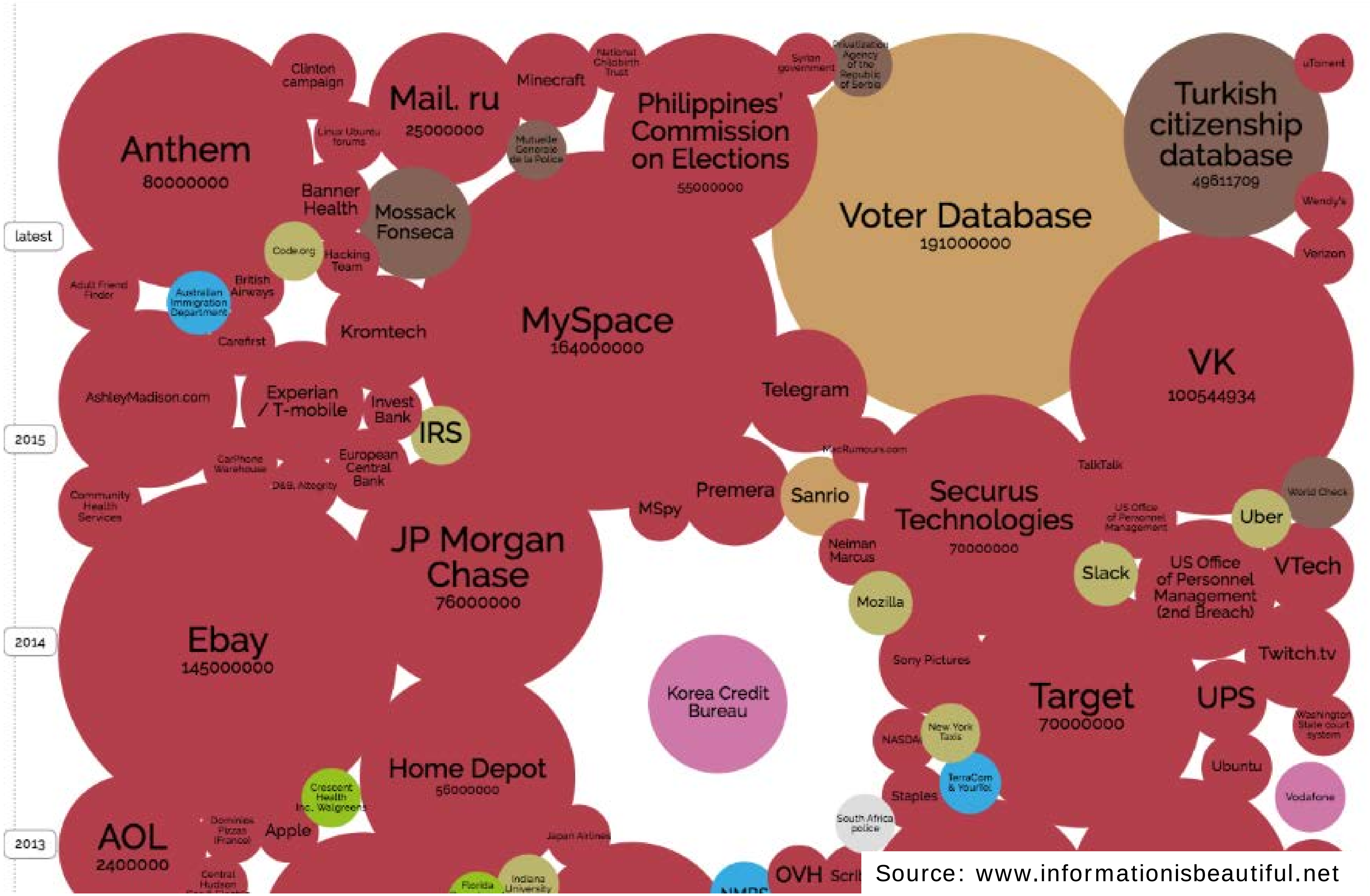
Multi-Layered Security in Road Tolling Services

Jon Wade
Security & Compliance Manager
Emovis UK

IBTTA
DENVER SEPT 11-14 2016
84TH ANNUAL MEETING & EXHIBITION

High profile data breaches



Source: www.informationisbeautiful.net

Key questions

- What would happen if you had a data breach?
- Would you be able to detect it?
- Would you be able to identify:
  - What systems and data were affected?
  - How did they do it?
  - Who did it?
  - Is it really over?
  - Could it happen again?

… or would it go unnoticed until it appeared in the press or social media?

Introduction

- Tolling service providers are typically required to comply with multiple security and data protection standards.

- These can be classified into 3 groups:
  - Legal requirements
  - Contractual requirements
  - Business requirements / best practices

Common data security standards

- Payment Card Industry Data Security Standard (PCI-DSS)
- Federal & local information security standards
- Federal & local data protection and privacy laws
- Safe Harbor agreements
- Evidential standards (for roadside images etc.)
- Financial standards
- ... others may apply

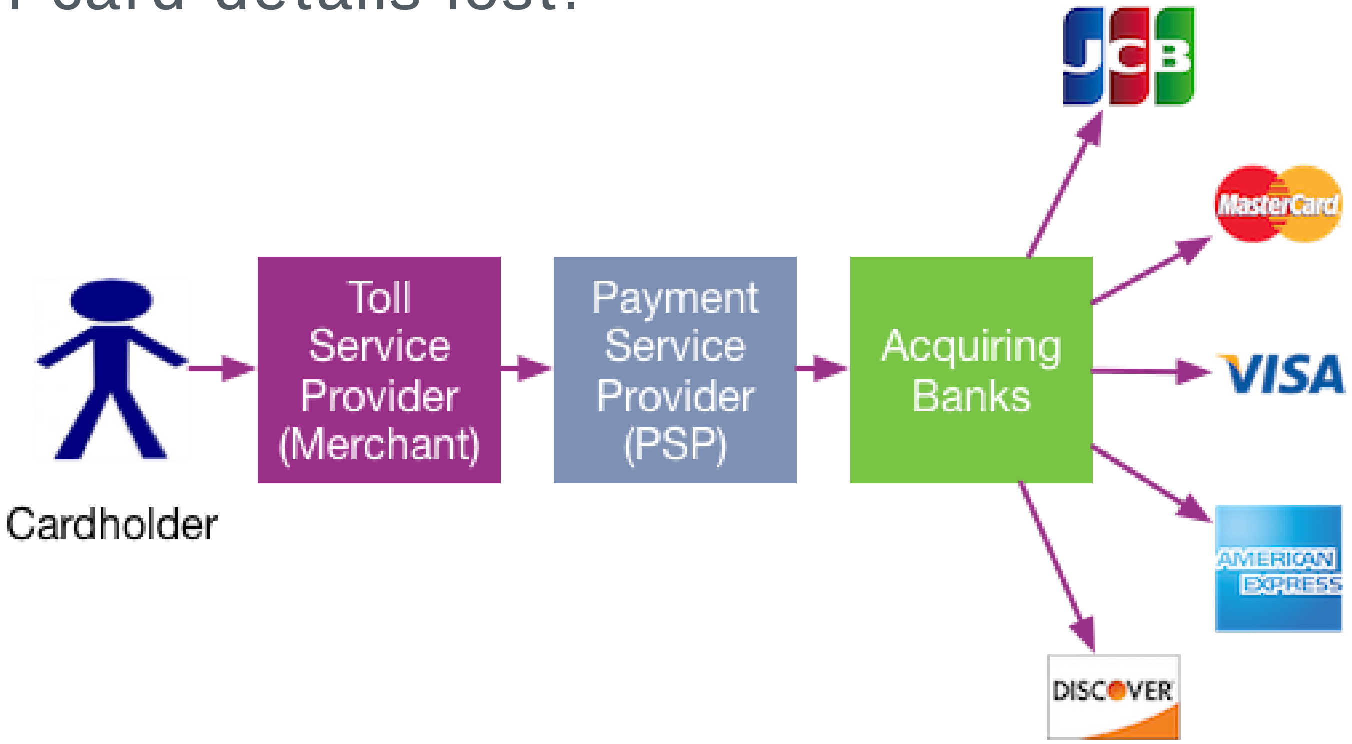
Reality

- The extent to which these standards are actually implemented and enforced is typically dependent on:
  - Whether they are legal / regulatory requirements
  - The appetite of the client to enforce contractual requirements
  - The risk appetite of the service provider

- PCI-DSS is a regulatory standard and generally well understood in the industry. Typically implemented on a ‘per contract’ basis.
- ISO27001 is often a *contractual* requirement but in practice it seems to be rarely implemented.
- The effort required to implement and operate an ISO27001 Information Security Management System is considerable and often under-estimated.

Payment Card Data

- The Payment Card Industry places regulations on acquiring banks who are required to oversee the compliance of their merchants.
- Merchants can face big fines for loss of cardholder data – dependent on the number of card details lost.



PCI-DSS Merchant Levels

- The merchant level and security controls required depends on the number of payment card transactions processed annually.

Level	Annual payment card transactions	Quarterly ASV Scans	Validation
1	**over 6 million**	**Required**	**Annual on-site review and Report on Compliance (RoC) by a Qualified Security Assessor**
2	over 1 million	Required	Annual Self-Assessment questionnaire
3	over 20,000	Required	Annual Self-Assessment questionnaire
4	under 20,000	Required	*Determined by the merchant's acquiring bank*

PCI-DSS Scope

- PCI-DSS scope is limited to the **Cardholder Data Environment**
- Multiple payment channels broadens the scope:
  - website
  - IVR
  - phone
  - mobile applications
  - batch payment processes
  - point of sale terminals
  - postal mail
- The scope (and risk) can be reduced significantly by not storing card holder data in your own system and tokenizing the data via a specialist Payment Service Provider.

HEALTH WARNING: If you’re not tokenizing card data you should be!

What is ISO27001?

- **ISO27001** is a specification for an Information Security Management System (ISMS)

- An ISMS is a framework of:
  - Policies
  - Procedures
  - Technical controls

- Together these form an organization's information risk management processes.

- An ISMS can be used as an ‘umbrella’ to include controls to meet applicable information security standards under a single framework.

ISO27001 Scope

Misconception: It’s all about IT

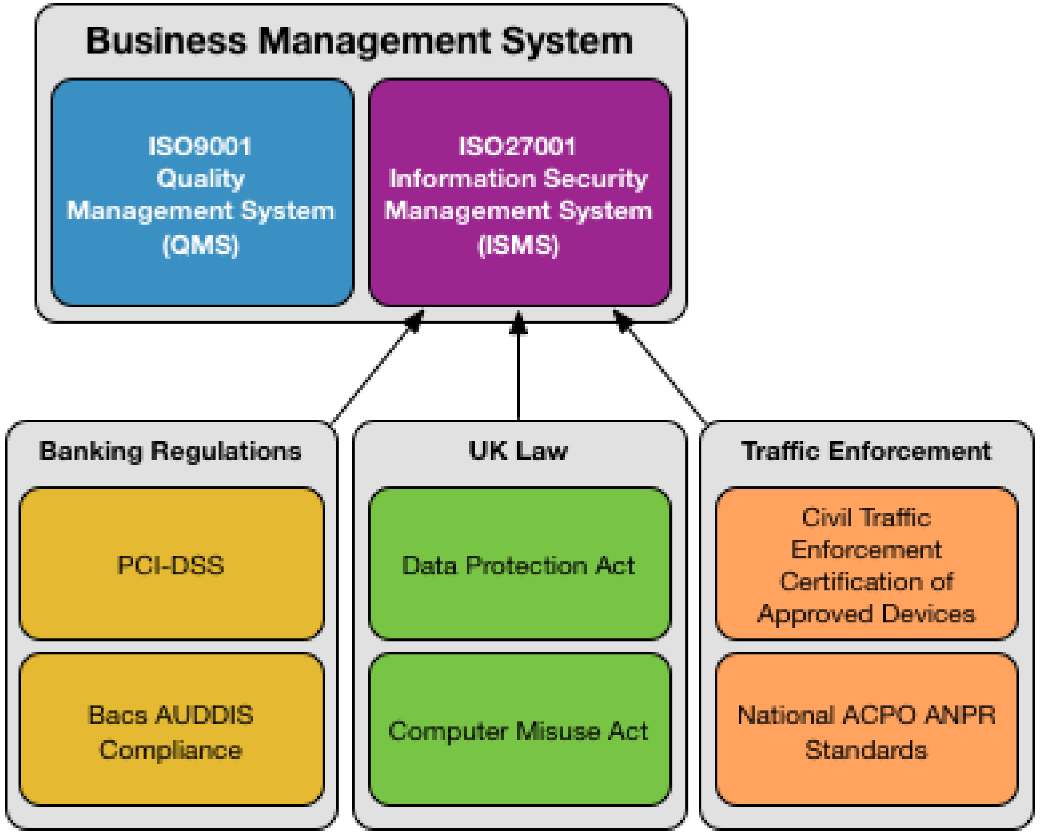
- ISO27001 impacts the whole organization
- It’s important to clearly identify which of the **114** ISO27001 controls are applicable to your organization (Statement of Applicability)

ISO27001 – 114 controls across 14 areas

1. Security policies
2. Organization
3. Human resources
4. Asset management
5. Access control
6. Cryptography
7. Physical & environmental security
8. Operational Security
9. Communications and network security
10. Systems acquisition, development & maintenance
11. Supplier relationships
12. Security incident management
13. Business continuity
14. Compliance

Compatibility with other ISO Standards

- ISO27001 is often implemented alongside other ISO standards (e.g. ISO9001) as part of a wider business management system (BMS).


Business Management System
ISO9001 Quality Management System (QMS)
ISO27001 Information Security Management System (ISMS)
Banking Regulations
PCI-DSS
Bacs AUDDIS Compliance
UK Law
Data Protection Act
Computer Misuse Act
Traffic Enforcement
Civil Traffic Enforcement Certification of Approved Devices
National ACPO ANPR Standards

ISO27001 Certification Path

1. Strategy

- Obtain management backing
- Ensure adequate skills and resources

2. Risk Assessment

- Define scope – people, sites, projects
- Inventory of information assets
- Conduct risk assessment (using a recognized methodology)
- Prepare Statement of Applicability
- Prepare Risk Treatment Plan (ISO27002)

3. ISMS Implementation Phase

- Develop ISMS implementation plan
- Policies
- Procedures
- Technical controls

4. ISMS Operation

- Start operating the ISMS
- Collate evidence (records, logs etc.)
- Carry out internal audits
- 'PLAN, DO, CHECK, ACT' cycles

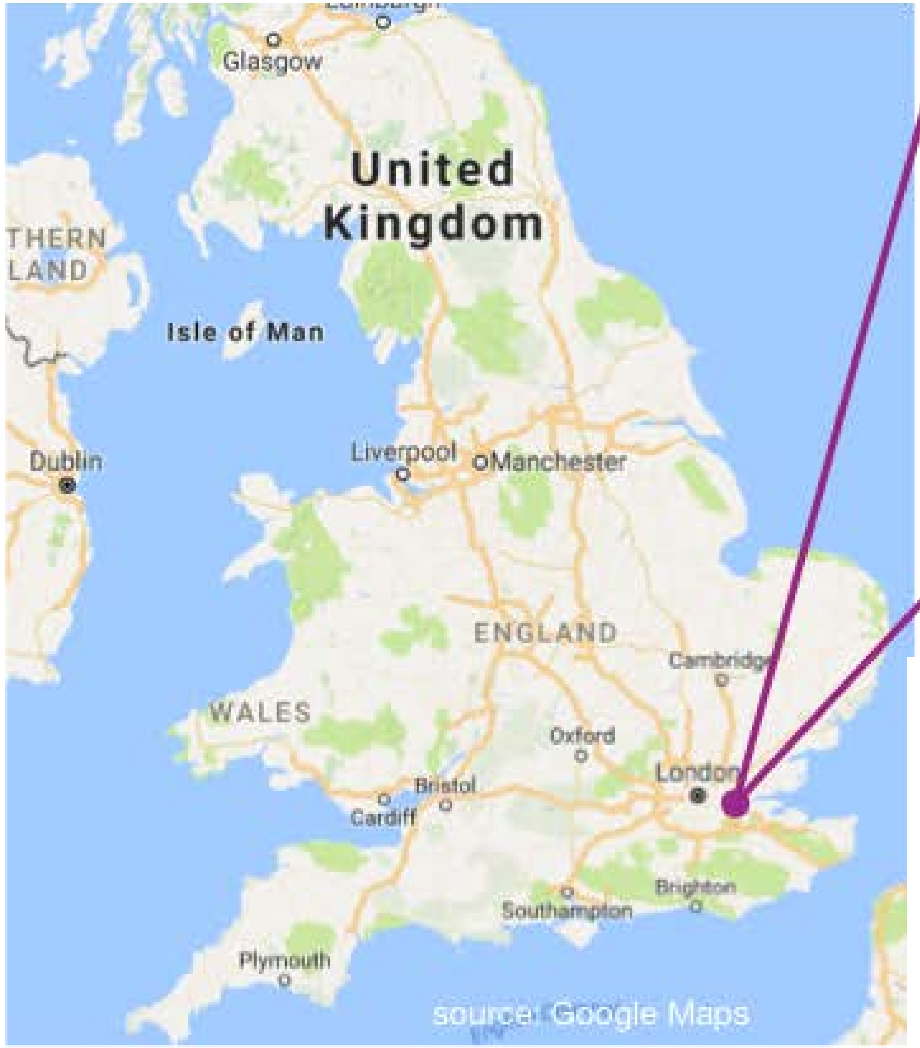
5. Pre Certification

- Internal compliance review
- External Pre-certification assessment
- External Certification audit

6. Post Certification

- Operate the ISMS routinely
- Annual surveillance audits
- Re-certification audit every 3 years

Case Study: Dartford Crossing



Source: Highways England

Dart Charge

- Queen Elizabeth II Bridge (1991)
- 2 tunnels (west: 1963, east: 1980)
- Video free-flow tolling system (since Nov 2014)
- Up to 180,000 toll transactions daily
- ~25,000 payment card transactions daily
- ~1 million account holders
- ~ £100m ($133m) toll revenue per annum

Dartford External Oversight

- **PCI-DSS Level 1**
  - Quarterly external ASV scans
  - Annual on-site audit by QSA and Report on Compliance
- **UK Government Security Policy Framework (SPF):**
  - Formal security risk assessment methodology (IS1/2)
  - Annual penetration testing (external and internal) by government approved (CHECK) security assessor.
  - Annual government cyber security review
- **UK Data Protection Act**
  - Registration with Information Commissioner Office
- **Driver Vehicle and Licensing Authority (DVLA)**
  - Six monthly compliance audits
  - Annual on-site compliance audits
- **Certification of Approved Devices (CoAD)**
  - Certification of data transfer from roadside for evidential purposes by the Vehicle Certification Agency

Key points

- A increasing number of tolling projects are now requiring ISO27001 certification
  - It is becoming an important differentiator for UK Government service providers

- It is expensive to implement ISO27001 on a per-project basis

- A more cost effective strategy would be to attain ISO27001 at an organizational level and increase scope to incorporate new projects at re-certification

- Organizations who have ISO27001 certification will increasingly have a competitive advantage.

Key questions

- Should service providers expect client contracts to pay for their ISO27001 certification?

- Should the onus be on service providers to implement ISO27001 as best practice to protect their own reputation and customer data? The risk ultimately lies with the service provider’s CEO.

- Are we moving to a position where some road tolling projects will only be available to service providers with ISO27001 certification? In the UK and Ireland this seems to already be the case.

emovis
moving technology

Thank you

an Abertis company