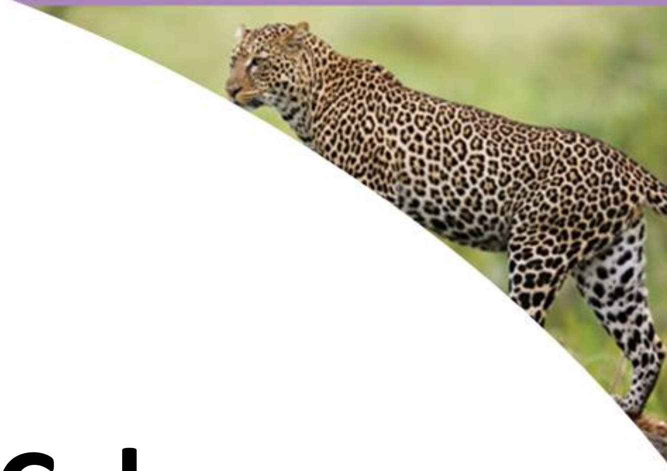


Cyber Security and Cake

22 March 2018

@AdaptaforNFP

adapta

processes, people and technology

INSTITUTE OF CONSULTING
RECOGNISED PRACTICE

Programme

14.00 **Arrival and welcome**
Paul Sypko, Adapta Consulting

14.15 **The pre-requisites to safeguarding data**
Philip French, Adapta Consulting

14.30 **Case studies**
Martyn Croft, Former CIO of Salvation Army and Co-founder of Charites Security Forum

COFFEE

Nicholas McGhee, Information Systems Director, GMB Union

15.45 **Discussion and feedback**
All

16.30- **Review and close**
17.00 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

The pre-requisites for safeguarding data

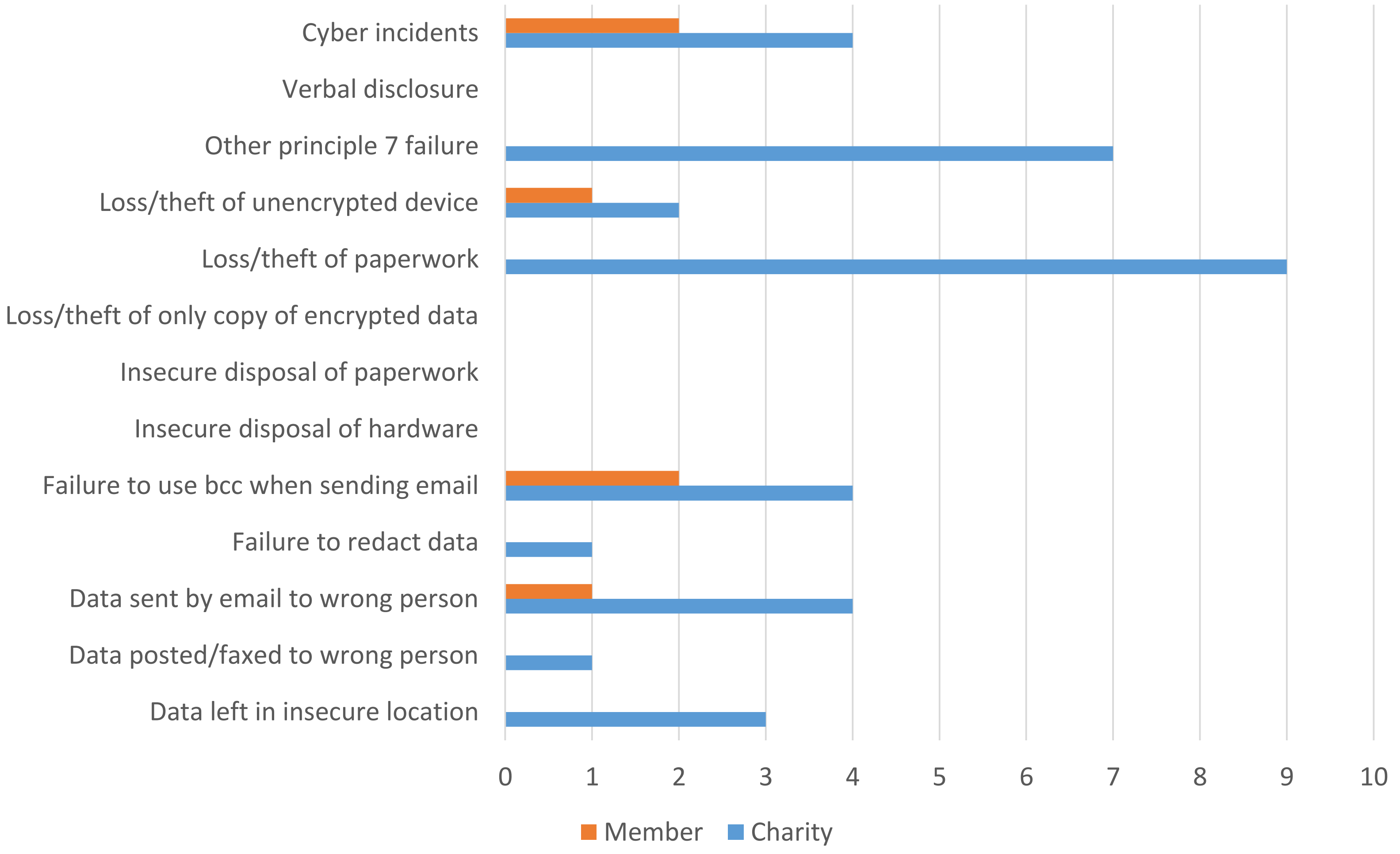
Philip French

Adapta Consulting

Ten simple principles

1. Know what information you hold, and why it matters. (Use the GDPR audit.)
2. Have clear policies, train staff in them, and check that they are being used.
3. Control access. Set proper passwords (and don’t leave them in plain sight!).
4. Password-protect, and hence encrypt, any sensitive documents.
5. Encrypt everything that moves: disks, tapes, laptops, USB memory sticks …
6. Keep software (and firmware) up to date: on PCs, servers and network devices. Use recent versions and automatic updates for Windows and Office.
7. Have effective anti-virus and anti-intrusion protection at the desktop, on the email server and at the network edge (firewalls and similar devices).
8. Test your defences, both technical and human (e.g. response to phone calls).
9. Don’t forget that paper also matters.
10. Above all, never be complacent: it can happen to you.

Don’t forget that paper also matters
Data loss incidents reported to ICO, Oct-Dec 2017



adapta

Never be complacent
Look who else has been hacked

Last month, websites around the world were successfully targeted to ‘mine’ the cryptocurrency Monero, for the benefit of the hackers. (These websites could equally well have been set to carry out far worse work, unbeknown to their owners.)

Over 4,000 websites were affected, including the US court portal and the UK privacy watchdog, the Information Commissioner’s Office (ICO).

This was done by compromising the Browsealoud plug-in, a useful piece of British software that reads out text for blind or partially-sighted users. The ICO’s website, and many others, loaded this plug-in on demand from Browsealoud’s website, without first verifying its provenance or integrity.

Never be complacent
Look how bad it can get

Year	Organisation	Description	Users affected
2011	Sony Playstation Network	Games consoles	77M
2012	Anthem	US health insurer (#2)	78M
2013-2015	Yahoo	Internet services (inc. BT email)	500M to 3B
2014	eBay	Online auctions	145M
2015	V-Tech	Toy maker	11M (6M children)
2016	Uber	Taxi service	57M
2017	Equifax	Credit rating	143M

Cyber Security and Cake

Martyn Croft

former CIO at The Salvation Army UK
co-founder of the Charities Security Forum
partner at martynandvalerie.com

Getting the Board onboard

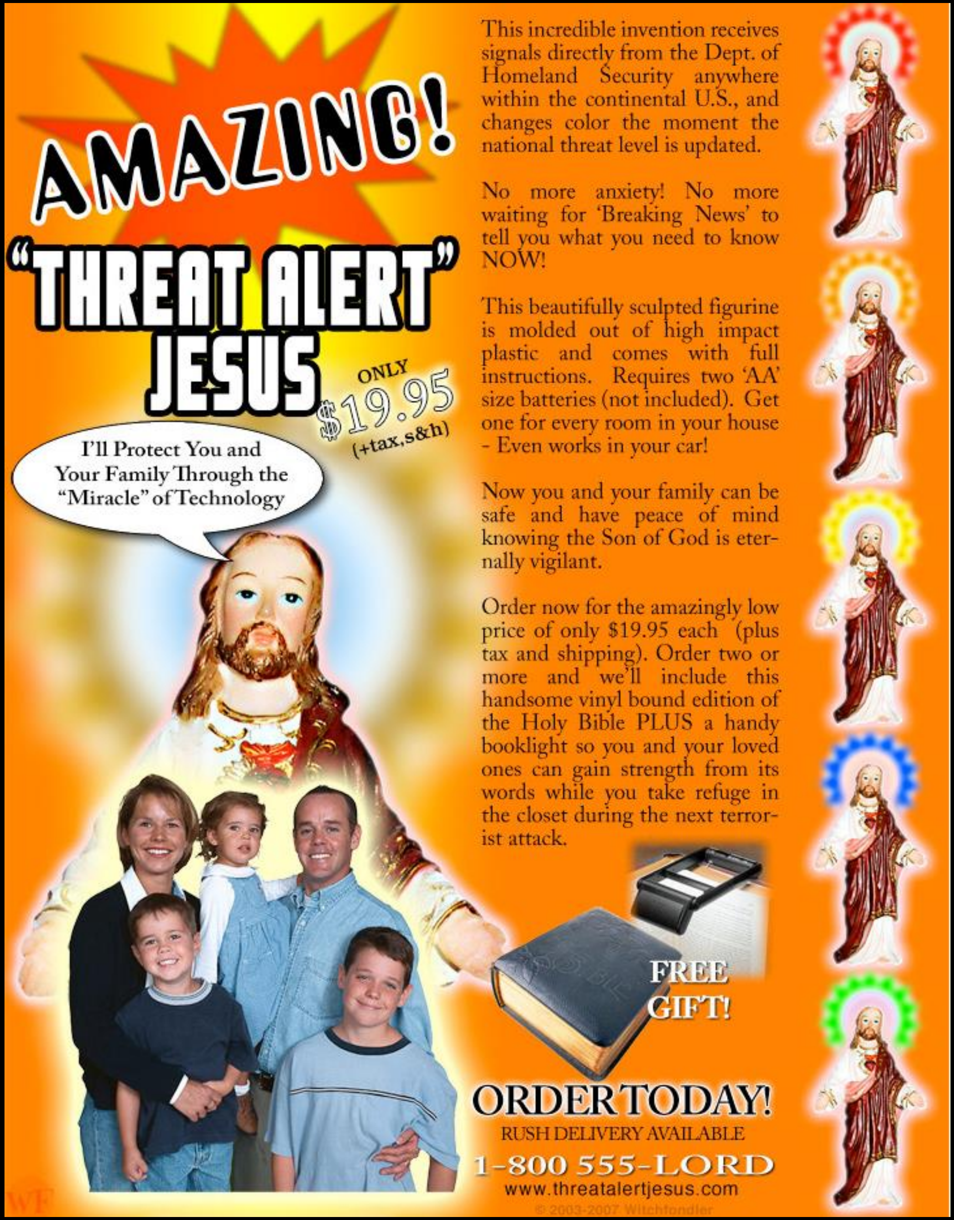
“So Martyn, do you think cyber-security
is a risk for charities?”

– chair of risk management committee

identifying the threats…

“We consider it likely that cybercriminals pose the most serious threat to the charity sector, but we are unaware of any large-scale statistical evidence to further support this.

This judgement is therefore presented with only medium confidence. Increased levels of reporting would enhance our evidence base.” - NCSC



AMAZING!

"THREAT ALERT" JESUS

ONLY $19.95 (+tax,s&h)

I'll Protect You and Your Family Through the "Miracle" of Technology

This incredible invention receives signals directly from the Dept. of Homeland Security anywhere within the continental U.S., and changes color the moment the national threat level is updated.

No more anxiety! No more waiting for 'Breaking News' to tell you what you need to know NOW!

This beautifully sculpted figurine is molded out of high impact plastic and comes with full instructions. Requires two 'AA' size batteries (not included). Get one for every room in your house - Even works in your car!

Now you and your family can be safe and have peace of mind knowing the Son of God is eternally vigilant.

Order now for the amazingly low price of only $19.95 each (plus tax and shipping). Order two or more and we'll include this handsome vinyl bound edition of the Holy Bible PLUS a handy booklight so you and your loved ones can gain strength from its words while you take refuge in the closet during the next terrorist attack.

FREE GIFT!

ORDER TODAY!

RUSH DELIVERY AVAILABLE

1-800 555-LORD

www.threatalertjesus.com

A 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.

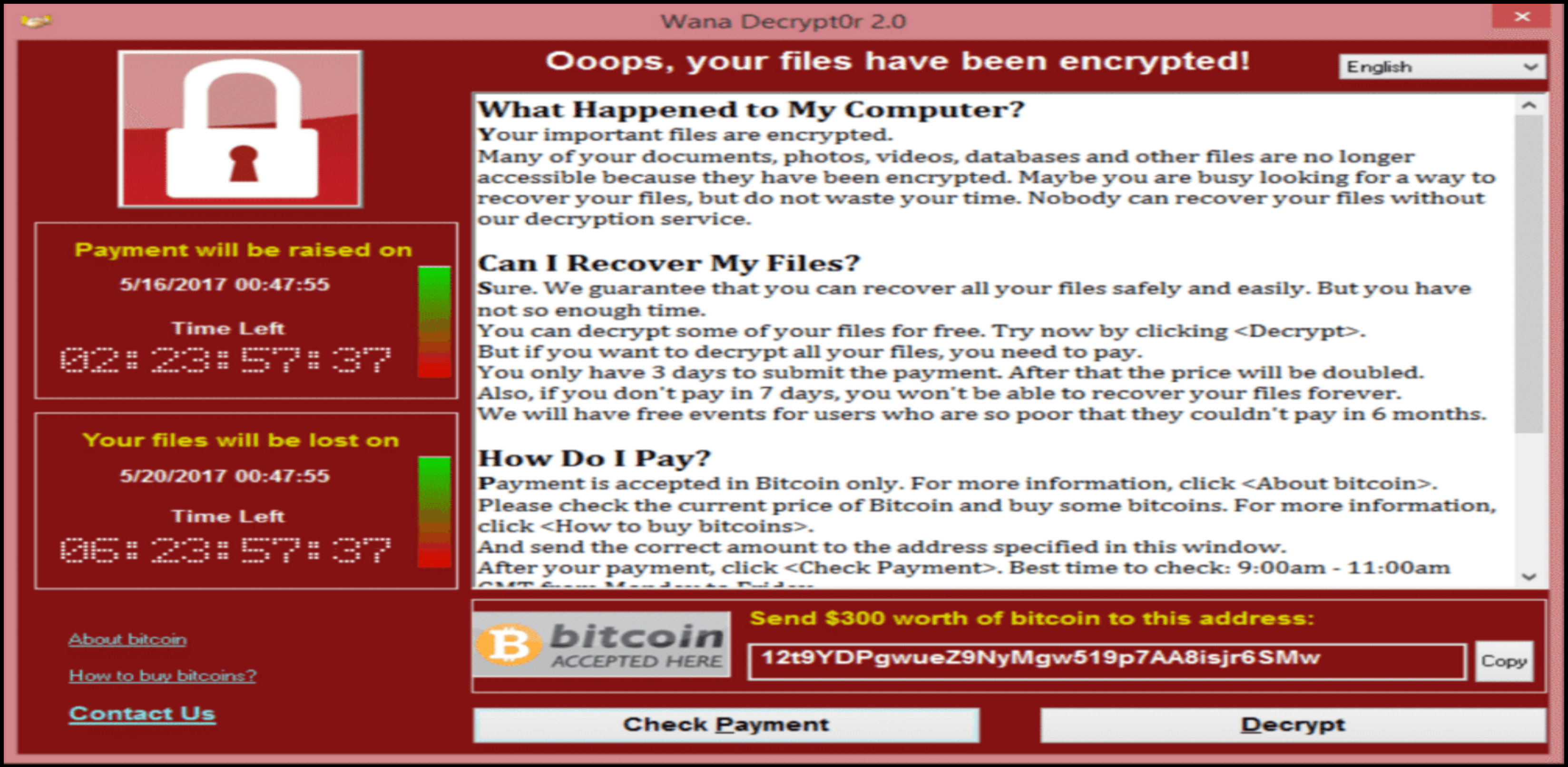
10 Steps: A Board Level Responsibility

10 Steps to Cyber Security

1. Risk Management Regime
2. Secure Configuration
3. Network Security
4. Managing User Privileges
5. User Education and Awareness
6. Incident Management
7. Malware Prevention
8. Monitoring
9. Removable Media Controls
10. Home and Mobile Working

“SMB v1 is unpatched on two servers”

“Yes Martyn, but how will it affect us?”



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

“I was just doing my job”

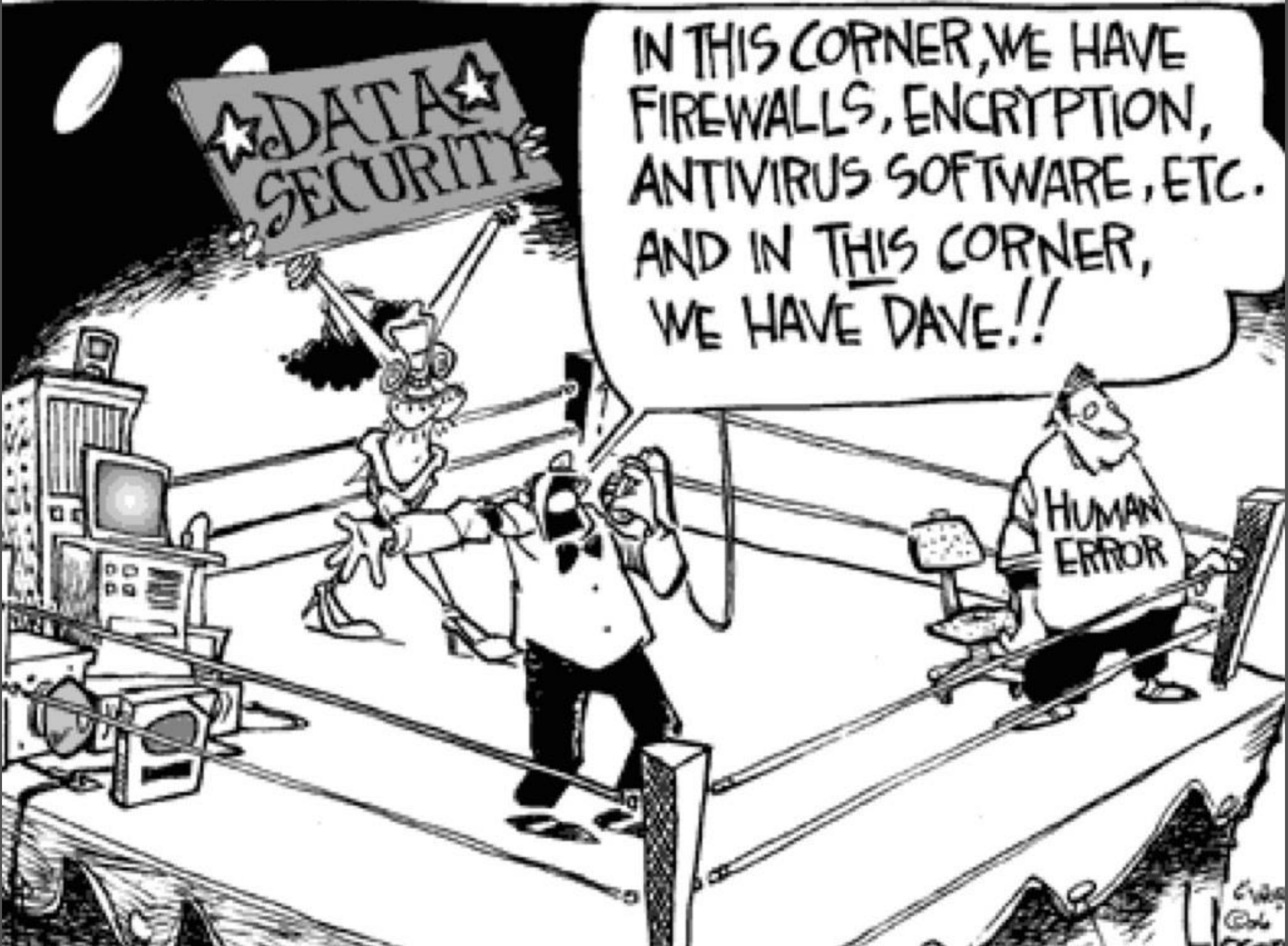
–Marcus Hutchins

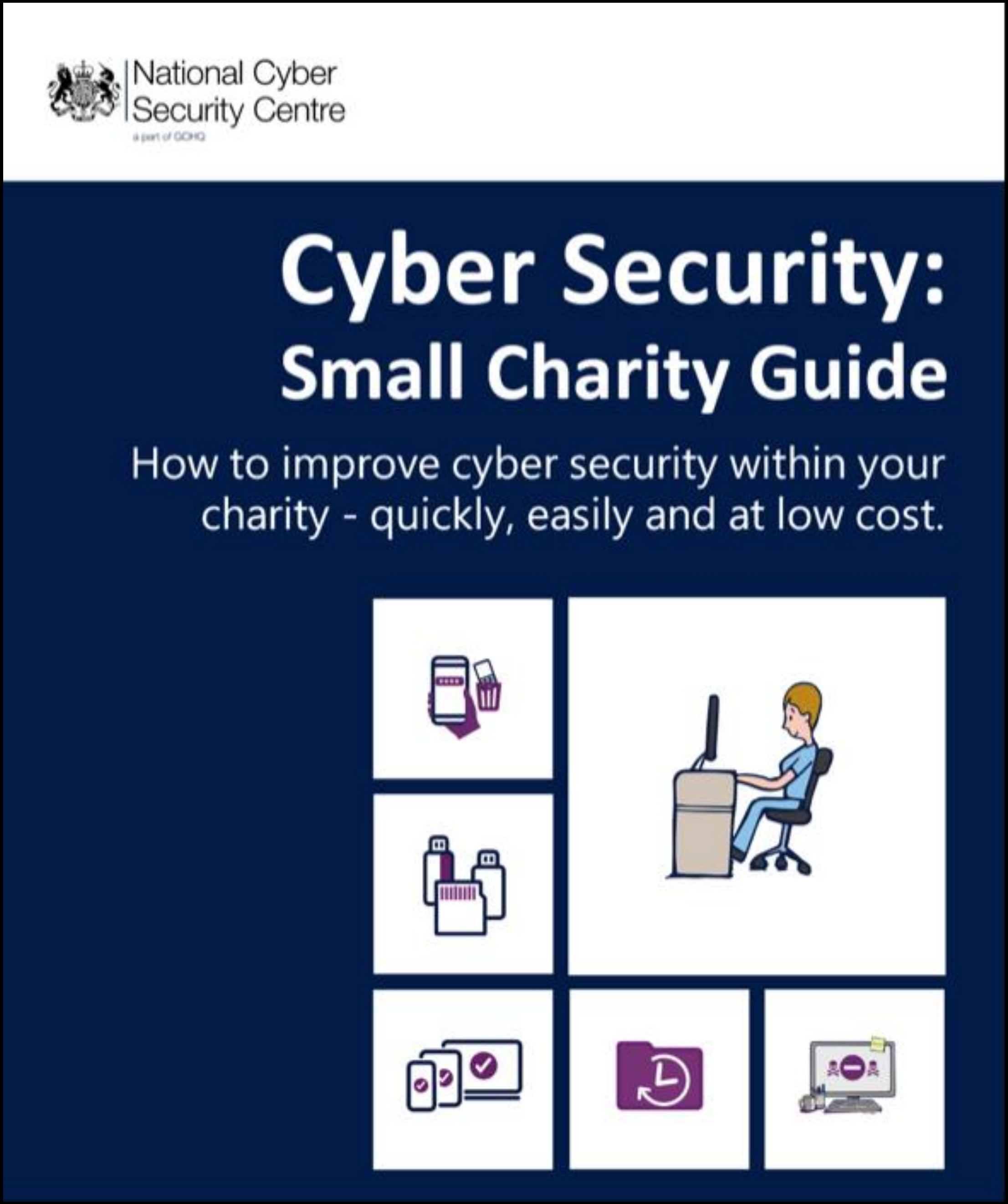
Cyber Essentials

- Secure your Internet connection
- Secure your devices and software
- Control access to your data and services
- Protect from viruses and other malware
- Keep your devices and software up to date

Challenges for Charities

- predisposed to be helpful
- nothing worth stealing
- attracted to ‘free’
- email is the only information system
- inconvenient rules
- sharing culture
- no training required, just helping out
- convoluted finances


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



National Cyber Security Centre
a part of GCHQ

Cyber Security: Small Charity Guide

How to improve cyber security within your charity - quickly, easily and at low cost.

Charities Security Forum

“The premier group for Information Security Professionals working in the charity sector. The group has over five hundred members representing many major and household name charities.

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

Brian Shorten

Martyn Croft

www.charitiessecurityforum.org.uk

Useful Resources

- Charities Commission: https://www.gov.uk/government/news/ransomware-threat-keep-your-charity-safe
- Get Safe Online: https://www.getsafeonline.org/articles/charitycommission/
- NCSC: https://www.ncsc.gov.uk
- Cyber Essentials: https://www.cyberessentials.ncsc.gov.uk/advice/
- ActionFraud: http://www.actionfraud.police.uk
- Charities Against Fraud: http://charitiesagainstfraud.org.uk
- IT Induction and Information Security Awareness: https://www.itgovernance.co.uk/shop/product/it-induction-and-information-security-awareness
- Open Web Application Security Project (OWASP): https://www.owasp.org/index.php/SQL_Injection
- The IASME Consortium: https://www.iasme.co.uk
- Charities Security Forum: http://charitiessecurityforum.org.uk
- SC Media: https://www.scmagazineuk.com/is-cybersecurity-a-risk-for-fundraisers-the-sc-guide-for-charities/article/675655/

Contact us

mail: info@martynandvalerie.com

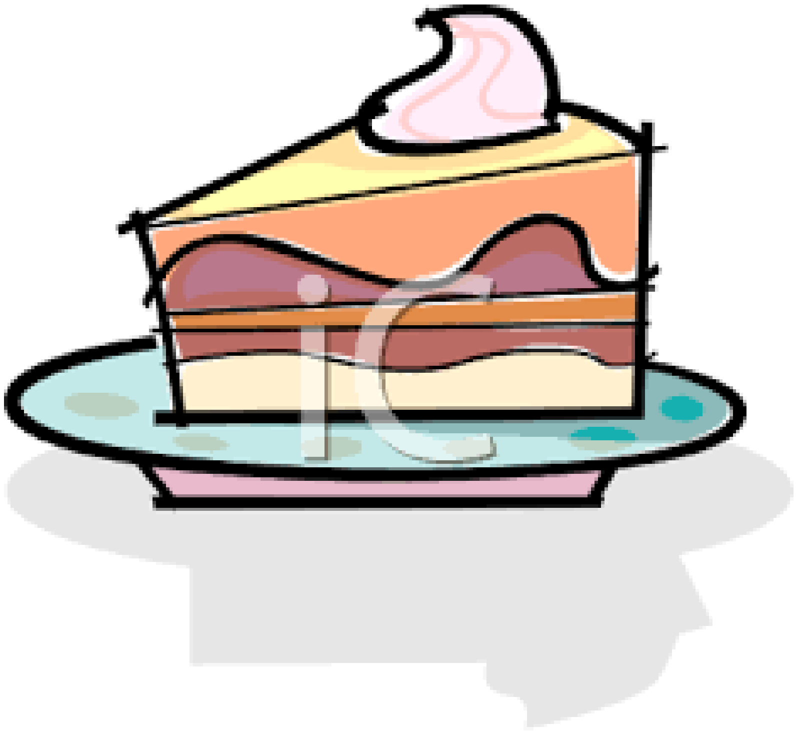
twitter: @martyn_valerie

web: www.martynandvalerie.com

CSF: www.charitiessecurityforum.org.uk

Copyright and Credits

Cake



CYBER SECURITY FORUM

Nicholas McGhee – IS Director – GMB (Trade Union) – Our experiences

INTRODUCTION

- GMB have 615,000 members spread geographically across the UK
- Britain’s general union
- Support members in a variety of sectors from teaching to NHS to banking to IT
- Organisation is split into 9 regions who operate largely autonomously
- Each region has its own management structure with staff who support members underneath
- Each of the regions have branches who execute the work of the union ‘on the ground’
- These individuals are effectively volunteers

THREATS WE HAVE FACED

- Over the course of the last 12 months
  - Social engineering attacks
  - Viruses
  - Ransomware
  - Malware
  - Phishing
  - Spam
  - Spoofing
  - Spyware/adware

THE IMPACT

- Staff who lose confidence in the security of data
- Productivity hours lost
- In some circumstances money lost
- A distrust of technology
- A lack of willingness to engage in other IT Projects
- A desire to revert back to older recording mechanisms
- A slower pace of technological change

HOW WE REACTED

- Concern, possibly an element of panic
- Too many cooks
- Risk based approach including risk matrix
- We needed a plan including key steps (or series of plans)
- We needed to understand our priorities
- We needed to prepare the company to respond to a potential breach
- We needed to investigate and implement a strong recovery approach

COMMUNICATING THE RISK

- We needed everyone to know the risk
- We wanted to paint a picture of how this would impact on the services we provide
- This allowed people to truly grasp the impact and take personal responsibility
- Tour the organisation/Email campaign/training
- Talk to staff face to face
- Discuss the importance of good housekeeping (the basics)
- Password's, locking computers, etc

COMMUNICATING THE RISK

- Understanding ALL the Risks
  - Environmental
  - Digital
  - Staff
  - Volunteers
  - Members
- Possible Investigations
- Fines
- Enforcement Orders
- Brand Damage (massive issue for a trade union)
- Legal proceedings against the organisation

PROJECT

- Identifying the Risks
  - Understanding the value of what we hold
  - Understanding our key vulnerabilities
  - Fix the big stuff first we can't solve everything overnight
- Protect
  - Protect against identified risks and there impacts
- Detect
  - Fid ways to identify risks and spot them before, during or at worst after occurrence
- Respond
  - Ensure everyone knows the response steps to minimise the impact
- Recover
  - Get in place steps to recover should the worst happen

STEPS

- Upgrading our protection
- Learning to ‘Break the kill chain’ (Detect, Deny, Disrupt, Degrade, Deceive Contain)
- Developing ways to find threats (Intrusion Detection, AntiVirus, SIEM (soon to come))
- TRAIN STAFF (Phishing training, Data Protection training)
  - Face to Face
  - Online
  - Over Web
- Update the training and reflect on the changing nature of threats

PREPARING FOR THE INEVITABLE?

- A breach may not be inevitable but we work on the basis it will be
- We needed staff to understand their responsibilities if breach occurs, all staff
- Practicalities
  - Who to call?
  - Who does what?
  - What happens if ‘they’ are unavailable?
  - How do key suppliers get involved and what is their role?
- How to invoke insurance
  - (We beefed up our cyber insurance in line with identified risks)

BUSINESS CONTINUITY AND DR

- We recognised we needed a strategy
- We needed to work on the basis that we have had a significant breach
- Possible destruction or encryption of data on a mass scale
- We needed infrastructure that could get us back up and running ‘quickly’
- New WAN infrastructure
- Investment in DR solutions
- Determining how long we could afford to be without services
- Documenting and detailing a plan
- Even consider media training for SMT

HOW ARE WE ADAPTING

- We utilise industry expertise
  - We are not the experts, we need to admit that
  - We have limited resource and we need support in finding and deploying the right technology
- We do not have the scale of resource to battle the threats and the speed of change
- We utilise the cloud where we can and benefit from its security scale
- We focus on good housekeeping/the basics (permissions, justified access, a properly understood and applied policy set)
- Staff are trained and this is treated as a requirement
- We are taking steps to promote cyber security at a senior management level

HOW GDPR COMPLIANCE HELPS

- Biggest change to Data Protection Law in a generation
- The single largest compliance item on our menu at the moment
- Involves every aspect of the organisation
- Increased fines
- Enough to make people stand up and pay notice
- Requires new thinking around how personal and sensitive data is managed
- GDPR and Cyber Security are neatly intertwined
- Utilised to drive the cyber security agenda

UTILISING GDPR AS A VEHICLE FOR CHANGE

- List high risk activities for each department
- Understand the importance in terms of priority
- Where items are high risk implement Data Protection Impact Assessments
- Ensure that the DPIA’s are properly resourced and that they are prioritised over less risky items
- Research emerging technology to understand what steps can be taken to mitigate risk at an affordable level, utilise our supplier network expertise
- Improving cyber security position while reducing Data Protection risks

THE FUTURE

- The weaponisation of ‘IoT’
  - IoT is still in its relative infancy in terms of its application to most of our workplace’s however as adoption rises ransomware or hacking may significantly impact on our businesses ability to function
- How this impacts
  - For GMB the addition of Internet enabled devices in the last 5 years has almost tripled
  - Users now have iPhones, iPads, some offices utilise smart heating and lighting, there has been a burst of individuals who wish to move quickly with emerging technology
  - We need to react and support and protect
  - Expensive and time consuming

THE FUTURE

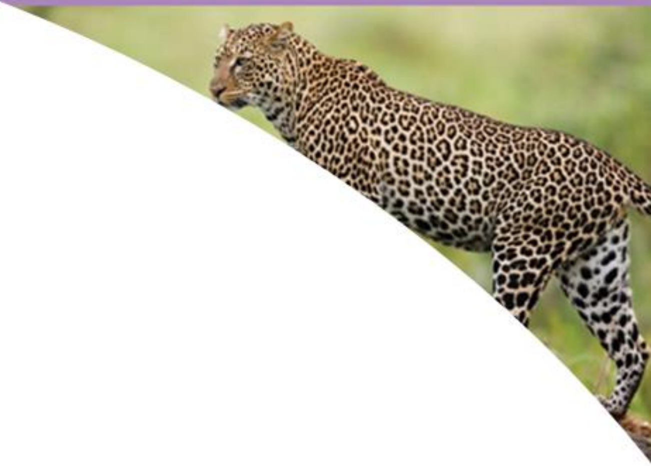
- Evolving threats
  - Utilisation of AI to improve the intelligence of attacks
  - More personalised phishing attempts
- Think carefully about what information we make public
- Ensure training keeps pace with evolving threats and stakeholders are abreast of developments
- Continue to build robust systems to deliver protection
- If protection fails ensure DR and business continuity is in place
- Constantly re-assessing

CONCLUSION

- Our Journey
  - Understand and quantify the risk
  - Communicate the risks and contextualise for our staff and senior team
  - Gap analysis
  - Project plan
  - Build in disaster recovery
  - Think to the future
  - Repeat!

Discussion and feedback

adapta



Review and close