# Information governance and cake

15 November 2016

@AdaptaforNFP

adapta
processes, people and technology

INSTITUTE OF CONSULTING
RECOGNISED PRACTICE

2016 MemberWise Recognised Supplier

# Adapta Consulting

We are:

- A specialist information systems consultancy
- We only work with membership organisations, charities, associations, trusts and others in the NfP sector
- We are completely supplier-independent
- Our consultants have held senior positions in a broad range of different organisations
- Our advice and guidance is based on practical experience gained over many years.

# Programme

| | |
|---|---|
| 14.00 | **Arrival and welcome**<br>Iain Pritchard – Adapta Consulting |
| 14:05 | **The Data Protection Act**<br>Fiona Brookes, Adapta Consulting<br>Fiona will give an overview of the Data Protection Act and its implications. |
| 15.00 | **Case studies**<br>Richard Norman, Director of Information Governance & Risk Management, British Council<br>Martyn Croft, CIO, Salvation Army UK Territory |
| 16:00 | **Discussion and feedback**<br>A round table discussion and feedback to draw our further best practice learning. |
| 16.45 - 17.00 | **Review and close**<br>Iain Pritchard – Adapta Consulting |

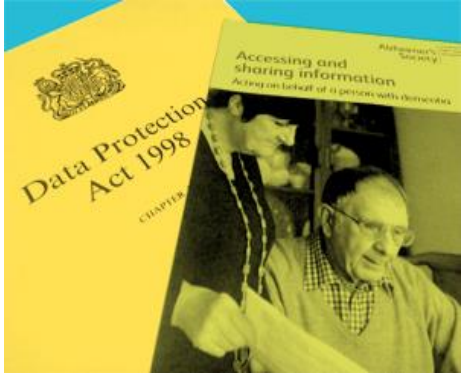
# The Data Protection Act

Fiona Brookes

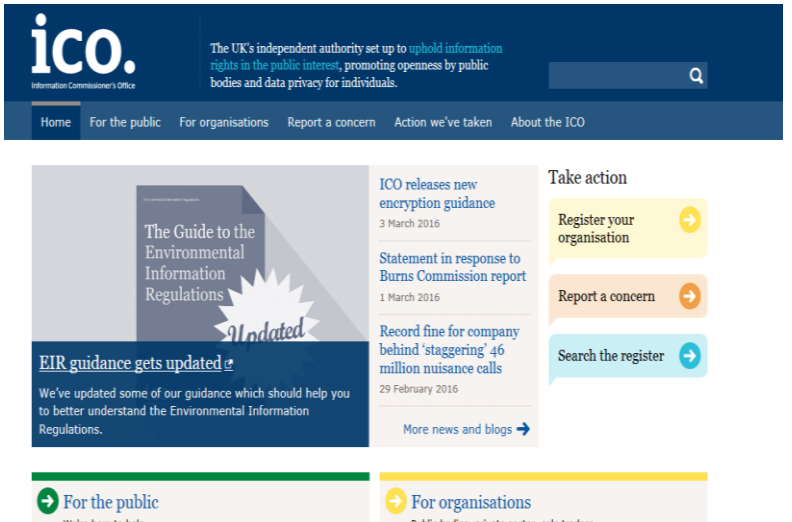
Associate, Adapta Consulting

adapta

# Introduction




- Data Protection Act 1984 and 1998 – in place for 30+ years
- Governed by the Information Commissioner
- Provides rules for organisations that collect and use personal information – applies to manual and electronic records
- EU General Data Protection Regulation (GDPR) comes into force in May 2018 …. We will have to comply regardless of Brexit
- GDPR builds on DPA but there are  significant changes too

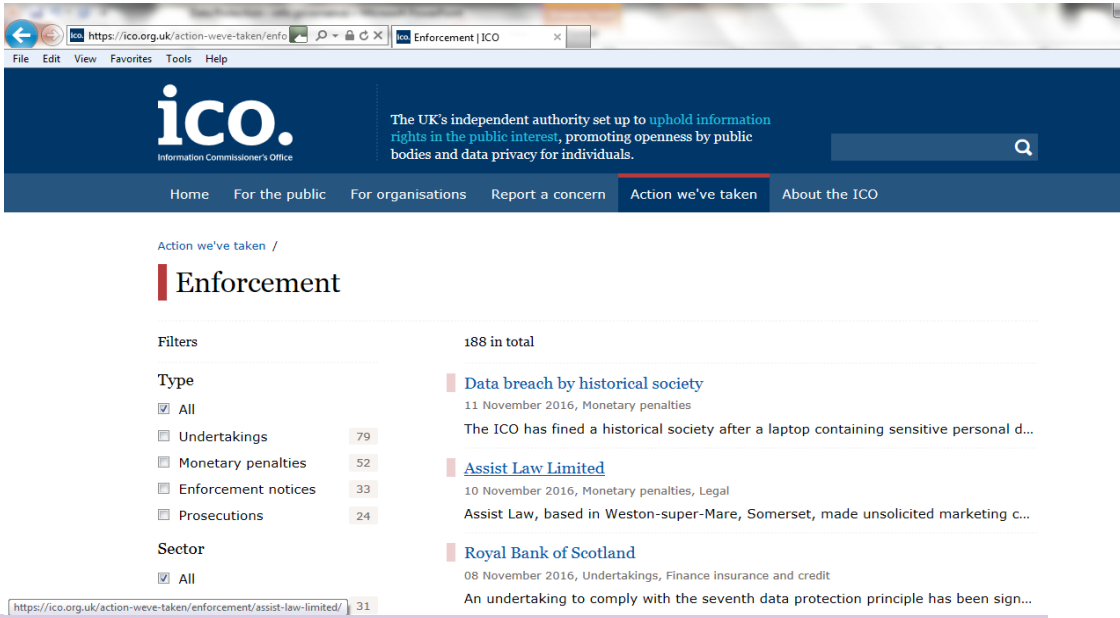



DATA DAY PROTECTION

# When things go wrong

- Investigation
- Enforcement
- Fines – up to £500k
- Criminal prosecution
  - Serious contravention of the Act
  - Causing substantial damage and / or distress
  - Deliberate or should have know better






*Everyone's got to stick to the law, and if the law's been broken then we will act*
*Information Commissioner, 2 September 2015*

# When things go wrong … some examples

- The Nursing and Midwifery Council … **lost dvds** … unencrypted.. £150k fine
- North East Lincolnshire Council … missing **unencrypted memory stick** …£80k fine
- Greater Manchester Police … **stolen USB stick** … unencrypted, no password protection … £150k fine
- Royal Veterinary College … **loss of a memory card** … signed undertaking
- British Pregnancy Advice Service … **hacked database** … £200k fine
- Surrey County Council … **misdirected emails** with attached files … not encrypted or password protected … £120k fine
- North Somerset Council … sent **unencrypted emails** with personal data to wrong NHS employee … £60k fine


adapta

# The Act

**Processing** -includes obtaining, recording, retrieval, consultation, holding, disclosing, using

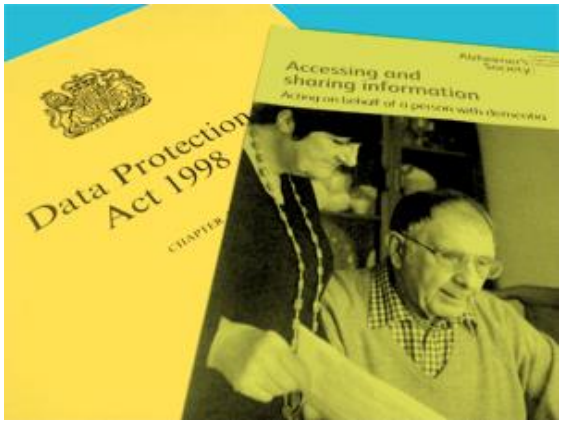
**Personal data** - information, facts or opinions, about a living individual which identifies the individual concerned - the data subject

**Sensitive personal data** - information or opinions about a living individual and relating to:

- Racial or ethnic origin
- Political opinions / trade union membership
- Religious beliefs
- Health
- Sex life
- Criminal proceedings or convictions


adapta

# Complying with the Act



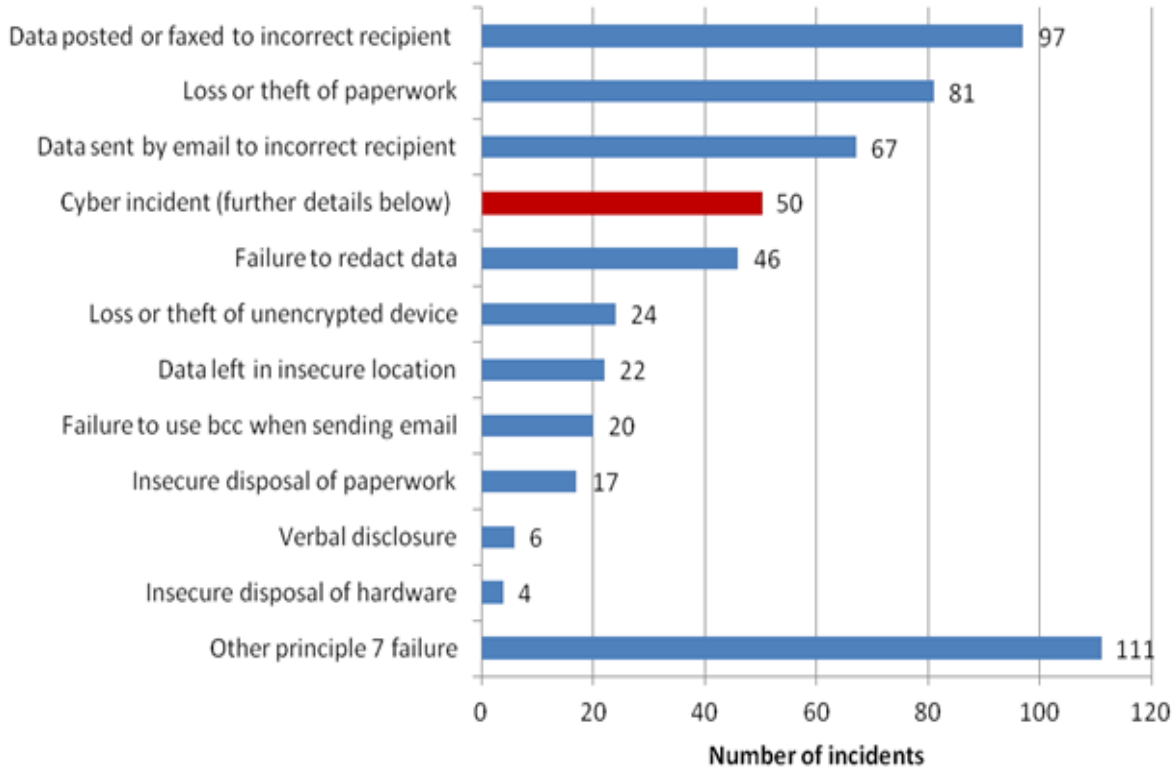

When processing personal and sensitive personal data we have to comply with the 8 principles:

1. Data must be collected lawfully and fairly
2. It must be used only for specified purposes
3. The quantity of data collected should be appropriate
4. The data should be accurate and up to date
5. It should be kept only as long as necessary
6. It should be processed in accordance with the rights of those it concerns
7. It should be kept securely
8. It should not be transferred out of the EEA unless it is to an area which has similar standards

adapta

# Key areas of risk


- Personal data – accuracy, appropriate, up to date, kept only as long as necessary
- Remote working
- Human error
- Volunteers
- Transferring data
- Emails
- Data processors




adapta

# The GDPR changes

Faster reporting of data breaches

Right to be informed

Faster subject access

Active consent

Right to erasure

Data protection impact assessments

Right to rectification

Accountability & governance

**Portability**

€20 million fines

Demonstrate consent

Recent consent

Privacy by design

*'If the UK wants to trade with the single market on equal terms we would have to prove "adequacy" – in other words UK data protection standards would have to be equivalent to the EU's General Data Protection Regulation framework starting in 2018.' ICO*

## The consequences of non compliance

- Reputational damage
- ICO enforcement notice
- ICO fines of up to £500k

## The benefits of compliance

- Improved business processes
- Less data, more accurate and up to date data
- Supporters' data is more secure
- Peace of mind


*There is a danger here of blackening a whole sector. Charities seem to be becoming the new dirty word, and that clearly isn't fair. But the rules on data protection and the rules about privacy and electronic communications apply to all who are processing data, whether businesses or charities. Everyone's got to stick to the law, and if the law's been broken then we will act*
*Information Commissioner, 2 September 2015*

adapta

# Minimising the risk of non compliance

- Compliance review – data handling processes
- Implement appropriate policies & procedures
- Tell people what you are doing with their personal data
- Encrypt all portable devices
- Staff & volunteer training
- Plan & prepare for GDPR


*'A key part of data protection legislation is to defend the rights of vulnerable people. Companies and organisations have a duty to keep people's data safe and are not allowed to simply hand out or consult on personal information without proper care or an individual's permission. In this way the DPA plays an important part in protecting vulnerable people'  Judith Jones, ICO*

adapta

# Information Risk Management Frameworks and Certifications

Information Governance and Cake
15 November 2016


Richard Norman

CISM, CRISC, CISA, CGEIT, FAIR Institute Charter Member


# There is a high risk of a virus infection!

| | | | |
|---|---|---|---|
| H | | | X |
| M | | | |
| L | | | |
| | L | M | H |


Image credit: http://www.mystudycorner.net/wp-content/uploads/2015/09/computer-virus-removal1.jpg

# Very Common

- Frustrated security team
- Frustrated management
- Information security spend led by vendors, other organisations etc.
- Very difficult to rank risk scenarios for treatment
- Prioritisation by crisis
- Information security viewed as a 'drag' on the business

# FAIR methodology

Factor Analysis of Information Risk is a quantitative risk assessment methodology to help address this.


photo credit: Dennis Yang (flickr.com)


Photo credit: http://www.ebay.com/gds/How-to-Attach-a-Tire-Swing-to-a-Tree-/10000000205290311/g.html


photo credit: Tom Bech (flickr.com)


photo credit: dfinnecy (flickr.com)

# The Bald Tire Scenario Analysis

Identify the components in this scenario:

- Threats
- Vulnerabilities
- Risk

Credit: http://www.slideshare.net/pjbeyer/risk-explained-in-5-minutes-or-less and http://www.risklens.com/hubfs/Resource_Center/The_Bald_Tire_Scenario_White_Paper_RiskLens.pdf

# Asset

- Risk depends on the ASSET
- How many ASSETS did you consider?
- What is/are the ASSET/S?
- The ASSET is the bald tire

# Threat

- Risk depends on the THREAT
- How many THREATS did you consider?
- What is/are the THREAT/S?
- The THREAT is the earth and the force of gravity that it applies

# Vulnerability

- Risk depends on the VULNERABILITY
- How did you consider VULNERABILITY?
- VULNERABILITY depends on the THREAT
- The potential VULNERABILITY is the frayed rope

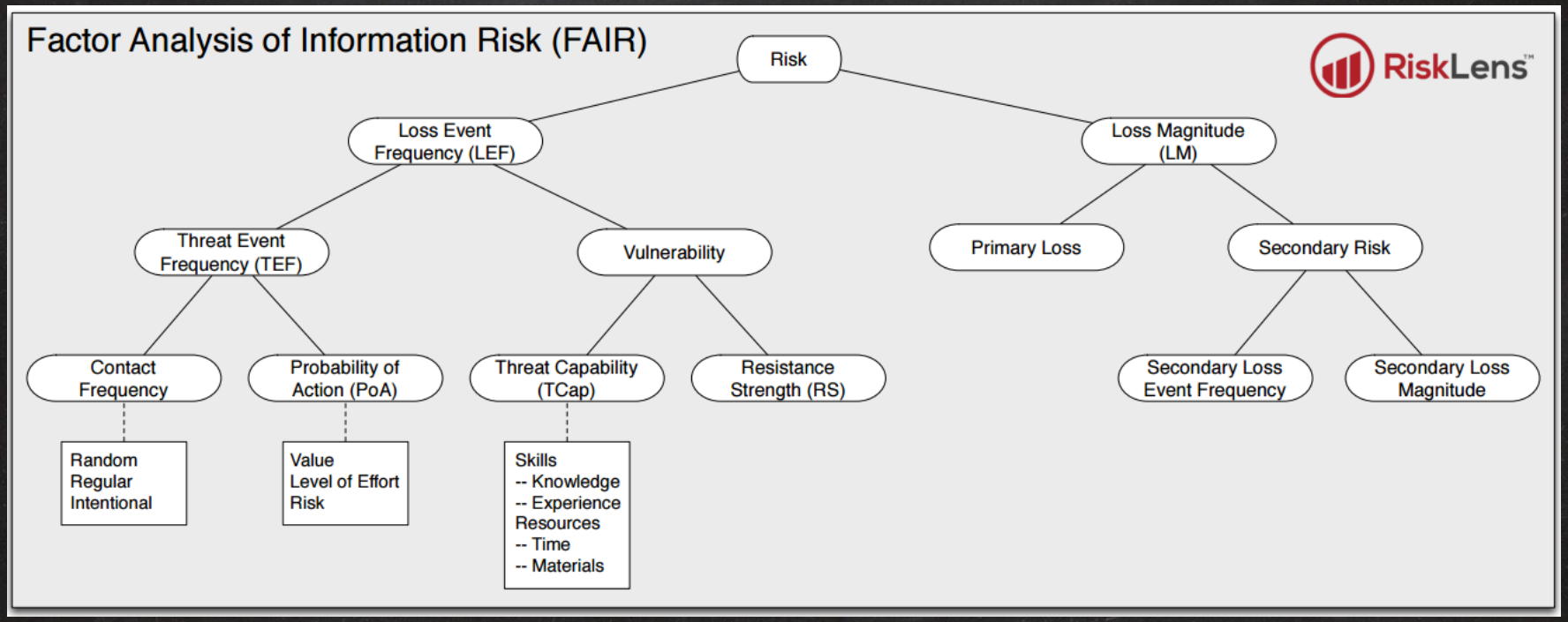
# RISK

The probable frequency and probable impact of future loss

# Risk Analysis

- Risk is a derived value
- Risk is a probability issue
- Risk has both a frequency and a magnitude component
- The fundamental nature of Risk is universal, regardless of context

# FAIR Ontology



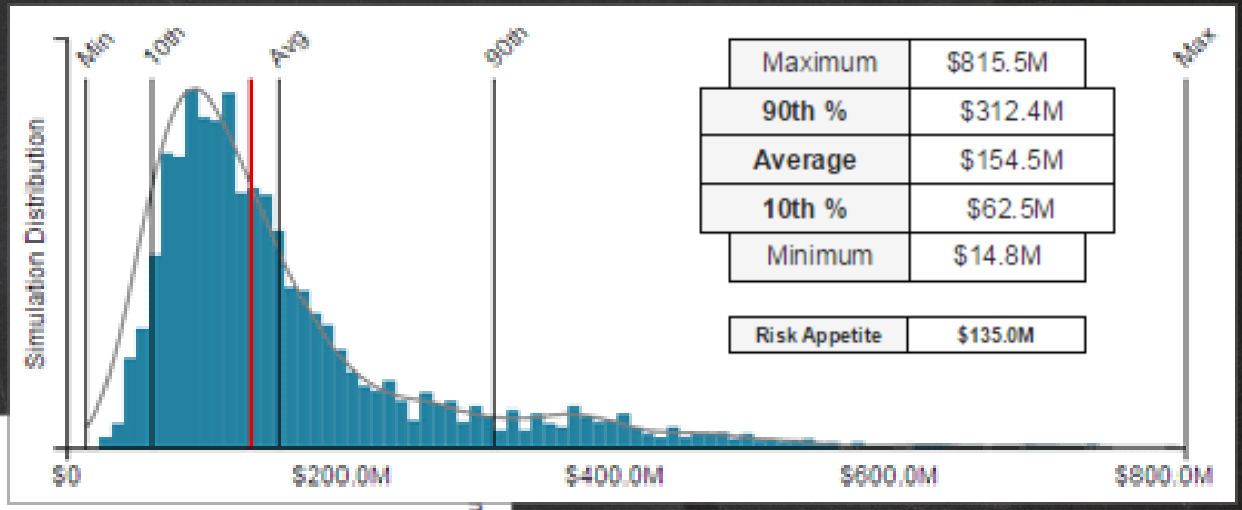

Source: http://www.risklens.com/hubfs/Resource_Center/FAIR_on_a_Page_RiskLens.pdf

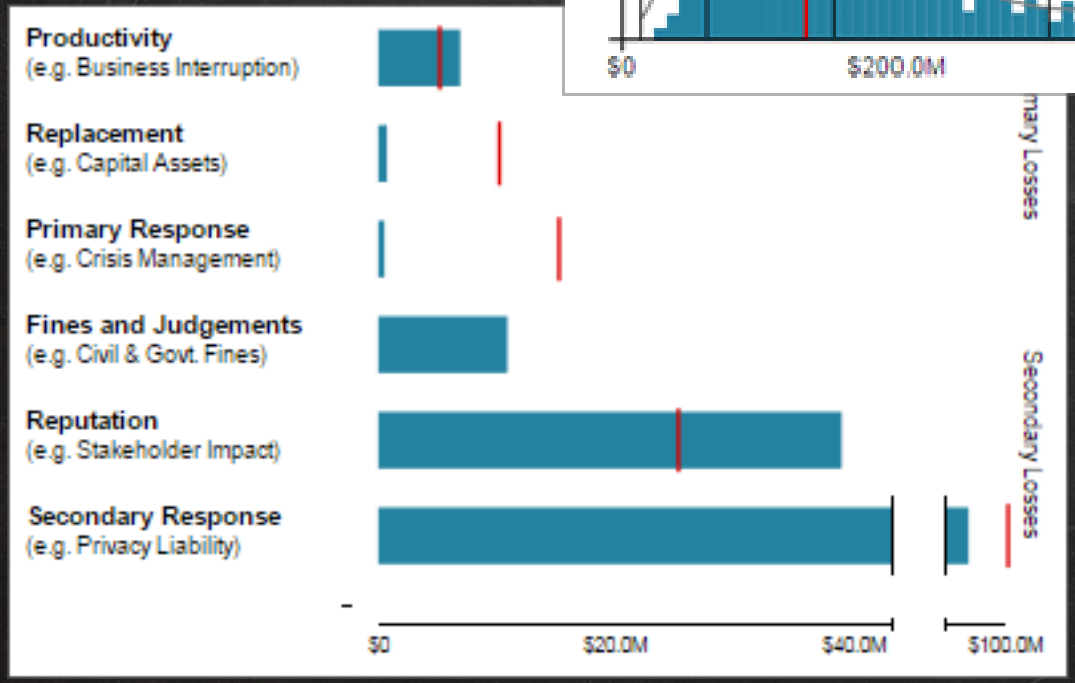
# Open & Accessible

- FAIR adopted by The Open Group
- Training and certification
- Can be programmed in Excel
- Helps 'techies' talk in 'business' terms
- Flexible & reusable


http://www.opengroup.org/subjectareas/security/risk

# Or commercial

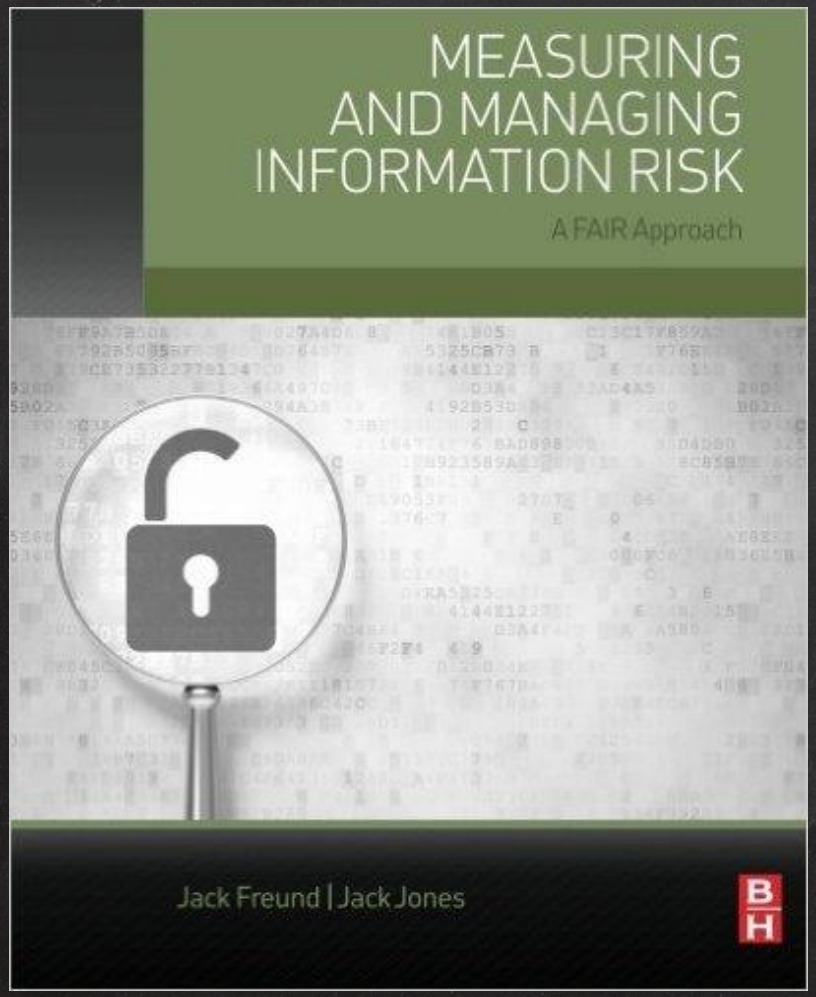


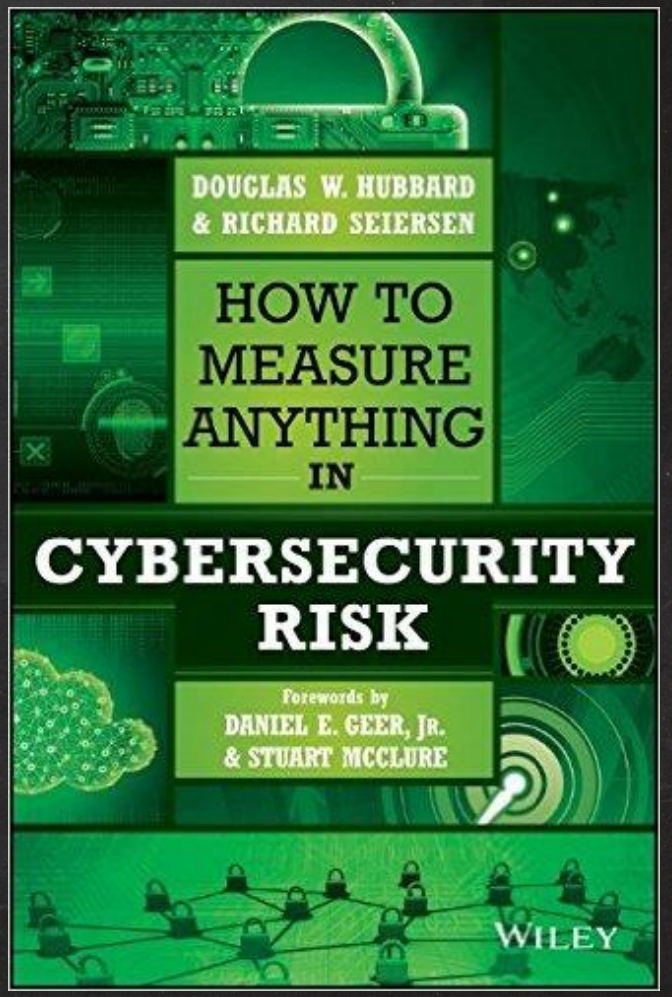




RiskLens™

http://www.risklens.com/

# Further Reading



# CRISC

Certified in Risk and Information System Controls

Benefits for organisations:

- Greater understanding of IT risk and how it relates to whole organisation
- More effective organisational risk management plans
- Common organisational perspective and language about IT risk

# CRISC


**2.** *2016 IT Skills and Salary Survey* conducted by *Global Knowledge*

# QUESTIONS?

InfoSec@rnorman.org

https://www.linkedin.com/in/richardgnorman

# Information Security

*in the third sector*

Martyn Croft

CIO, The Salvation Army UK Territory
Co-founder, Charities Security Forum

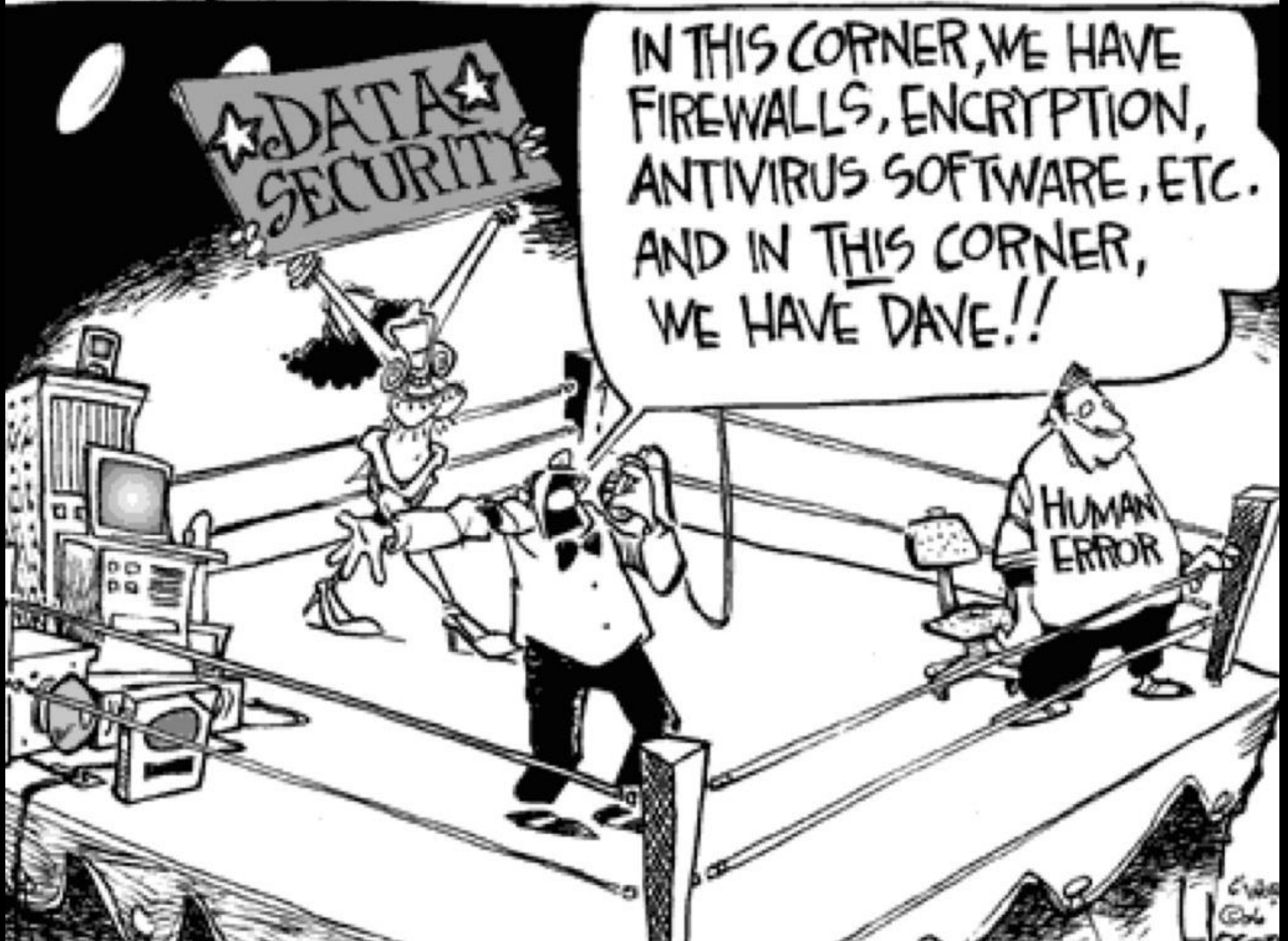
Charities don’t need security…

…do they?

# The Salvation Army

a Church and a Charity


SOUTHSIDE CHURCH OF CHRIST
GOD NEVER TURNS OFF HIS SECURITY SYSTEM
WORSHIP ASSEMBLY 9:00 AM
BIBLE CLASSES 10:30 AM
EVENING SERVICES :00 PM
WEDNESDAY SERVICES 7:00 PM
OFFICES


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR


# USER SKILLS

## EVERYONE'S AN IT EXPERT

“UK Charities hold information on 3 in 4 people. How would YOU feel if your personal data was stolen and put on the internet for all to see?”

giveaday.co.uk

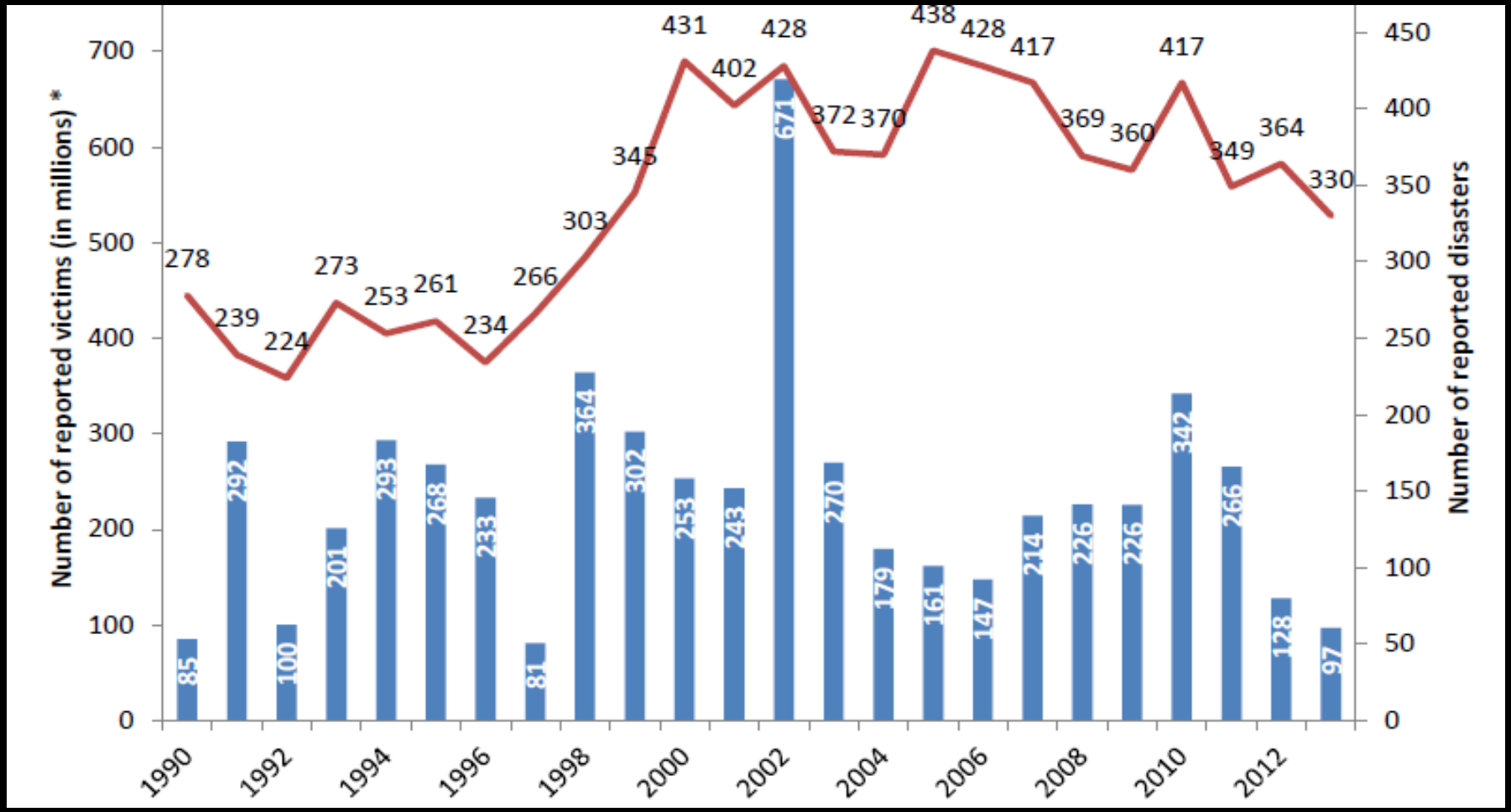

Make it easy to do the right thing


POLYB

44% of the UK population
donated £10.6bn
to charities

15% by online, 11% by text

CAF UK Giving 2014




## Victims & Disasters

Centre for Research on the Epidemiology of Disasters – 2013
cred.be

“Fake charities (scammers) will try to take advantage of your generosity and compassion for others in need.”

people help by giving money

# Philanthropic Phishing ©2015

# and predictably…

## Katrina heralds wave of phishing fraud

Share this article:

Spammers and phishers hoping to profit from hurricane Katrina have been waging a week-long email campaign.

With depressing predictability, fake Red Cross and other charity donation sites have been set up to con users out of money and emails containing malware are being spammed under the guise of Katrina news.

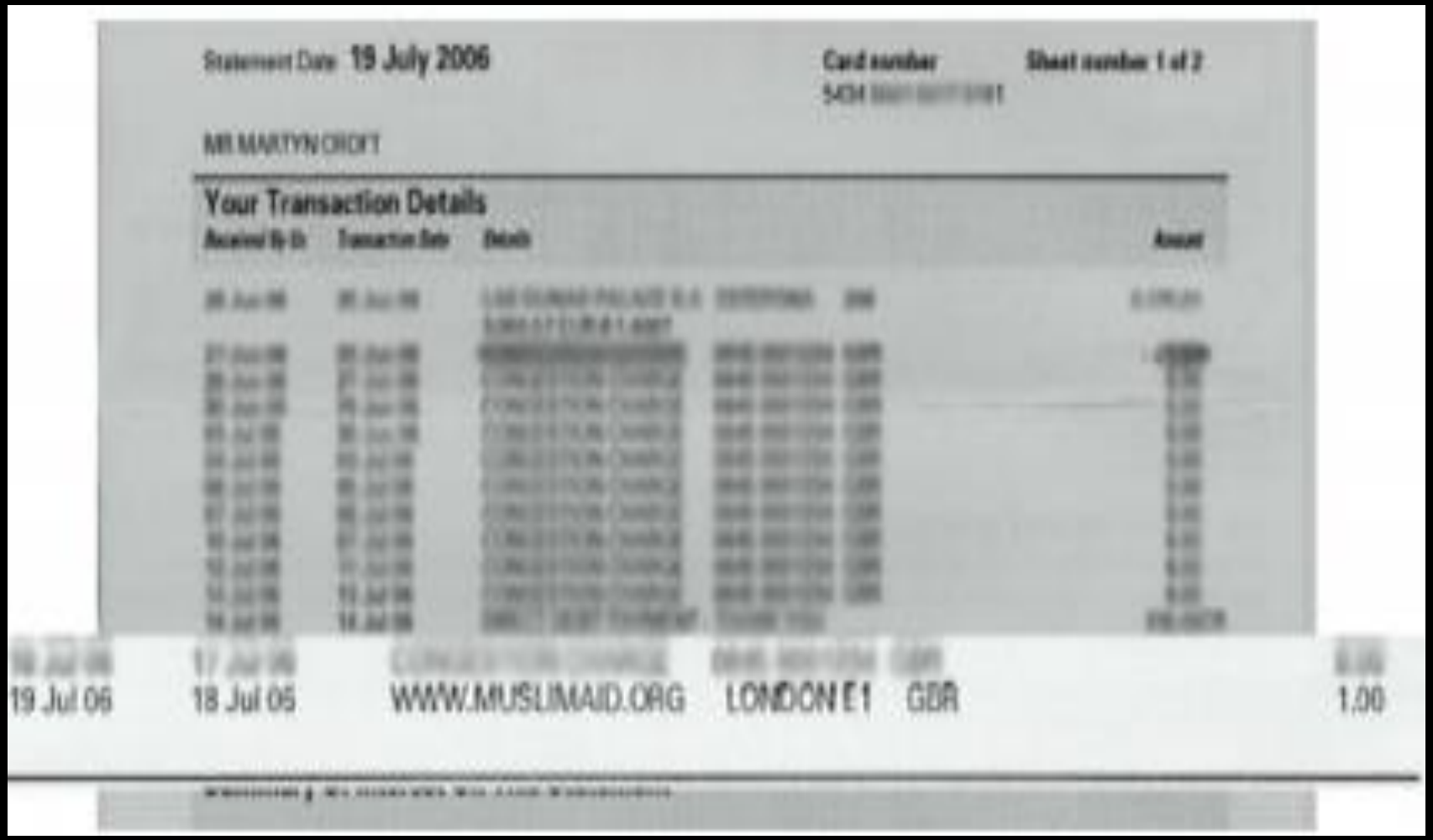
"This is not the first time we have seen immoral opportunists take advantage of a natural disaster to fill their pockets with money meant for victims," said Carole Theriault, security consultant at antivirus company Sophos. Back in January SC reported internet criminals were cashing in on the Asian tsunami disaster.

But the swathe of Katrina scams took a little longer than expected to arrive in user inboxes. According to SurfControl, such scams typically occur within two to three days of the event, but a lack of public awareness and electrical blackouts may have slowed spammers and phishers hoping to benefit from hurricane Katrina.

In the latest scam, an email pretending to be from the Red Cross directs users to a spoofed website that looks very similar to the real American Red Cross Hurricane relief fund website. But any donations will only end up in the pockets of criminals.

# What to do with your stolen cards?

# Philanthropic Phishing©



Statement Date 19 July 2006

Card number

Sheet number 1 of 2

MR MARTYN CROFT

Your Transaction Details

| Posting By Dt | Transaction Date | Details | | | Amount |
|---|---|---|---|---|---|
| 19 Jul 06 | 18 Jul 05 | WWW.MUSLIMAID.ORG | LONDON E1 | GBR | 1.00 |

A recent survey of Charity Security Forum members indicated that whilst a breach of the donor database was top of their threat list, close behind was the loss of beneficiaries' personal information.

"Almost every charity is custodian of extremely sensitive personal information ranging from sex abuse and child abuse to health issues like cancer, mental illness and diabetes.

The problem is, in Cyberspace, most, if not all charities have this immensely personal and sensitive information exposed and often inadequately protected, making them an easy target for the cyber attacker."

Amar Singh, CEO of GiveADay

# cyber attack maps

# Security risk checklist

- ❑ How easy is it to get access to the system?
- ❑ Is physical access limited, particularly to critical components?
- ❑ Are there any physical hazards which might disrupt systems?
- ❑ What are the opportunities for physical tampering?
- ❑ What is the access control policy?
- ❑ What security is applied to network connections to systems?
- ❑ What are the interactions between systems?
- ❑ Do the systems produce audit trails?
- ❑ How many people can move files and data to/from systems ?
- ❑ What controls are in place to ensure data integrity and reliability?
- ❑ To what extent can the system be used for fraud?
- ❑ To what extent will professional hackers want to gain access?
- ❑ What's  the level of staff turnover?

# Cyber Essentials

1. Boundary firewalls and internet gateways
   designed to prevent unauthorised access to or from private networks, but good setup is important for them to be fully effective
2. Secure configuration
   ensuring that systems are configured in the most secure way for the needs of the organisation
3. Access control
   ensuring only those who should have access to systems do have access, and at the appropriate level.
4. Malware protection
   ensuring that virus and malware protection is installed
   and is up-to-date
5. Patch management
   ensuring the latest supported version of applications is used and all the necessary updates have been applied

## Self-Assessment Questionnaire

Cyber Essentials sets out five security controls which will help all organisations protect themselves against the most common cyber threats. Take this quick test to give you an idea of how you measure up. You can then decide whether to apply for one of the Cyber Essentials badges.

Question 1 of 13

What size is your business?
Small (up to 50 employees)
Medium (50 – 249 employees)
Large (Over 250 employees)

SMALL MEDIUM LARGE

https://www.cyberstreetwise.com/cyberessentials/#questionnaire

# Charities Security Forum

*“The premier group for Information Security Professionals working in the charity sector. The group has representatives from many major and household name charities and meets quarterly in London.*

*Its members participate in discussions and presentations on information security issues of particular relevance and importance to the not-for-profit sector.*

*Its annual conference has become a must-attend event”*


Brian Shorten

Martyn Croft

www.charitiessecurityforum.org.uk

# Copyright and Credits

# Discussion and feedback

adapta

# Review and close

Presentations will be available to download from the Adapta website soon

**www.adaptaconsulting.co.uk**

adapta
*processes, people and technology*

INSTITUTE OF CONSULTING
RECOGNISED PRACTICE

2016 MemberWise Recognised Supplier