THE CHALLENGES, METHODS AND BENEFITS OF IMPLEMENTING OF ISO27001:2013 IN THE NORTHERN IRELAND CANCER REGISTRY

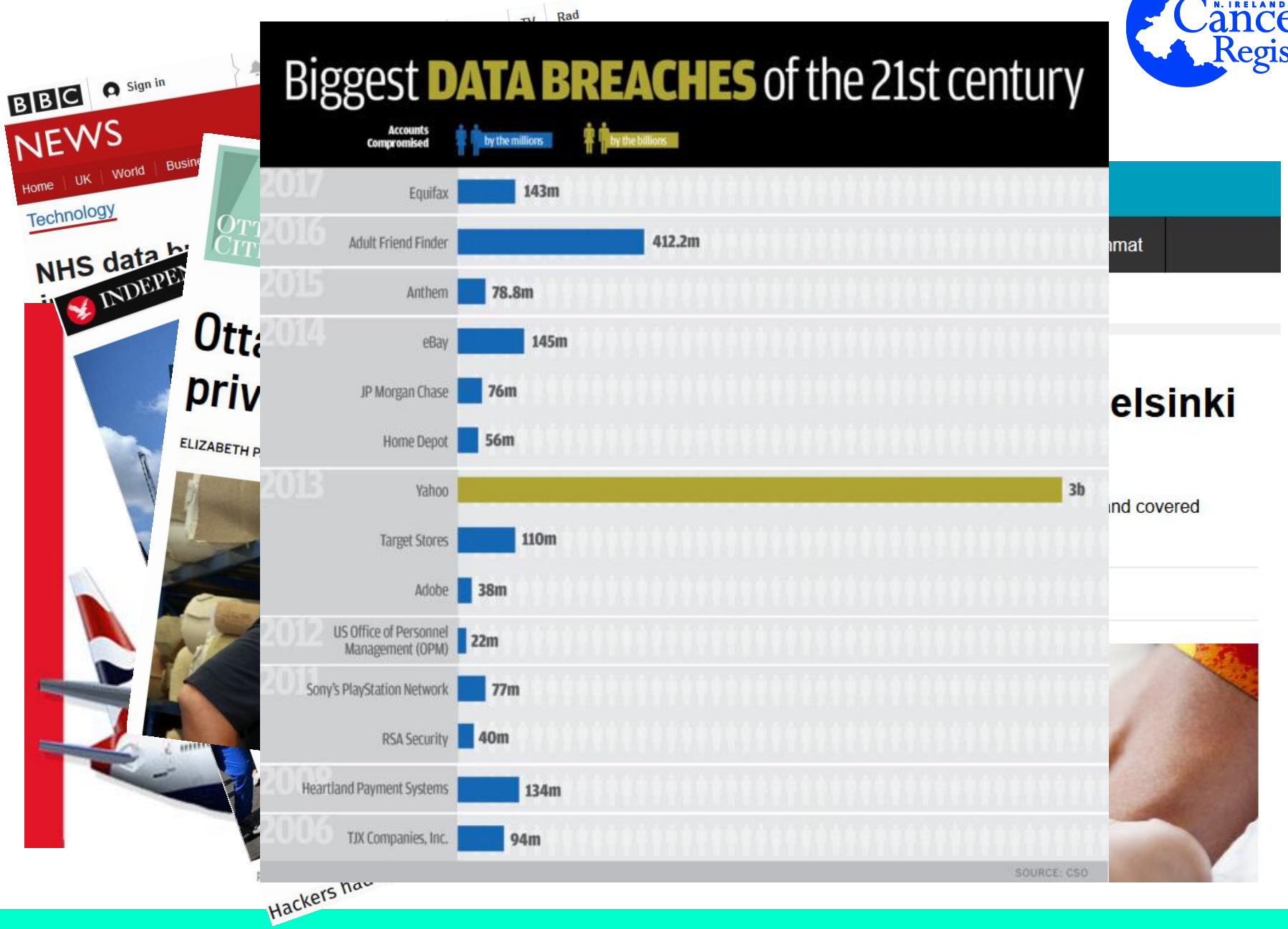
Ronan Campbell MSc

Information Management and Technology Officer

N. Ireland Cancer Registry

Queen's University Belfast

Email: nicr@qub.ac.uk Tel: +44 (0)28 9097 6028 Website: www.qub.ac.uk/nicr



Email: nicr@qub.ac.uk Tel: +44 (0)28 9097 6028 Website: www.qub.ac.uk/nicr

Why did we implement 27001?

- To demonstration that we treat the confidentiality of patient information very seriously.
- Industry best practice for information security.
- Reduced workloads when applying for funding/grants.

- Raise the profile of the organisation.
- Enhance stakeholder confidence.
- GDPR compliance/awareness.
- Internal governance.

What is I

- ISO27001 is sessing the Information MS) of an organisation
- 𝐼𝑆𝑂 (ISOS
- Policies, pro d by an externally accredited b
- Certifies tha ecurity practices meet the sta
- 3 Year certif
- Looks for ev and continu

CERTIFICATE OF REGISTRATION

This is to certify that

Northern Ireland Cancer Registry
Centre for Public Health, Mulhouse Building
Grosvenor Road
Belfast
Northern Ireland
BT12 6DP

has been audited and found to meet the requirements of standard
ISO/IEC 27001:2013 Information Security Management Systems Requirements

Scope of certification

The collection, processing, storing and sharing of information regarding instances of cancer and premalignant disease in Northern Ireland in line with all legal, regulatory and ethical obligations from the Mulhouse Building in Belfast.

Statement of applicability: Version 1, November 2016)

Certificate number: 191
Issue number: 2017-01
Certificate start date: 1 June 2017
Certificate expiry date: 31 May 2020
Date of initial certification: 1 June 2017

Karen Prendergast
Sector Director - Certification
Exova BM TRADA

Exova (UK) Ltd, (T/A Exova BM TRADA), Chiltern House, Stocking Lane, High Wycombe, Buckinghamshire, HP14 4ND, UK
Registered Office: Exova (UK) Ltd, Lochend Industrial Estate, Newbridge, Midlothian EH28 8PL United Kingdom. Reg No. SC070429.

This certificate remains the property of Exova (UK) Ltd. This certificate and all copies or reproductions of the certificate shall be returned to Exova (UK) Ltd or destroyed if requested. Further clarification regarding the scope of this certificate and verification of the certificate is available through Exova BM TRADA or at the above address or at www.exovabmtrada.com

The use of the UKAS accreditation mark indicates accreditation in respect of those activities covered by the accreditation certification 012

© International Organisation for Standardisation

NICR ISO27001 Scope and Context

- **NICR Scope Statement**

  "The collection, processing, storing and sharing of information regarding instances of Cancer and premalignant disease in Northern Ireland in line with all legal, regulatory and ethical obligations from the Mulhouse Building in Belfast. "

- **Aligns with the legal, statutory and regulatory business objectives of the organisation**

  The NICR units (TVO, Statisticians, IT etc) work together to gather, analyse, report and assure the information which this ISMS is designed to help safeguard.

The CIA triad.

Confidentiality is assurance of data privacy.

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle.

Availability is assurance in the timely and reliable access to data services for authorized users.

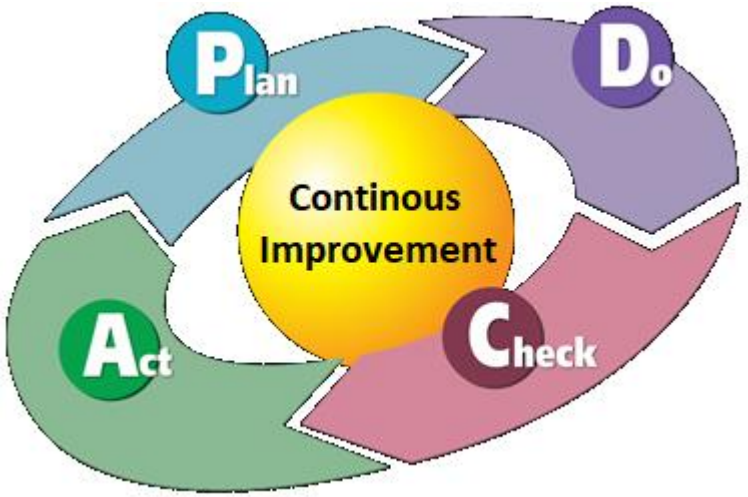
The implementation Process

- Implementation project training.
- Management buy-in
- Enlisting outside experience
- Identification of information assets
  - Identify threats and vulnerabilities
- Risk Assessment matrix
  - Treat/Tolerate/Transfer
- Risk treatment options
  - Physical/Logical/Administrative

- ISO27001 Certified ISMS Lead Implementer
- Certified in Information Security Management Principles
- ISACA Certified Information Systems Manager

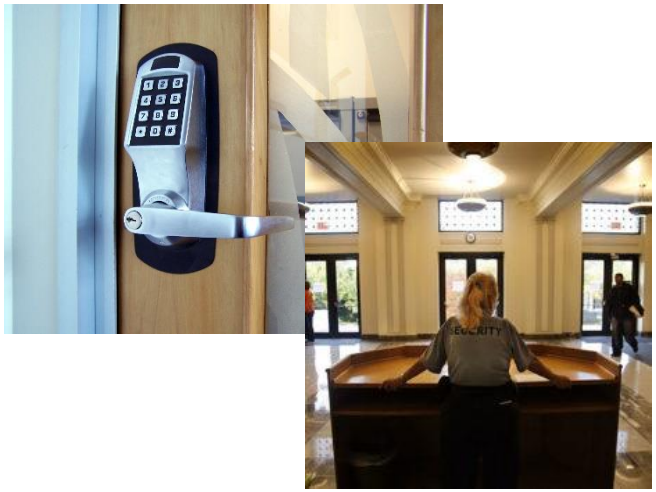
bcs The Chartered Institute for IT
Professional Certification

CISM



Risk Treatments

- Physical
  - Door locks
  - CCTV
  - Segregated secure working areas



- Logical
  - Passwords/Biometrics
  - Network Access
  - Encryption
  - Firewalls

- Administrative
  - Policy
  - Awareness/Training
  - Segregation of duties

Implementation Continued

- Staff Awareness & Training.
- Policy development and implementation.
- Process reviews.
- Internal Auditing.

- Enlisting external accreditation body.
- External/Certification Audit.
- Continual maintenance.

Benefits and Outcomes

- Focussing the attention of staff and management in information security processes.
- Stakeholder confidence and peer reputation.
- Process integration.

- Supporting documentation when applying for grants and projects.
- Success for the organisation!

Email: nicr@qub.ac.uk Tel: +44 (0)28 9097 6028 Website: www.qub.ac.uk/nicr

Thank you.

r.campbell@qub.ac.uk

Any Questions?

N. Ireland Cancer Registry

Queen's University Belfast

Email: nicr@qub.ac.uk Tel: +44 (0)28 9097 6028 Website: www.qub.ac.uk/nicr