 2**

- **Attack target**
  - Exploit vulnerabilities
  - Defeat remaining controls

- **Countermeasures:**
  - Architectural system design
  - Standard controls (i.e. ISO 27001)
  - Penetration testing

# CREST - Three Phases of Cyber Attack



- **Stage 3**

- **Achieve objectives**
  - Disruption of systems
  - Extraction of data
  - Manipulation of information

- **Countermeasures:**
  - Cyber security incident response planning
  - Business continuity and disaster recovery plans
  - Cyber security insurance

# The Top Ten Challenges Facing Organisations



- Organisations can have significant difficulty in responding to cyber security incidents, particularly sophisticated cyber security attacks.
- The top ten challenges organisations face in responding to a cyber security incident in a fast, effective and consistent manner are:
  - Identifying a suspected cyber security incident;
  - Establishing the objectives of an investigation and a clean-up operation;
  - Analysing all available information related to the potential cyber security incident;
  - Determining what has actually happened;
  - Identifying what systems, networks and information (assets) have been compromised;
  - Determining what information has been disclosed to unauthorised parties, stolen, deleted or corrupted;
  - Finding out who did it and why;
  - Working out how it happened;
  - Determining the potential business impact of the cyber security incident;
  - Conducting sufficient investigation using forensics to identify those responsible.

# CREST Cyber Incident Response Approach



- **Prepare:**
  - Conduct a criticality assessment;
  - Carry out a cyber security threat analysis;
  - Consider the implications of people, process, technology and information;
  - Create an appropriate control framework;
  - Review your state of readiness in cyber security incident response

# CREST Cyber Incident Response Approach



- **Respond:**
  - Identify cyber security incident/s;
  - Define objectives and investigate the situation;
  - Take appropriate action;
  - Recover systems, data and connectivity.

# CREST Cyber Incident Response Approach



- **Follow up:**
  - Investigate incident more thoroughly;
  - Report incident to relevant stakeholders;
  - Carry out a post incident review;
  - Communicate and build on lessons learned;
  - Update key information, controls and processes;
  - Perform trend analysis.

- Utilising the CREST Cyber Incident response approach and drawing from ISO 27001 and ISO 27035 standards IT governance can assist you in defining and implementing an effective **prepare**, **respond**, and **follow up** incident response approach

# Article 33: Personal Data Breaches



- The definition of a Personal Data Breach in GDPR:
  - A 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

# Article 33: Personal Data Breaches



- Obligation for data processor to notify data controller
  - Notification without undue delay after becoming aware
  - No exemptions
  - All data breaches have to be reported
  - EDPB to issue clarification with regard to ‘undue delay’

# Article 33: Personal Data Breaches



- Obligation for data controller to notify the supervisory authority
  - Notification without undue delay and not later than 72 hours
  - Unnecessary in certain circumstances
  - Description of the nature of the breach
  - Communicate details of the Data Protection Officer
  - No requirement to notify if unlikely to result in a high risk to the rights and freedoms of natural persons
  - Failure to report within 72 hours must be explained
  - EDPB to issue further clarification with regard to “undue delay”

# Article 34: Personal Data Breaches



- Obligation for data controller to communicate a personal data breach to data subjects
  - Communication to the data subject without undue delay if high risk
  - Communication in clear plain language
  - Supervisory authority may compel communication with data subject
  - Exemptions if appropriate technical and organisational measures taken
  - High risk to data subject will not materialise
  - Communication with data subject would involve disproportionate effort

# Independent Supervisory Authorities



- Member states must create independent supervisory authorities and resource them appropriately
  - Tasks:
  - Monitor and enforce
  - Communicate
  - Promote awareness
- Powers:
  - To investigate, correct, advise, enforce
- Leading Supervisory Authority for multi-state controllers

# European Data Protection Board (EDPB)



- Ensure cooperation, communication, consistency and mutual assistance between national supervisory authorities
- Monitor and ensure correct application of the Regulation
- Examine any question dealing with its application

- Ie: Ensure a level playing field

# GDPR - Summary



- Complete overhaul of data protection framework
  - Covers all forms of PII, including biometric, genetic and location data
- Applies across all member states of the European Union
- Applies to all organizations processing the data of EU citizens – wherever those organizations are geographically based
- Specific requirements around rights of data subjects, obligations on controllers and processors, including privacy by design
- Administrative penalties for breach up to 4% revenue or €20 million
  - Intended to be 'dissuasive'
- Data subjects have a right to bring actions (in their home state) and to receive damages if their human rights have been breached *('Right to an effective judicial remedy against a controller or processor')*
- Fines to take into account *'the technical and organizational measures implemented…'*

# Data Breaches in the 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)

*Source: UK Information Commissioner's Office*

# Data Breaches in the UK

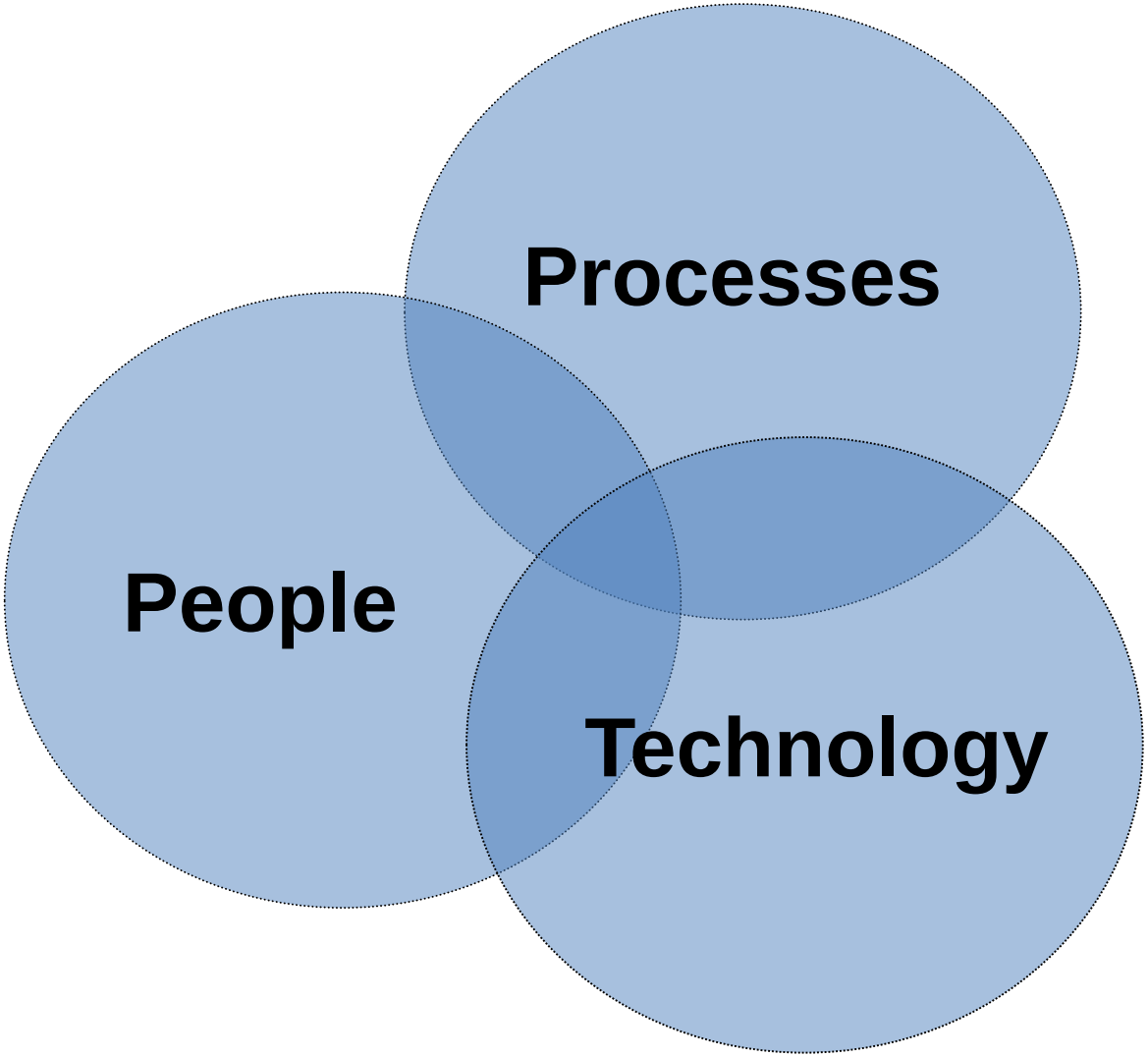


- January to March 2016
- Data Breaches by type
  - Loss or theft of paperwork (74)
  - Data posted of faxed to wrong recipient (74)
  - Data sent by e-mail to wrong recipient (42)
  - Webpage hacking (39)
  - Failure to redact data (28)
  - Insecure disposal of data (24)
  - Loss or theft of unencrypted device (20)
  - Information uploaded to web page (10)
  - Verbal disclosure (7)
  - Insecure disposal of hardware (2)
  - Other principle 7 failure (128)

*Source: UK Information Commissioner's Office*

# Information Security





# Cyber Security Assurance



- 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"
  - ICO and BSI are both developing new GDPR-focused standards
- 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

# IT Governance: GDPR One-Stop-Shop



- Accredited Training – 1 Day Foundation Course
  - London OR Cambridge: http://www.itgovernance.co.uk/shop/p-1795-certified-eu-general-data-protection-regulation-foundation-gdpr-training-course.aspx
  - ONLINE http://www.itgovernance.co.uk/shop/p-1834-certified-eu-general-data-protection-regulation-foundation-gdpr-online-training-course.aspx
- Practitioner course, classroom or online
  - www.itgovernance.co.uk/shop/p-1824-certified-eu-general-data-protection-regulation-practitioner-gdpr-training-course.aspx
- Pocket Guide www.itgovernance.co.uk/shop/p-1830-eu-gdpr-a-pocket-guide.aspx
- Documentation Toolkit www.itgovernance.co.uk/shop/p-1796-eu-general-data-protection-regulation-gdpr-documentation-toolkit.aspx
- Consultancy support
  - Data audit
  - Transition/implementation consultancy
  - www.itgovernance.co.uk/dpa-compliance-consultancy.aspx

# Questions?

aross@itgovernance.co.uk

**0845 070 1750**

www.itgovernance.co.uk