

Effective Management of Data In a Connective World

What to what to keep a look-out for given
all these inter-connected new devices



Agenda

- Introduction
- Data Management – what does it encompass?
- Application to FEA member types
- Data Breach – what is the implication?
- Preventative approaches
- Further information
- Questions

Introduction

Carl Kruger

MD

Oxford Quality Centre Ltd

- t/a Qualitation
- t/a Secure Business Data

Previous life as Director of B2B Compliance
WEEE Compliance Scheme



Oxford
Quality
Centre Ltd

Qualitation
THE BRITISH QUALITY CENTRE



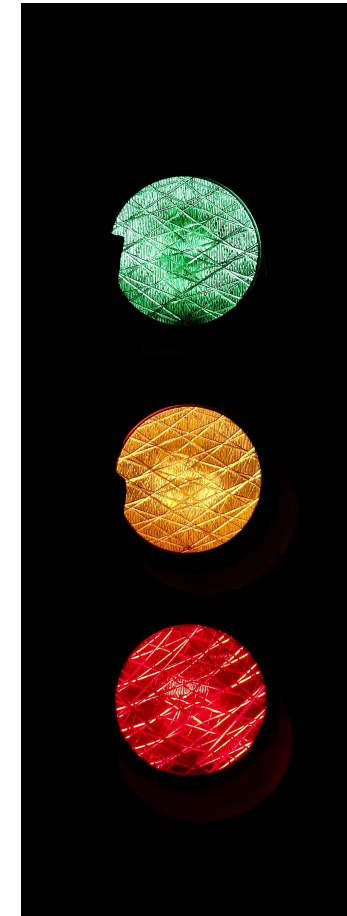
27k1 ISMS

ISO27001 management software

Recognised advisor to the FEA on Data Security Systems and Consultancy

Data Management – what does it encompass?

- **Availability**
 - Accessible by those authorised to use it
- **Usability**
 - Format pertinent to necessary usage
- **Currency**
 - Sufficient date clarity for optimising usage
- **Complete**
 - All relevant data available in both time frame and scope
- **Confidentiality**
 - Secure, controlled and safe
- **Integrity**
 - Unchanged, undamaged, complete, known location



GDPR Obligations

- General Data Protection Regulations (GDPR)
- If you pay your staff, you have GDPR obligations!
- If you take personal details from anyone, you have GDPR obligations.

- You must register with the ICO and pay annual fee (3 tiers)
 - <https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/>

- You must follow requirements of GDPR:
 - Identify your data security risks, assess them after remedial activity and monitor this internally going forwards.
 - Determine your legal grounds for holding and processing data (Consent, Contract, Legal Obligation, Vital Interest, Public Task, Legitimate Interest (with Legitimate Interest Assessment))
 - Respond to requests for data held – hard or soft copy (Access, Obstruct, Restrict, Disposal, Portability) within 1 month, no fee
 - Privacy by Design
 - Report data breaches within 72 hours of discovery
 - 3rd Party Suppliers' Compliance Responsibilities
 - In some instances appoint Data Protection Officer

PECR Obligations

Privacy & Electronic Communications Regulations (PECR)

- Relate to emails, electronic marketing and communication for all organisations
- Some public bodies covered for wider controls (eg traffic monitoring)
- General overlap with GDPR but some corporate information included where it is not in GDPR (ie. If a company requests you desist from contacting them, you must comply under PECR, whereas GDPR only relates to individuals so requesting).

Whose Data is it Anyway?

- Everyone has the right to expect you will look after their details
- Would you be happy to have your data distributed/destroyed?
- So why would anyone else if you did that to data about them?
- So start with the idea that: Data “belongs” to the person or organisation to which it relates
- That may not be the legal interpretation of who “owns” the data
- Until you lose it...

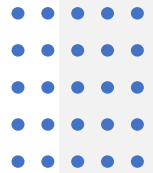


Data Breach – what is the implication?

Reputation Loss

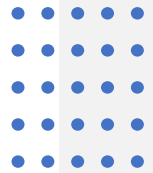
- Bankruptcy: faster than any fine.
- Customer loss: faster than your reactions.
- Drags business down: faster than any criminal sentences.
- Adverse impact: faster than any reaction by Authorities.
- Slow to impossible to rebuild - even if you had the chance.
- NB Out of all proportion to the scale if the news gets out





Applying Data Focus to FEA member types

- Business Services
- Servicing
- Manufacturing
- Distributors/Dealers



Why do FEA Member Types matter?

In the following FEA Member Type Slides, consider the different controls necessary for:

- On and off-site data
- IoT and data recording devices
- Regular and irregular activity
- Internal and outsourced data flows
- Differential scale of specific data sets eg customers, staff, suppliers

And thus the controls required for data under each of these parameters

Business Services

Potential Profile

- Support services to the industry
- Outsourced services
- Typically not core operations
- Temporary visitors
- Off-site activities
- Specific focus areas

Potential Data Impact

- Access to some/all data streams
- Data recorders used
- Internal reports made from data
- Staff controls esp offsite
- Data controls esp offsite
- Outsourced individuals: fall under GDPR

Servicing

Potential Profile

- Regular contracts
- Occasional one-offs
- Variety of different tasks
- Flexibility focus
- Temporary visitors
- Off-site activities

Potential Data Impact

- Instrumental data flows
- Possible unique data requirements
- Data concern may not be first
- Staff controls esp offsite
- Data controls esp offsite

Manufacturing

Potential Profile

- Regular tasks daily
- Volume focus
- Tight knit workforce
- Some outsourced supply

Potential Data Impact

- Key data on materials, usage etc
- Clear instructions possible
- Familiarity / tradition issues
- Issue re outsourced data flows
- Staff and Data On-site

Distributors / Dealers

Potential Profile

- Proffering specific brand(s)
- Large selection of customers
- Selling focus
- International outreach?

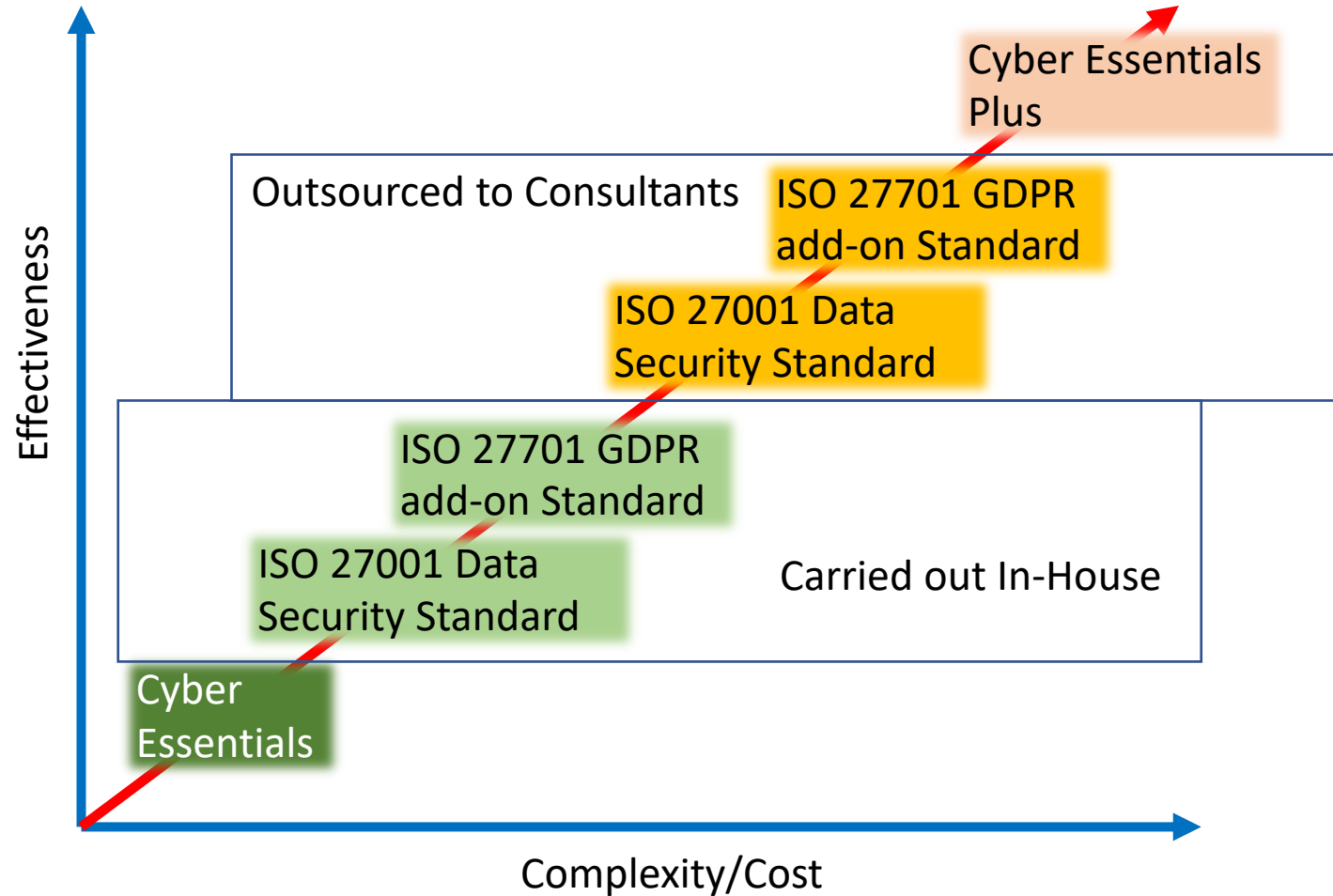
Potential Data Impact

- Different data sets between brands
- Large customer data volume
- High proportion finance data
- Interacting different legislation
- Individual's focus on sale first

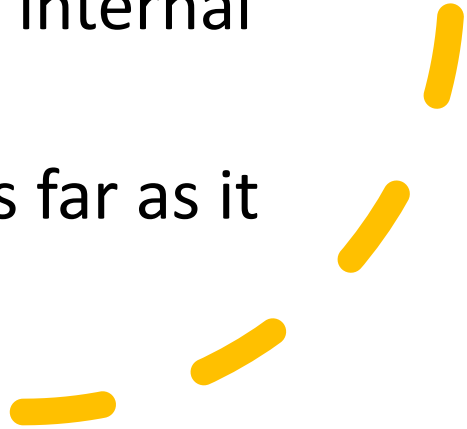
Internal Issues for all FEA Types

- Data input: scanning, IoT, upload, internal systems
- Data recording: computer, server, mobile, portable device, hard copy..
- Data processing: by staff, by computer, by external
- Data storage: cloud, server (where located + how communicated)
- Data sharing and authorisation: who, how, passwords, permissions
- Data deletion: when, how long, what for
- Data permissions: cookies, re-contacts
- Data monitoring: what, why, what effect, controls

Preventative approaches



Cyber Essentials

- A Government-led suggested minimal requirements:
 1. Secure your Internet connection
 2. Secure your devices and software
 3. Control access to your data and services
 4. Protect from viruses and other malware
 5. Keep your devices and software up to date
 - Clearly 'how' this is done is key – further advice given and needed
 - Minimal external cost (£300) but internal costs to make changes....
 - Practical, necessary and good...as far as it goes
- 

ISO 27001 Data Security & 27701 GDPR Standards

- 27001 is a full standard
 - Around 100 pre-set “controls” with additional procedures
 - Current version is 2013 with amendments from 2017
 - Comprehensive approach to physical and virtual precautions and awareness
 - Creates an Information Services Management System (ISMS)
 - Being installed by the ICO for their own data security
 - Voluntary 3rd party Certification applies
- 27701 is an add-on, you need 27001 first
 - Focus on GDPR variants of data security
 - Released late 2019
 - Not yet clear how this will be assessed




In-House v Outsourced Consultant

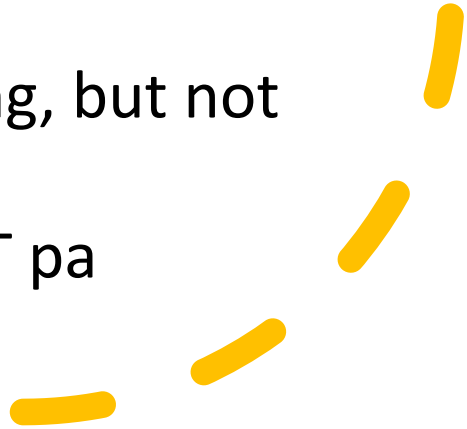
In-House better than Outsourced

- Knowledge held in-house already
- Pace to suit organisation
- Perfectly tailored to suit
- Much lower cash costs
- From £1,200+VAT pa) + Certification if applicable

Outsourced better than In-House

- Familiarity with Standards
 - Familiarity with organisation type
 - Faster to attain completion
 - Slightly lower demand on organisation staff
 - From £12,000+VAT upwards + Certification if applicable
- 

Cyber Essentials Plus

- Comprises Cyber Essentials with additional “Penetration” Tests
 - ... but which require systems covered in 27001
 - Penetration Tests are carried out by 3rd party as a “friendly” hack to the systems to see how they stand up.
 - NB. Systems includes people – so includes phishing emails to see if they are opened, inappropriate telephone requests to see if answered
 - Requires to be repeated on on-going, but not necessarily continuous basis
 - Certification costs from £1,500+VAT pa
- 

Further information

- Legislation:
 - Data Protection Act (DPA) 1998 updated by DPA 2018 which also incorporates GDPR legislation https://en.wikipedia.org/wiki/Data_Protection_Act_2018
 - Recent post-Brexit UK adjustment to EU Privacy and Electronic Communications Regs (PECR) 2003, now require consent for all statistical/analytics cookies
- Authority:
 - Information Commissioner's Office (ICO) <https://ico.org.uk/>
 - National Cyber Security Centre (NCSC) <https://www.ncsc.gov.uk/>
- Guidance:
 - <https://ico.org.uk/for-organisations/guide-to-data-protection/>
- Tools
 - Consultants, Dark Web searches, GDPR Legal advice, Monitoring services etc

Questions?

- Contact Details:
- Carl Kruger
- T: 0345 600 6975
- M: 07900 896975
- E: carl.kruger@oxfordqualitycentre.co.uk
- E: carl.kruger@qualitation.co.uk
- E: carl.kruger@securebusinessdata.co.uk
- W: <https://qualitation.co.uk> + now <https://securebusinessdata.co.uk>

Recognised advisor to the FEA on Data Security
Systems and Consultancy

