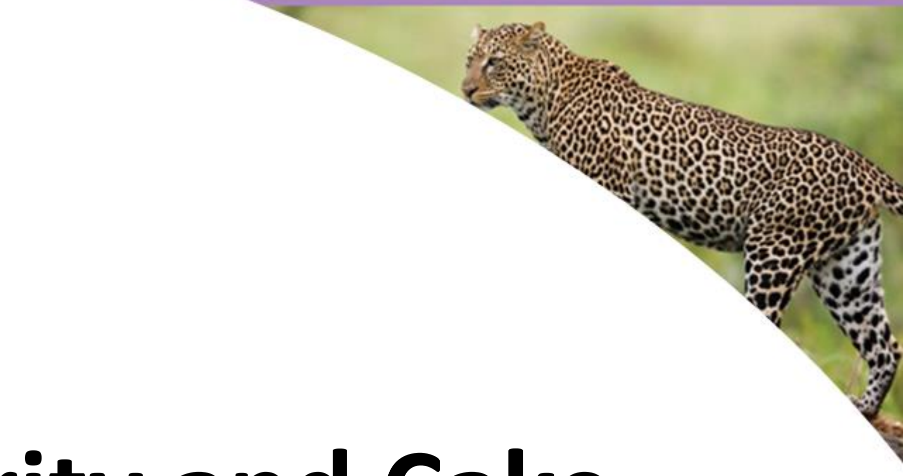


Information Security and Cake

22 November 2017

@AdaptaforNFP

adapta
processes, people and technology

INSTITUTE OF CONSULTING
RECOGNISED PRACTICE

2017 MemberWise Recognised Supplier

Programme

14.00	**Arrival and welcome** Paul Sypko – Adapta Consulting
14:10	**Why we need effective and robust information security in place** Brian Shorten – Charities Security Forum
15:00	**Case studies** Short stories from speakers Jon Vogel, Girls' Day School Trust Andy Fenton, Techrose Consultancy – discussing BHF project
15:50	**Discussion and feedback** All A round table discussion and feedback.
16.30 - 17.00	**Review and close** Paul Sypko – Adapta Consulting

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.

Introductions

Information Security and Cake
November 2017

Brian Shorten *MSc CISSP FBCS*

Chairman – Charities Security Forum

Today’s topic

'Why we need effective and robust information security processes in place'

CHALLENGES -

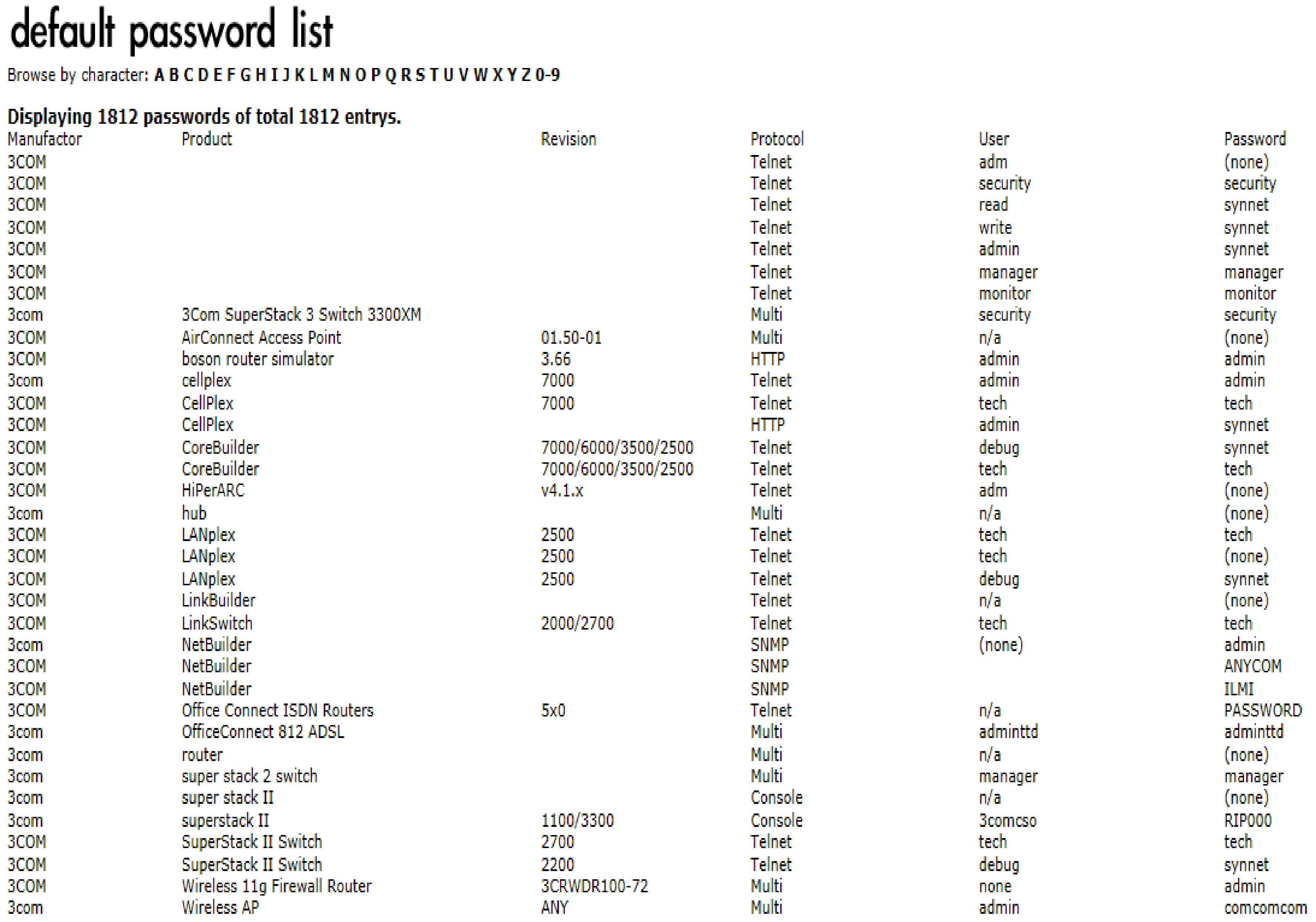
- Media attention impacting reputation
- Data loss impacting the running of the charity
- Donor’s confidence shaken
- Action by ICO
- Action by Charity Commission
- Scam websites

So…

How do we protect the information?

First IT

- Keep your operating system up to date
- Patch regularly
- Don’t forget all applications, printers & WiFi router
- Harden servers
- Access control – least privilege
- Change ALL Default passwords



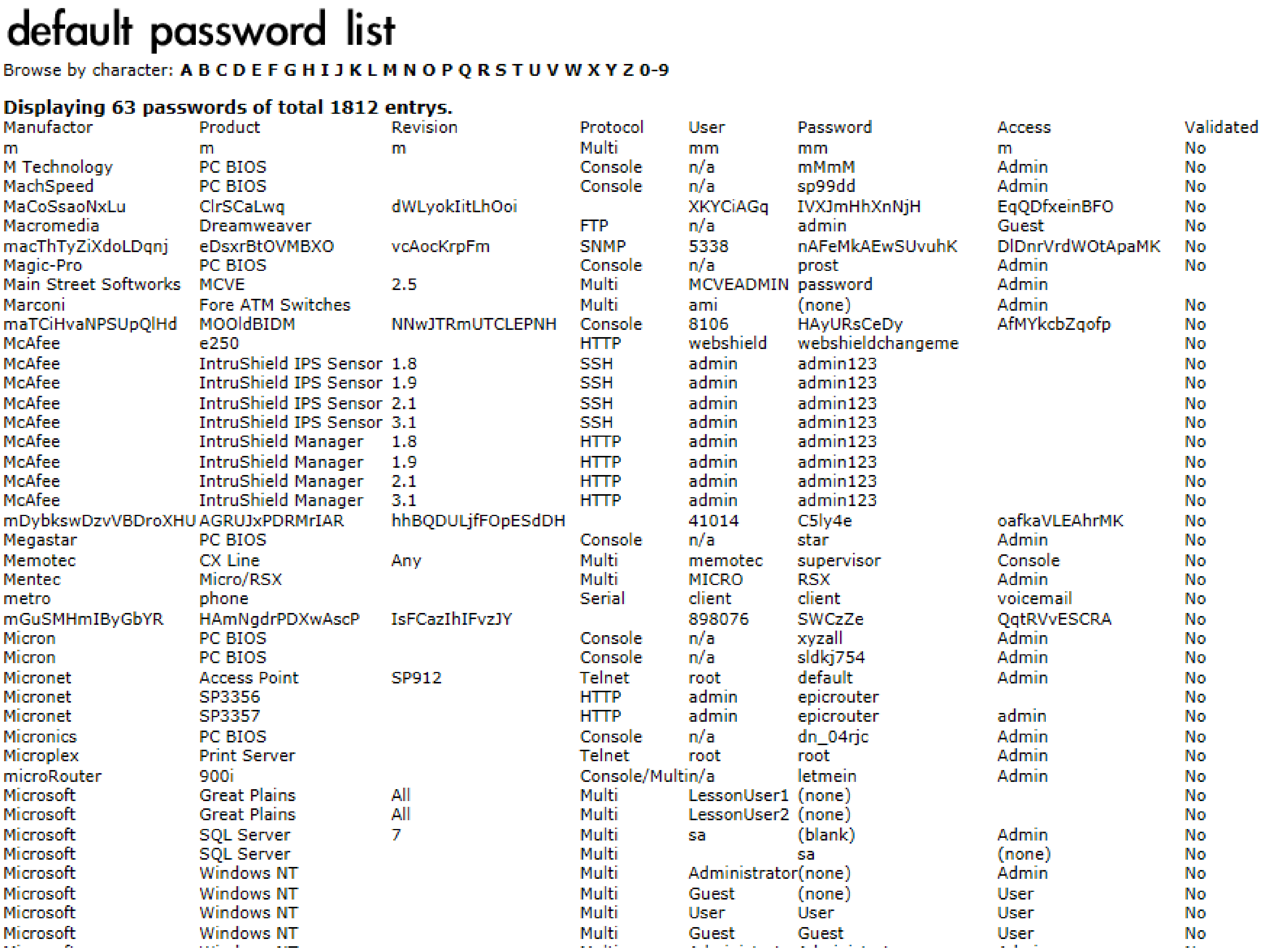
default password list

Browse by character: **A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0-9**

Displaying 1812 passwords of total 1812 entrys.

Manufactor	Product	Revision	Protocol	User	Password
3COM			Telnet	adm	(none)
3COM			Telnet	security	security
3COM			Telnet	read	synnet
3COM			Telnet	write	synnet
3COM			Telnet	admin	synnet
3COM			Telnet	manager	manager
3COM			Telnet	monitor	monitor
3com	3Com SuperStack 3 Switch 3300XM		Multi	security	security
3COM	AirConnect Access Point	01.50-01	Multi	n/a	(none)
3COM	boson router simulator	3.66	HTTP	admin	admin
3com	cellplex	7000	Telnet	admin	admin
3COM	CellPlex	7000	Telnet	tech	tech
3COM	CellPlex		HTTP	admin	synnet
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	debug	synnet
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	tech	tech
3COM	HiPerARC	v4.1.x	Telnet	adm	(none)
3com	hub		Multi	n/a	(none)
3COM	LANplex	2500	Telnet	tech	tech
3COM	LANplex	2500	Telnet	tech	(none)
3COM	LANplex	2500	Telnet	debug	synnet
3COM	LinkBuilder		Telnet	n/a	(none)
3COM	LinkSwitch	2000/2700	Telnet	tech	tech
3com	NetBuilder		SNMP	(none)	admin
3COM	NetBuilder		SNMP		ANYCOM
3COM	NetBuilder		SNMP		ILMI
3COM	Office Connect ISDN Routers	5x0	Telnet	n/a	PASSWORD
3com	OfficeConnect 812 ADSL		Multi	adminttd	adminttd
3com	router		Multi	n/a	(none)
3com	super stack 2 switch		Multi	manager	manager
3com	super stack II		Console	n/a	(none)
3com	superstack II	1100/3300	Console	3comcso	RIP000
3COM	SuperStack II Switch	2700	Telnet	tech	tech
3COM	SuperStack II Switch	2200	Telnet	debug	synnet
3COM	Wireless 11g Firewall Router	3CRWDR100-72	Multi	none	admin
3com	Wireless AP	ANY	Multi	admin	comcomcom

http://www.defaultpassword.com/



default password list

Browse by character: **A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0-9**

Displaying 63 passwords of total 1812 entrys.

Manufactor	Product	Revision	Protocol	User	Password	Access	Validated
m	m	m	Multi	mm	mm	m	No
M Technology	PC BIOS		Console	n/a	mMmM	Admin	No
MachSpeed	PC BIOS		Console	n/a	sp99dd	Admin	No
MaCoSsaoNxLu	ClrSCaLwq	dWLyokIitLhOoi		XKYCiAGq	IVXJmHhXnNjH	EqQDfxeinBFO	No
Macromedia	Dreamweaver		FTP	n/a	admin	Guest	No
macThTyZiXdoLDqnj	eDsxrBtOVMBXO	vcAocKrpFm	SNMP	5338	nAFeMkAEwSUvuhK	DlDnrVrdWOtApaMK	No
Magic-Pro	PC BIOS		Console	n/a	prost	Admin	No
Main Street Softworks	MCVE	2.5	Multi	MCVEADMIN	password	Admin	
Marconi	Fore ATM Switches		Multi	ami	(none)	Admin	No
maTCiHvaNPSUpQlHd	MOOldBIDM	NNwJTRmUTCLEPNH	Console	8106	HAyURsCeDy	AfMYkcbZqofp	No
McAfee	e250		HTTP	webshield	webshieldchangeme		No
McAfee	IntruShield IPS Sensor	1.8	SSH	admin	admin123		No
McAfee	IntruShield IPS Sensor	1.9	SSH	admin	admin123		No
McAfee	IntruShield IPS Sensor	2.1	SSH	admin	admin123		No
McAfee	IntruShield IPS Sensor	3.1	SSH	admin	admin123		No
McAfee	IntruShield Manager	1.8	HTTP	admin	admin123		No
McAfee	IntruShield Manager	1.9	HTTP	admin	admin123		No
McAfee	IntruShield Manager	2.1	HTTP	admin	admin123		No
McAfee	IntruShield Manager	3.1	HTTP	admin	admin123		No
mDybkswDzvVBDroXHU	AGRUJxPDRMrIAR	hhBQDULjfFOpESdDH		41014	C5ly4e	oafkaVLEAhrMK	No
Megastar	PC BIOS		Console	n/a	star	Admin	No
Memotec	CX Line	Any	Multi	memotec	supervisor	Console	No
Mentec	Micro/RSX		Multi	MICRO	RSX	Admin	No
metro	phone		Serial	client	client	voicemail	No
mGuSMHmIByGbYR	HAmNgdrPDXwAscP	IsFCazIhIFvzJY		898076	SWCzZe	QqtRVvESCRA	No
Micron	PC BIOS		Console	n/a	xyzall	Admin	No
Micron	PC BIOS		Console	n/a	sldkj754	Admin	No
Micronet	Access Point	SP912	Telnet	root	default	Admin	No
Micronet	SP3356		HTTP	admin	epicrouter		No
Micronet	SP3357		HTTP	admin	epicrouter	admin	No
Micronics	PC BIOS		Console	n/a	dn_04rjc	Admin	No
Microplex	Print Server		Telnet	root	root	Admin	No
microRouter	900i		Console/Multi	n/a	letmein	Admin	No
Microsoft	Great Plains	All	Multi	LessonUser1	(none)		No
Microsoft	Great Plains	All	Multi	LessonUser2	(none)		No
Microsoft	SQL Server	7	Multi	sa	(blank)	Admin	No
Microsoft	SQL Server		Multi		sa	(none)	No
Microsoft	Windows NT		Multi	Administrator	(none)	Admin	No
Microsoft	Windows NT		Multi	Guest	(none)	User	No
Microsoft	Windows NT		Multi	User	User	User	No
Microsoft	Windows NT		Multi	Guest	Guest	User	No

http://www.defaultpassword.com/

- A former employee of Rochdale Connection Trust has been prosecuted by the ICO at Preston Court. Robert Morrisey sent spreadsheets containing the information of vulnerable clients to his personal email address without any business need to do so, which was without the consent of the data controller.
- 11 emails were sent from his work email account on 22 February 2017, which contained the sensitive personal data of 183 people, three of whom were children. The personal data included full names, dates of birth, telephone numbers and medical information. Further investigation showed that he had sent a similar database to his personal account on 14 June 2016.
- Mr Morrisey pleaded guilty to 3 offences under section 55 of the Data Protection Act and was sentenced to a 2 year Conditional Discharge, ordered to pay costs of £1,845.25 and a £15 Victim Surcharge.

What about …

The introduction of foreign species to Hawaii has greatly affected the populations of the islands' native species. In many cases, the introduction of foreign species has wiped out the entire population of certain species, rendering them extinct. This is especially devastating because many of these species are endemic, meaning they are found only in one particular location and nowhere else in the world. The majority of species living in Hawaii are the result of thousands of years of island biodiversity. A few birds of one species migrate from some distant island due to some rare occurence of nature and eventually evolve into several new species, each perfectly adapted to the environment in which it has come to live. Unfortunately, each of these endemic species is especially susceptible to the effects of invasive species, which means the impact on Hawaii's animal life has been tremendous.

When goats were first introduced to Hawaii by Captain Cook in the late 1700s, they immediately began eating all the local plant life. Most of these plants were unused to being preyed upon until the introduction of foreign species into their habitat, and so suffered massive population loss from grazing animals. The goat population, on the other hand, grew rapidly, as it had no natural predators to keep it in check. The introduction of European pigs to Hawaii had similar effects on the native species, although, due to a scarcity of protein in natural Hawaiian forests, the European pig population did not grow as rapidly as the goats until the 1900s with the introduction of earthworms and foreign plants which made up large portions of the pigs' diets (Stone and Loope 1987).

European pigs and goats are both primarily grazing animals, meaning their diet consists mostly of plant life found near the ground. Rats, mice, and mongooses, however, are easily able to reach low hanging branches of trees containing fruit, seeds, and sometimes even bird nests. Mongooses were first introduced to Maui in the 1880s to prey upon rats in sugarcane fields and quickly extended their range to include almost every hospitable nook in the island. They feed on most plants and animals smaller than them, including lizards, insects, crabs, rodents,

Humans are not only indirectly responsible for the reduction and
ction of native Hawaiian species through the introduction of invasive
ies, but are also sometimes the direct cause. The Townsend's
water, one of the handful of surviving Hawaiian seabirds, are greatly
ed by the light pollution from both urban and resort locations in
. These birds, whose breeding colonies were undiscovered until
1980s, are blinded and disoriented while flying from inland
areas to the coast, causing them to crash, often in the developed
ducing the lights, where they are usually killed by cars or
pets (Scott et al. 1988). Younger shearwaters are the most
to being disoriented by light pollution; therefore, the majority
d this way are too young to have reproduced, leading to a
population of mostly older birds with few young to take their
sure the continued survival of their own species. This
observed in 1961, has elevated as more and more land was
response to Hawaii's booming tourism in the 1970s.
methods have been put into action hoping to reduce
e of light-blocking shields to reduce light pollution.

Kepler, C. van Riper III, and S.I. Fefer. 1988.
Hawaii's vanishing avifauna. BioScience 38(4):238-253.
L.L. Loope. 1987. Reducing negative effects of
s on native biotas in Hawaii: What is being done, what
the role of national parks. Environmental Conservation

Loope, and C.P Stone. 1987. Introduced species in
ects and opportunities for ecological research.
d Evolution 2(7):224-227.

Printed

- Secure ALL media
- Shred paper containing secure information
- Institute a clear desk policy

Lenovo

- Encrypt laptops
- Encrypt removable media – but prevent copying to removable media if possible
- Have a process for managing lost /stolen devices.

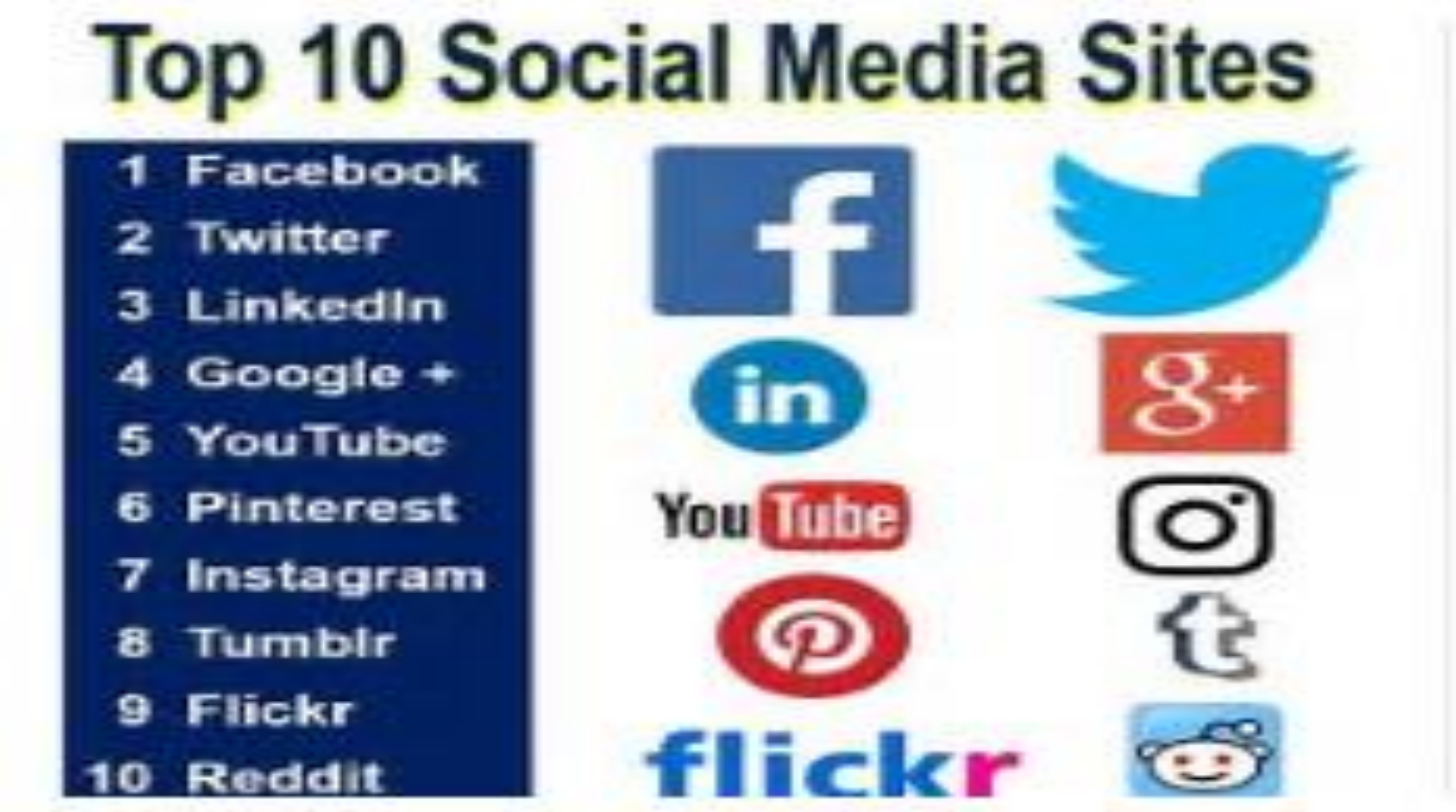
or

What about?

People

- People are friendly and want to help, but not every caller is who that say they are
- When you talk to colleges others may be listening
- Don’t copy information to removable media
- Don’t gossip on social media –
- Facebook, Instagram AND LinkedIn
- Take care at smoke breaks

Finally ….



Top 10 Social Media Sites

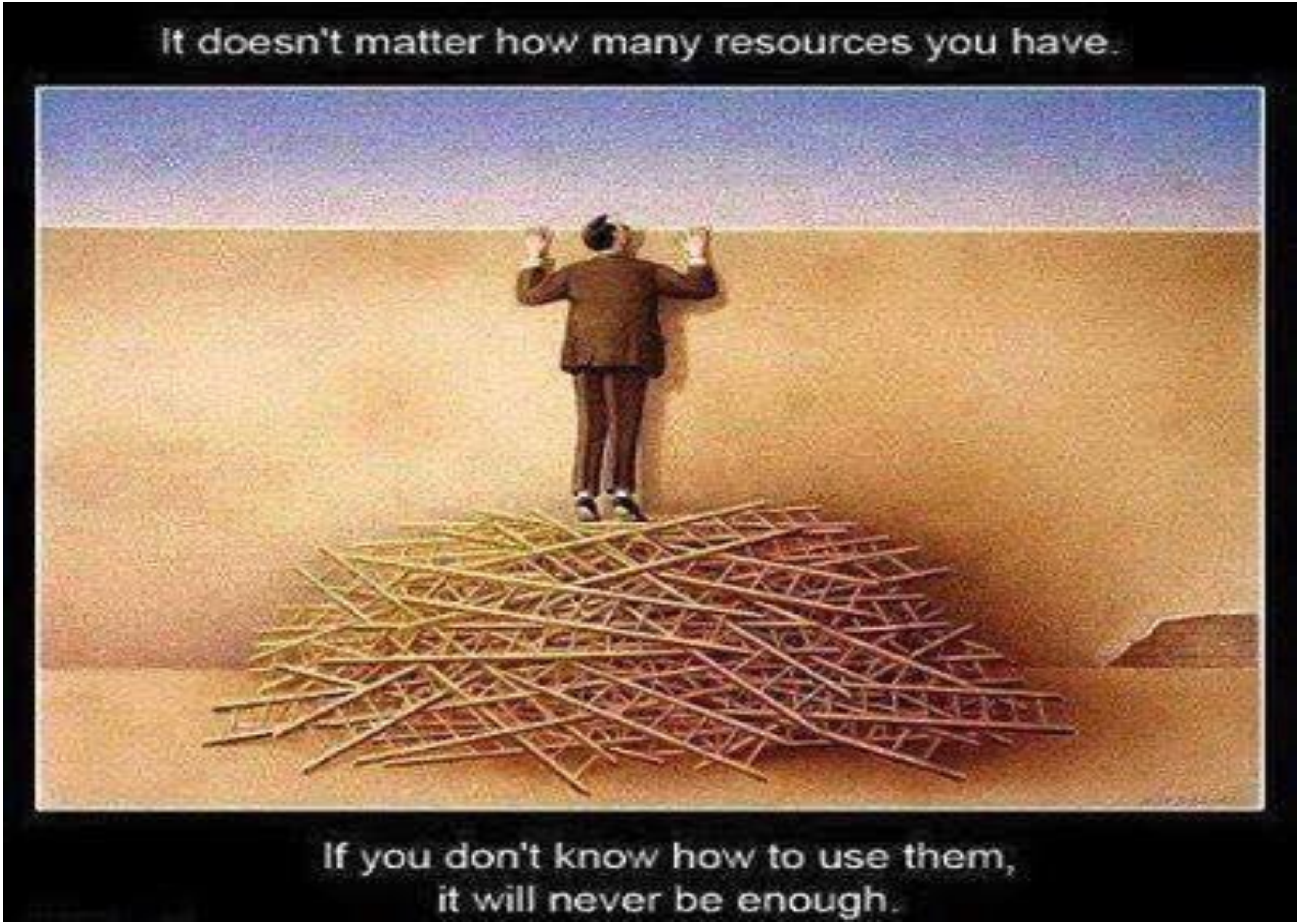
1 Facebook
2 Twitter
3 LinkedIn
4 Google +
5 YouTube
6 Pinterest
7 Instagram
8 Tumblr
9 Flickr
10 Reddit

website

- All data capture must be secured with HTTPS
- Validate all input

Operational

- Have a J/M/L process
- Tell reception of leavers
  Email - "say good bye to......."
- Retrieve Id cards
- Change Digilock numbers
- Return of keys and swipe cards
- Remember staff leaving under a cloud or to a competitor
- Change Admin passwords - regularly and on leaving


It doesn't matter how many resources you have.
If you don't know how to use them,
it will never be enough.

Useful resources

Cyber Essentials

https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

Information Commissioner’s Office

https://ico.org.uk/for-organisations/data-protection-reform/

Plus, of course …….

CSF

Charities Security Forum

Charities Security Forum

www.charitiessecurityforum.org.uk

brian.shorten@charitiessecurityforum.org.uk

CSF

Charities Security Forum

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

- Members participate in discussions and presentations on information security issues of relevance and importance to the not-for-profit sector

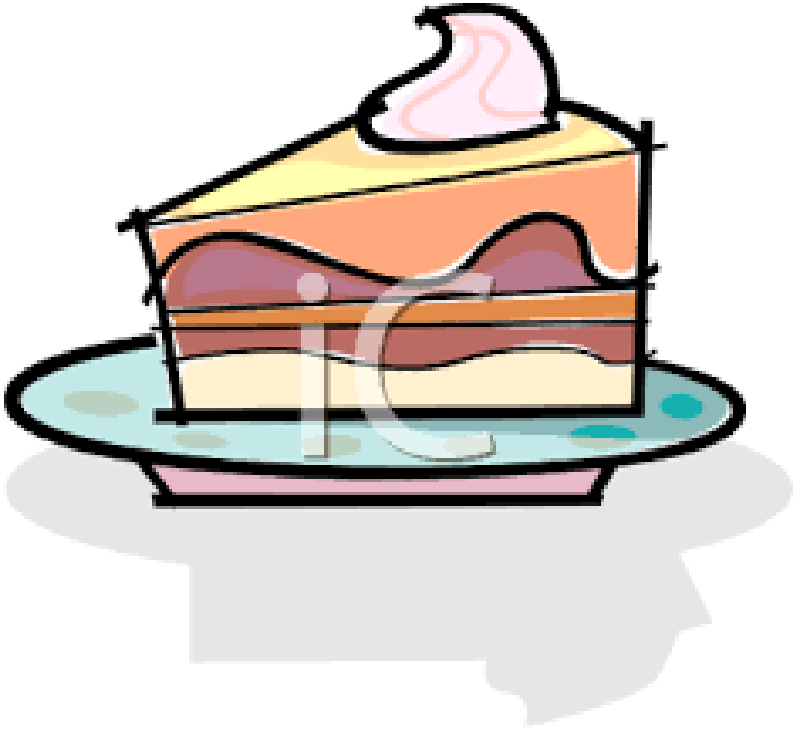
Thank you for your time

any questions?

CSF

Charities Security Forum

Cake



gdst Girls' Day School Trust

The GDPR journey............

Jon Vogel

Information Security and Governance

22nd November 2017

GDPR Project

- GDPR Will replace DPA 1998 on 25 May 2018

- Describes the principles under which data must be processed, and introduces new rights for Data Subjects

- Organisations need to show *how* they comply with these principles, ensuring appropriate technical and organisational measures

- Introduces mandatory reporting of data breaches (72hrs)

- Far higher fines (increasing from £500k to €20m), and compensation to data subjects for financial loss or distress

Project Phases

1. **Undertaking a data inventory**. Information Security Champions are currently identifying the personal data held within schools and how this is being processed

   (target date for completion – 15th November 2017)

2. **Identifying the legal basis for processing data.** Once all of data processing activities have been identified it is necessary to identify the legal basis for processing this data.

   (target date for completion - 15th December 2017)

3. **Demonstrating compliance with data subjects rights.** This is the most complex phase of the work stream and the level of complexity will be determined by phases 1 and 2.

   (schedule of work will be completed by 9th January 2018)

Processing Special Categories of Data

Processing of personal data revealing

- racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership
- genetic data, biometric data for the purpose of uniquely identifying a natural person
- data concerning health or data concerning a natural person’s sex life or sexual orientation

shall be prohibited.

Processing Special Category Data

1. Explicit Consent
2. Employment / Social Security / Social Protection Law
3. Vital Interests of Data Subject
4. Foundation / not-for-profit body with a political, philosophical, religious or trade union aim
5. Made Public by the Data Subject
6. Substantial Public Interest
7. Preventive or Occupational Medicine
8. Public Interest in the area of Public Health
9. Archiving Purposes / Public Interest, Scientific or Historical Research

SCHEDULE 1 Part 2 of the UK Data Protection bill

SUBSTANTIAL PUBLIC INTEREST CONDITIONS

Parliamentary, statutory and government purposes
6(1) This condition is met if the processing—
(a)is necessary for a purpose listed in sub-paragraph 2, and
(b)is necessary for reasons of substantial public interest.

(2) Those purposes are—
(d)the exercise of a function of the Crown, a Minister of the Crown or a government department.

INFOSEC LESSONS

ANDY FENTON

TECHROSE CONSULTANCY LIMITED

07930 802804

INTRODUCTION

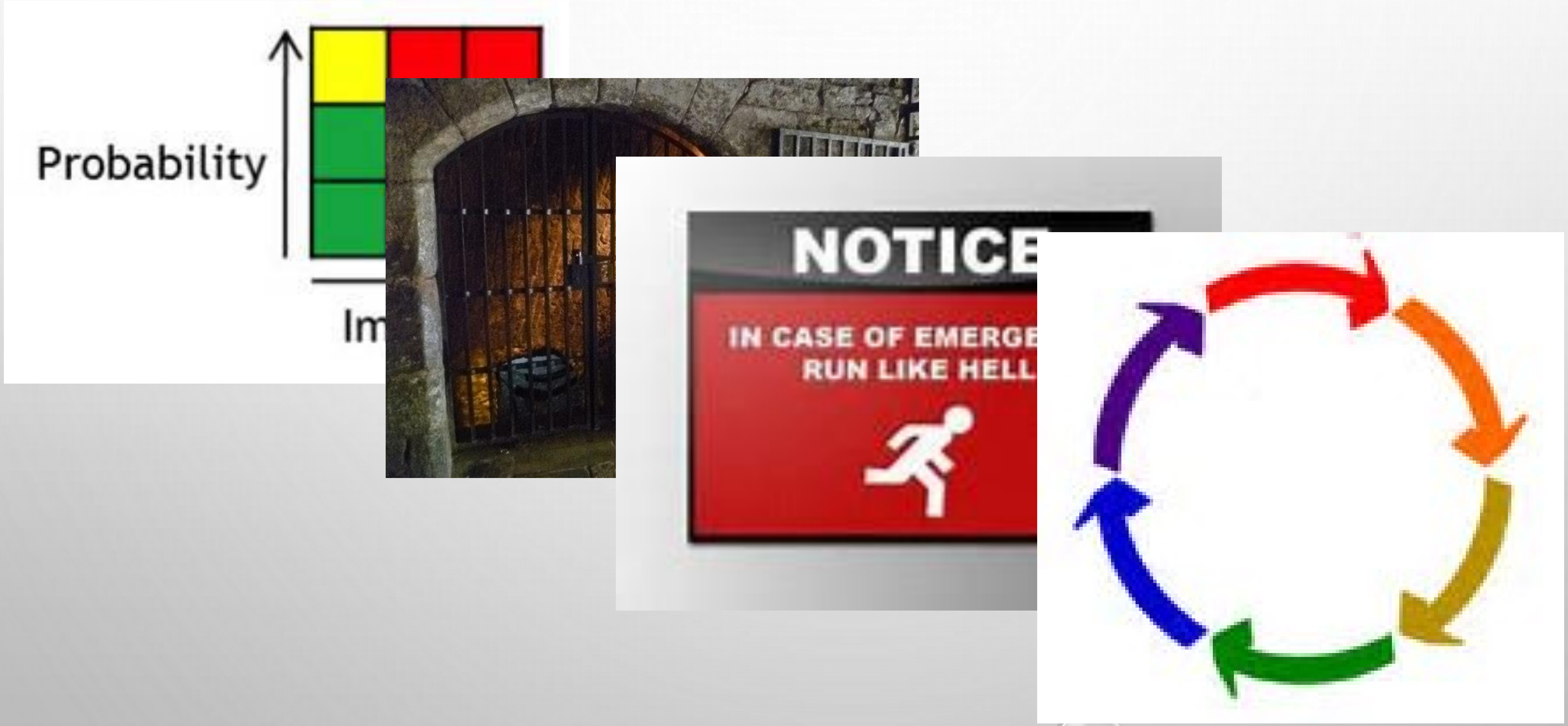
BACKGROUND

- PREVIOUSLY WORKED IN AUTOMOTIVE AND PHARMACEUTICAL SECTORS
- HELP THE AGED HEAD OF IT IN MID 2000S
- THEN CONSULTANT TO LARGE UK CHARITIES – NSPCC, AGE UK, RNIB
- CHIEF INFORMATION OFFICER (CIO) FOR THE BRITISH HEART FOUNDATION (BHF) 2011 TO JULY 2017
- NOW PROVIDING CONSULTANCY AND INTERIM SENIOR IT AND DIGITAL MANAGEMENT SERVICES IN THE NOT FOR PROFIT SECTOR
- CURRENTLY INTERIM CTO FOR INTO FILM, (THREE DAYS PER WEEK)
- WILL DRAW ON MY BHF EXPERIENCE, BUT AM ALSO SENSITIVE TO THE NEED TO MAINTAIN CONFIDENTIALITY

INFOSEC STRATEGY

HEALTH & SAFETY
IN GAMES OF HIDE & SEEK THE PLAYER BEING SOUGHT MUST WEAR A HIGH VISIBILITY JACKET

INFOSEC STRATEGY



INFOSEC STRATEGY

- ADOPT A RISK-BASED APPROACH – AND TARGET THE BIGGEST RISKS FIRST
- CONTINUE PERIPHERY PROTECTION, BUT ADD KEY ASSET PROTECTION - PROTECT THE ‘CROWN JEWELS’ ON THE ASSUMPTION ‘THEY’ GET INTO YOUR NETWORK
- ADD INTRUSION DETECTION TO EXISTING INTRUSION PREVENTION. ADD INTERNAL PENETRATION TESTING TO EXTERNAL PEN TESTING
- ASSUME A BREACH WILL HAPPEN – AND ACTIVELY PLAN FOR IT
- SENIOR ENGAGEMENT IS CRITICAL TO GET TRACTION AND AUTHORITY – THIS IS NOT JUST YOURS
- PUT AN INFORMATION SECURITY PROGRAMME OF WORK IN PLACE – BUT KEEP LOOKING FOR MORE SECURITY ISSUES AND EXPECT THE PLAN TO CONTINUOUSLY CHANGE
- NEVER ASSUME YOU HAVE FINISHED

THE JOURNEY

GOVERNANCE

Staff Training

RESPONSIBILITY

ing

LESSONS FROM THE JOURNEY

- THE PRESSURE TO ACT CONTINUES TO INCREASE
- CONSIDER USING EXTERNAL RESOURCE TO GET DIFFERENT VIEWS OF YOUR INFORMATION SECURITY
- YOU MAY NEED AN INFORMATION SECURITY ADMINISTRATOR TO MAINTAIN COMPLIANCE AS YOU PUT MORE SECURITY MEASURES IN PLACE
- GOVERNANCE
  - ESTABLISH AND MAINTAIN FORMAL GOVERNANCE WITH YOUR EXEC AND TRUSTEE BOARDS
  - CONSIDER A FORMAL REPORTING PROCESS (QUARTERLY?) TO ENSURE YOU SECURITY STATUS IS CONTINUOUSLY UPDATED, UNDERSTOOD AND AGREED BY SENIOR COLLEAGUES
- CREATE A FORMAL PROGRAMME OF WORK FOR IT SECURITY
- TRAINING AND EDUCATION OF STAFF IS CRITICAL
  - TAKE OPPORTUNITIES (LIKE WANNACRY) TO ENGAGE WITH SENIOR COLLEAGUES AND EDUCATE
  - ADD INFOSEC TO INDUCTION
  - CREATE AN ANNUAL SECURITY COMMUNICATIONS PLAN TO ENGAGE ALL STAFF – AND USE MANY CHANNELS
- JOIN FORCES WITH OTHER DEPARTMENTS WHERE YOU CAN

FINAL THOUGHTS

- WHERE ARE YOU ON THE JOURNEY?
- ORGANISATION SIZE, MATURITY
- SENIOR MANAGEMENT AND STAFF – FIND WAYS TO CONTINUOUSLY ENGAGE
- CONTINUOUSLY ASSESS YOUR RISKS TO TAILOR YOUR STRATEGY
- PLAN FOR THE BREACH
- NEVER-ENDING JOURNEY

ANDY FENTON, TECHROSE CONSULTANCY, 07930 802804

Discussion and feedback

Review and close