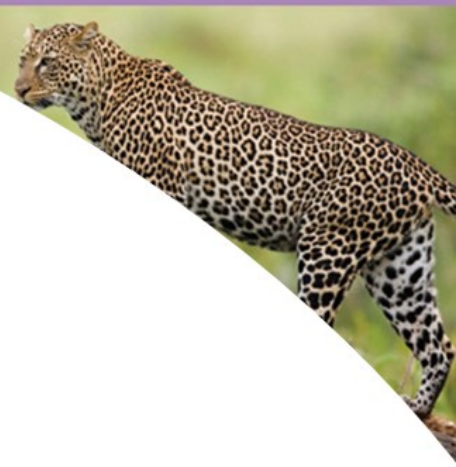


Information Security and (virtual) cake

30 March 2021

@AdaptaforNFP

adapta
processes, people and technology

INSTITUTE OF CONSULTING
RECOGNISED PRACTICE

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.

Our speakers

Paul Sypko

Partner, Adapta Consulting

IT strategy, risk management, information security, data protection, 20+ years sector experience working with hundreds of NFP organisations

Martyn Croft

Co-Founder, Charities Security Forum

Co-founded CSF in 2007, CIO of Salvation Army UK until retiring in 2017. Long-time interest and recognised expert in information security. Masters degree in information security and non-exec director for a small bank.

Naomi Da Silva

Head of Business Assurance, Central YMCA

Focused on risk, governance, data protection and management controls… making sure risks are properly addressed throughout the whole organisation

adapta

Programme

14:00	**Arrival and welcome** Welcome to the event, introductions and overview of the agenda for the afternoon Paul Sypko, Adapta
14:10	**Why we need effective and robust information security** A short overview of the current threats and the practical measures organisations are putting in place.
14:25	**Case Studies** Martyn Croft, Charities Security Forum Naomi Da Silva, Central YMCA *Grab a coffee (and a slice of cake if you have it)*
15:15	**Virtual roundtable discussion & feedback** All
15:50- 16:00	**Review & close** Paul Sypko, Adapta

adapta

Practicalities

- ‘Share screen’ should only be used for speaker presentations.
- Please **remain in mute mode** unless you wish to participate in the Breakout Room discussions.
- Your profile name should be your name and organisation – Hover over your name in Participants and select Rename.
- **If you have a question relating to any of the presentations or plenary discussions**, please feel free to submit these at any time using the Chat feature. Questions will be picked up once each presentation has ended.
- If we do not have time to cover questions/all questions, we hope to open a private discussion space following this event.
- We’ll be sharing the presenters’ slides after the event.
- **If you have a technical question** please use the Chat facility, and select **Paul Stirrat**, who will be able to help.

Breakout sessions will discuss:

What worries you most about information security in your organisation (or, if you prefer, what do you think are the biggest information security risks to NfP organisations generally)?

What steps could an organisation take to improve its information security posture, without necessarily incurring significant cost?

Each group will have a member of the Adapta team who will facilitate the discussion and capture headline notes. Everyone will be returned to the main room for wrapping up.

During breakout sessions: To contribute you should raise your hand using the 'Raise Hands' feature. Unmute once you have been prompted to by the Facilitator.

How to raise your hand: Click on the icon labelled 'Participants'.
Click on your name and select "Raise Hand".
You may have to click the screen to access the menu.

Information security… do we actually care?

If we don't… we certainly should!

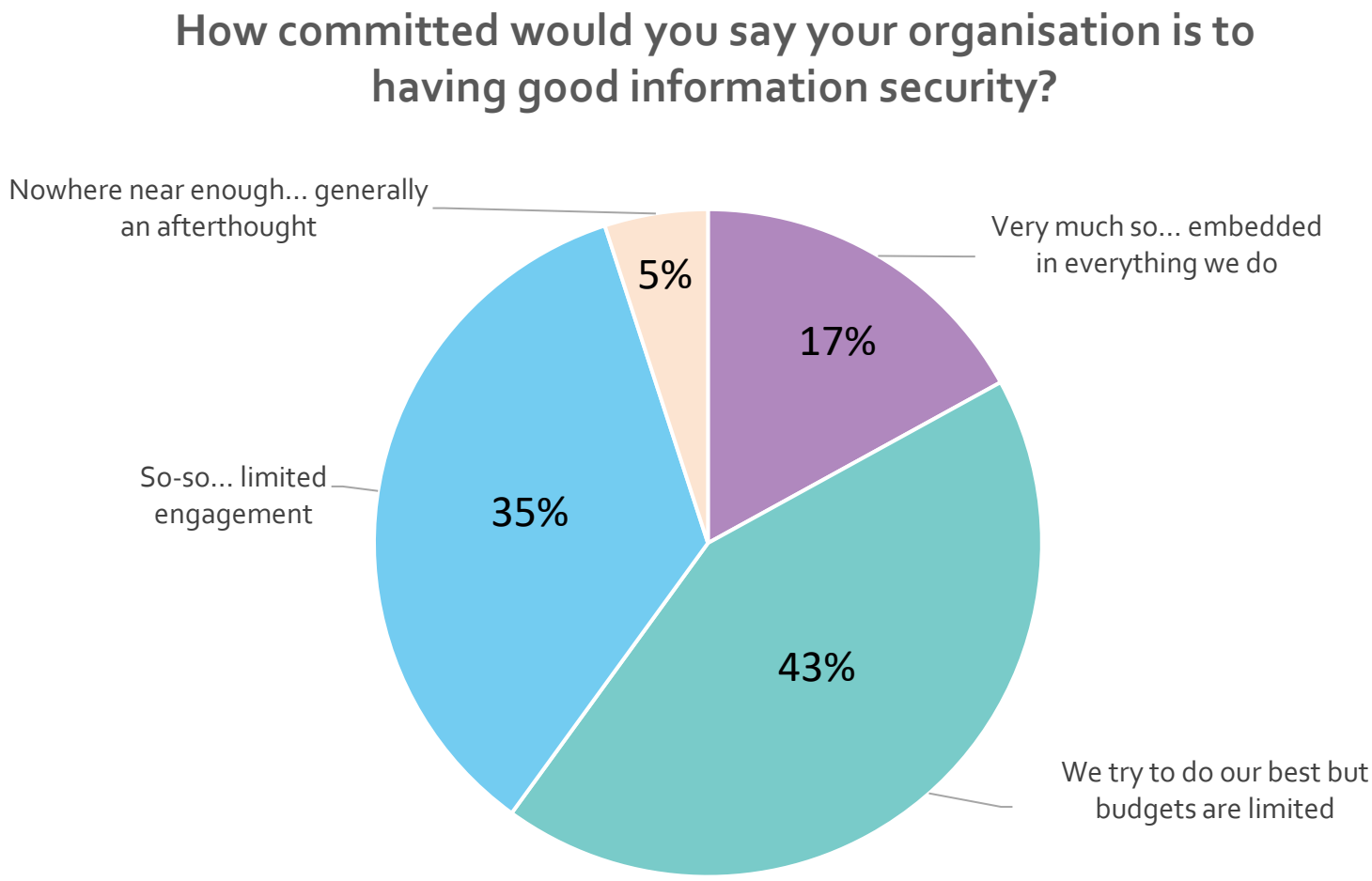
Charities in England & Wales spend **£80Bn** per year!

58% of charities think cybercrime is a major risk to the charity sector

22% believe cybercrime is a greater risk to the charity sector than other sectors

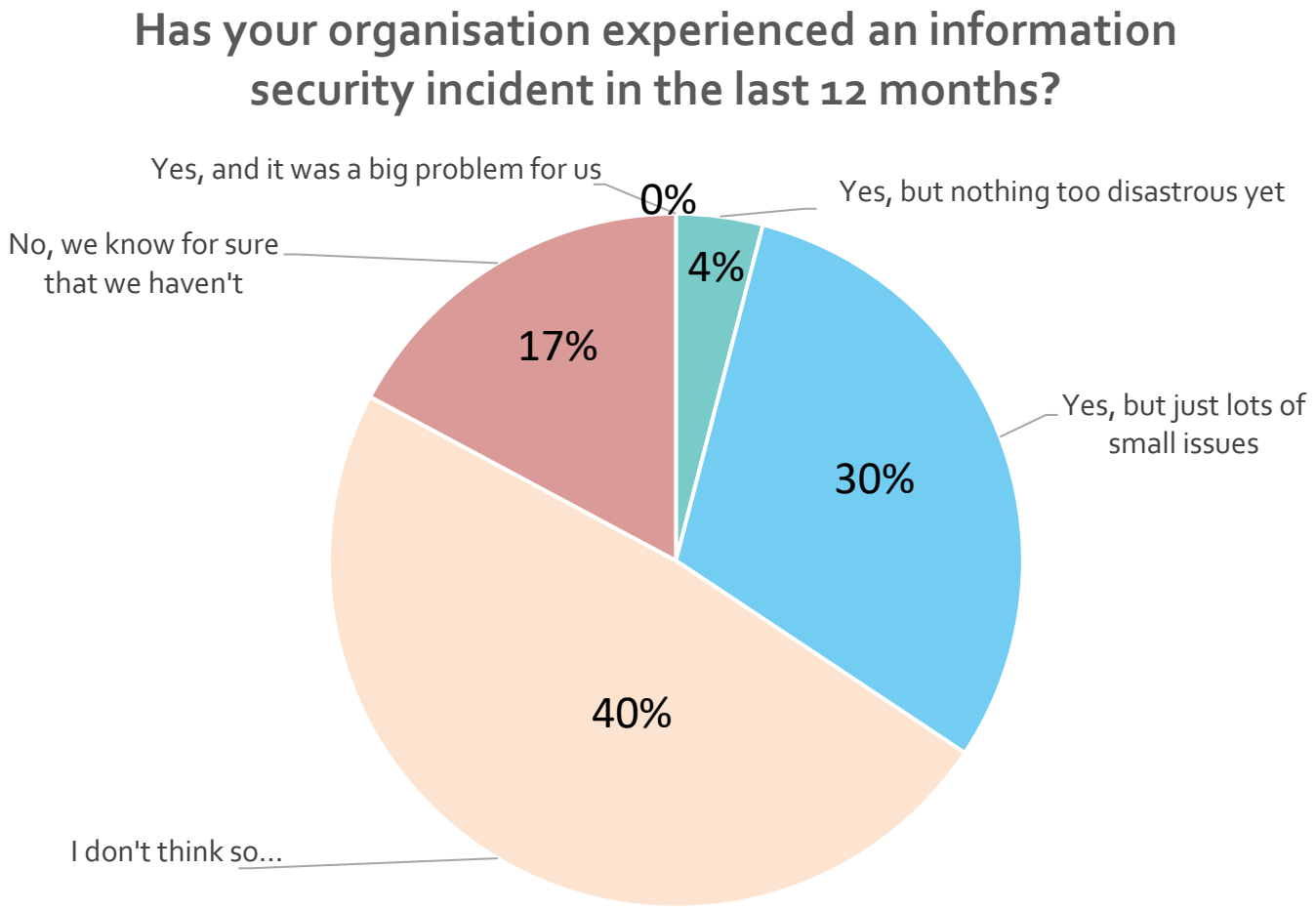
Source: Preventing Charity Cybercrime: Insights+Action. Charity Commission Fraud Advisory Panel, October 2019. Sample of 15,000 charities.

Pre-event survey: Commitment



Source: Adapta Consulting 2021; Survey of 75 webinar participants

Pre-event survey: Incidents



Source: Adapta Consulting 2021; Survey of 75 webinar participants

Pre-event survey: What's on your minds

Engaging others

Improving organisational engagement

How to communicate its importance to exec team – short of having an incident

How to ensure staff and volunteers take responsibility

How to get it taken seriously in my organisation

How do you get buy-in from staff throughout the organisation (at all levels)?

How can we justify investment on security at a time when budgets are being cut?

How are other charities structuring their information security function?

Products and solutions

How secure is Office 365?

What's the right balance between internal vs. supplier responsibilities?

What security products are out there?

Are there any free online resources that would help us plan an audit?

Are cloud products as secure as on-premise solutions?

What to do

Where do we start?

As a trustee, what questions should I be asking?

How to we go from "not sure" to "confident"?

How does information security relate to data protection?

What's appropriate for a charity our size?

What are the emerging changes and regulations?

What must we be doing about it?

How do we keep up to date with the latest security measures?

What should we be doing to address any issues linked to home working?

adapta

Some more stats…

- 51% of IT Leaders have detected ransomware[1]
- 73% of those suffered an effective attack[1]
- 36% of charities don't know which types of cyber attacks they're most vulnerable to[2]
- Half of charities state that the Board has overall responsibility for cyber security; 15% state that nobody has responsibility[2]
- During 2019-2021, 1 in every 6 charities will suffer from cybercrime[2]

Source: (1) Four key tips from incident response experts; Sophos 2020 (based on survey of 5,000 IT managers)
(2) Preventing Charity Cybercrime: Insights+Action. Charity Commission Fraud Advisory Panel, October 2019

How could it affect us?

- Financially
- Reputationally
- Disruption to operations, ability to serve the cause

Cyber breaches – common types

- **Phishing** – 'Dear accounts team, Pay this invoice immediately. Yours sincerely, the CEO' (54%)
- **Ransomware** – 'Send us some bitcoins if you want your files unencrypted' (31% including extortion)
- **Extortion** – 'Give us some money or we'll leak your data on the dark web'
- **DDoS** – 'Botnet' attacks to overwhelm and take an organisation's systems 'down' (5%)
- **Social engineering** – Pretending to be someone else (e.g. you!), diverting donations
- **Innocent/no motivation** – Accidents!

adapta

Source: Preventing Charity Cybercrime: Insights+Action. Charity Commission Fraud Advisory Panel, October 2019. Sample of 15,000 charities.

Who does this (examples)?

Intentionally:

- Criminals – Anything to make some money…
- Hacktivists – 'I'm good with computers and I disagree with your cause'
- Insiders – Disgruntled staff
- Terrorists – Defacing websites, doxing (publishing personal details of victims online)
- 'Nation State' hackers – maybe you're involved in international conflicts

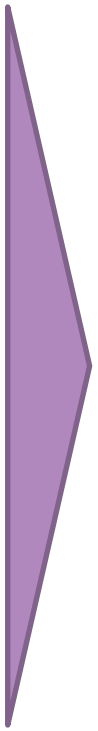
Unintentionally:

- Insiders – Well-meaning but careless or inadequately trained staff
- Suppliers/3rd parties – People who look after data for/with you and suffer their own breaches

Common misconceptions…

What's often said:

- It's an IT issue
- We need a penetration test
- Hackers only target big, well-funded organisations
- Nobody with a conscience would attack a cause like ours
- Our servers are in a ISO/IEC 27001 accredited data centre



The reality:

- Everyone uses information; it's a corporate risk
- Management controls are equally important (if not more so)
- Small organisations have money too! (and possibly have weaker defences)
- Many attacks are automated and indiscriminate
- If they're connected to the outside world, they're vulnerable

adapta

What can we do to protect ourselves?

Clarifying responsibilities

- IT - technical
- Corporate risk ‘owner’ (FD?) – governance and controls
- Trustees – oversight
- DPO/Data Protection Lead
- Managers, staff – processes, daily work
- ‘Information Asset Owners’ – accountability

National Cyber Security Centre
a part of GCHQ

Cyber Security
Small Charity Guide

This advice has been produced to help charities protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/charity** .

Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

- **Identify what needs to be backed up.** Normally this will comprise documents, emails, contacts, legal information, calendars, financial records and supporter or beneficiary databases.
- **Ensure the device containing your backup is *not* permanently connected** to the device holding the original copy, neither physically nor over a local network.
- **Consider backing up to the cloud.** This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

- **Switch on PIN/password protection/fingerprint recognition** for mobile devices.
- Configure devices so that when lost or stolen they can be **tracked**, **remotely wiped** or **remotely locked**.
- Keep your **devices** (and all **installed apps**) **up to date**, using the '**automatically update**' option if available.
- When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs**.
- **Replace devices that are no longer supported by manufacturers** with up-to-date alternatives.

Preventing malware damage

You can protect your charity from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

- **Use antivirus** software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.
- **Patch all software and firmware** by promptly applying the latest software updates provided by manufacturers and vendors. Use the '**automatically update**' option where available.
- **Control access to removable media** such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.
- **Switch on your firewall** (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

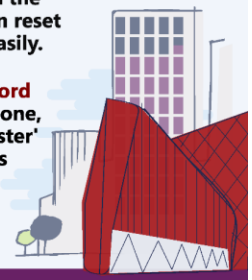
In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

- Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges**. This will reduce the impact of successful phishing attacks.
- **Scan for malware** and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).
- Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

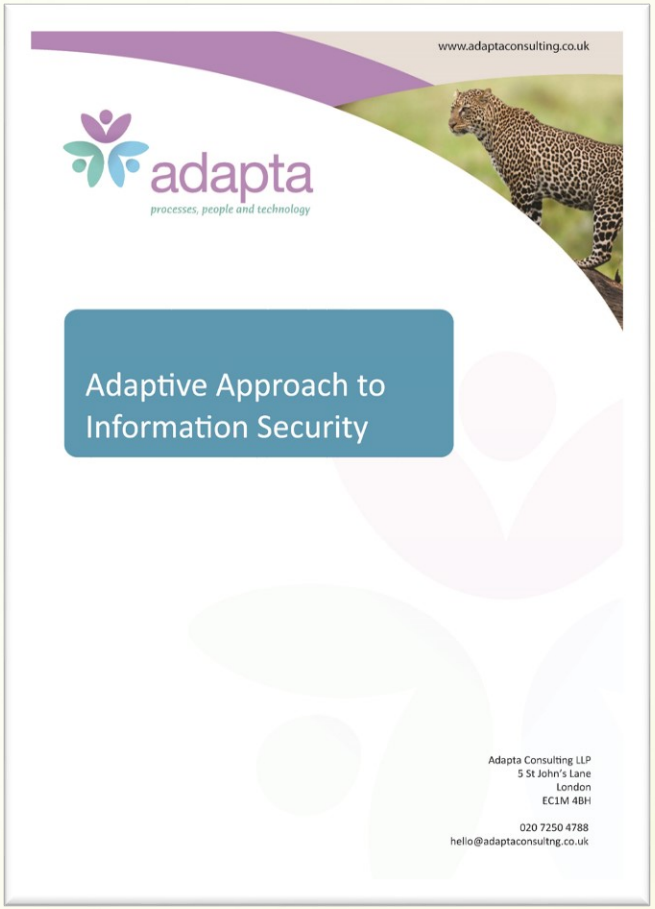
Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

- Make sure all laptops, MACs and PCs **use encryption products** that require a password to boot. Switch on **password/ PIN protection** or **fingerprint recognition** for mobile devices.
- **Use two factor authentication (2FA)** for important websites like banking and email, if you're given the option.
- **Avoid using predictable passwords** (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).
- Do not enforce regular password changes; they only need to be changed when you suspect a compromise.
- **Change** the manufacturers' default passwords that devices are issued with, before they are distributed to staff.
- **Provide secure storage** so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.
- **Consider using a password manager.** If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.



New/updated – Adapta's InfoSec guide



Useful resources

- National Cyber Security Centre (NCSC) – 10 steps to cyber security https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security
- NCSC Small Charity Guide - https://www.ncsc.gov.uk/collection/charity
- Cyber Essentials - https://www.ncsc.gov.uk/cyberessentials/overview
- Preventing Charity Crime (Charity Commission) - https://www.gov.uk/government/publications/preventing-charity-cyber-crime-insights-and-action
- Charity Security Forum - https://charitiessecurityforum.org.uk/

adapta

Questions

Information Security & Cake

Martyn Croft
Charities Security Forum

Charities Security Forum

- founded in 2007 to help colleagues
- promoting awareness of cybersecurity issues and challenges
- facilitating discussion and learning
- over 250 members in diverse charities and not-for-profits
- newsletter updates, LinkedIn group, webinars
- free to join…
- …always ready to help

CSF
Charities Security Forum

Dear CSF…

when we get back to the office our IT and Finance directors have decided they can reduce costs in the IT department by allowing staff to use their own laptops and tablets in the office for work functions.

They see this a win-win solution to rising costs - fewer staff, less qualified staff, no software upgrades to manage, and no expensive hardware costs.

I'm the IT manager and also responsible for information security. What do you think?

CSF
Charities Security Forum

- Bring Your Own Device
- Networks and VPNs
- De-coupling corporate systems
- Virtual machines
- Run an internal ISP

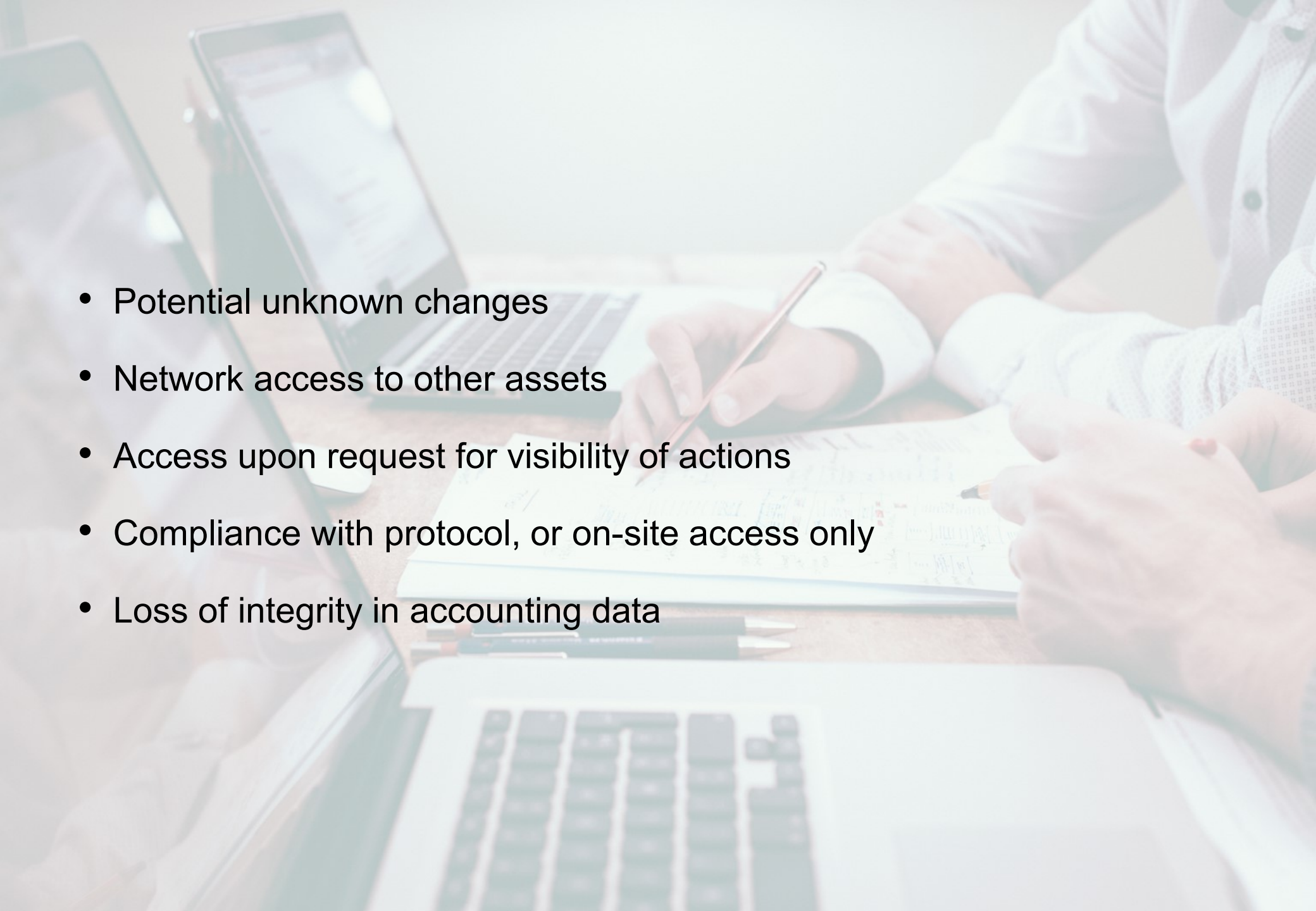
Dear CSF,

the supplier of our new finance system wants remote access to the system so they can support and fix problems.

They want open access all the time and don't see the need for any change control.

The finance director is insisting we give them access but it seems to me like this is an open door to a critical system, and to our network. What's best practice and what should I do?

CSF
Charities Security Forum



- Potential unknown changes
- Network access to other assets
- Access upon request for visibility of actions
- Compliance with protocol, or on-site access only
- Loss of integrity in accounting data

Dear CSF,

We are a very small charity. Our fundraisers have a spreadsheet of our supporters and the details of their donations on a laptop in the finance office.

That is name, address, type of donation (one-off/regular/legacy), amount, bank account details, credit/debit card details.

The fundraisers say they need to keep these details so they can go back to the supporters for more money.

I'm not sure we should keep all of this information. Can you advise please?

CSF
Charities Security Forum

- Purpose of data collection
- PCI-DSS requirements
- GDPR compliance
- Encrypted data and physically safe
- Keep trusted information safe

Dear CSF,

I'm the security manager of a medium sized charity.

My IT director has been watching the news and wants me to produce a "critical incident response' plan.

Any advice on how I start?

CSF
Charities Security Forum

- Business Impact Analysis
- Business Continuity & Disaster Recovery plans
- Probable and Realistic Threats
- Risk = Impact * Likelihood
- Multi-disciplinary Incident Response Team

Charities Security Forum

because security is better together

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

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

Brian Shorten

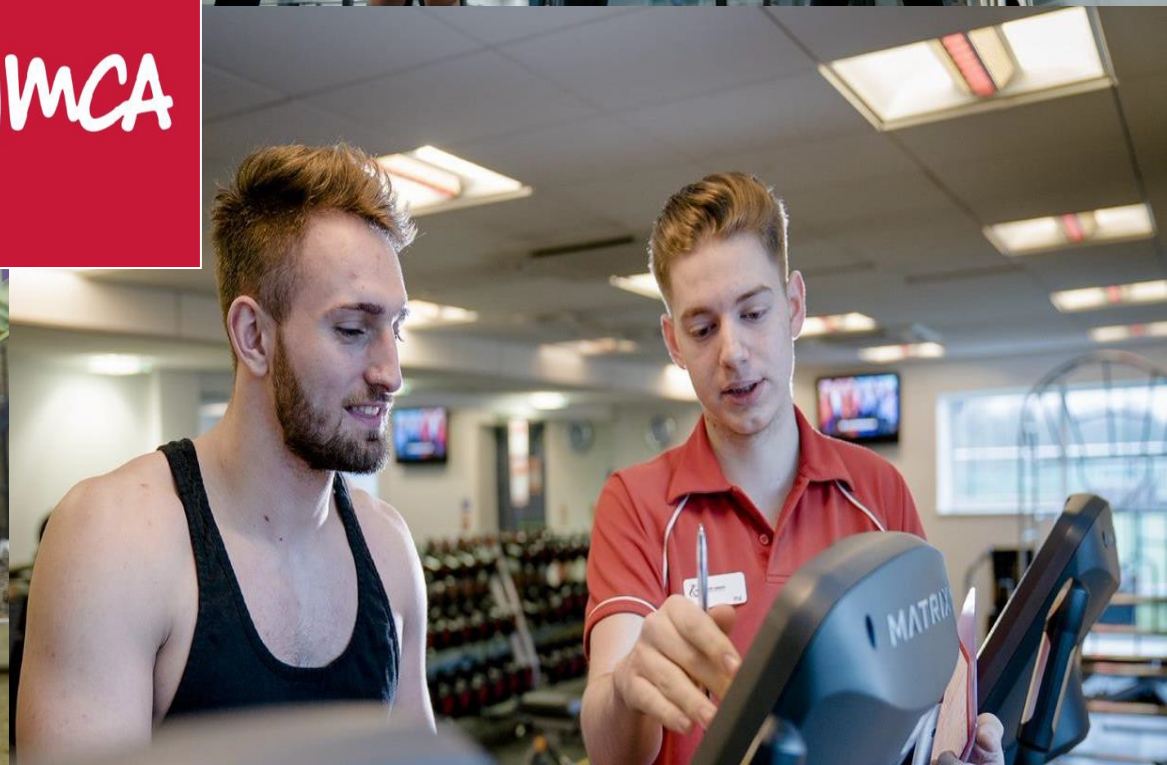
Martyn Croft

www.charitiessecurityforum.org.uk

CSF
Charities Security Forum

Information security case study – Central YMCA

ymca



About Central YMCA

Founded in 1844, the world's first YMCA.

Today, we are a health, wellbeing and education charity, with commercial operations to generate funds to support our charitable projects.

Information security: the business case

- The risk of a major cyber-security or data breach has been a long-standing item on our corporate risk register, with a range of potential causes identified

- We have a duty to protect the Charity's information, assets and the personal data of all our stakeholders

- A failure to mitigate this risk could lead to:
  - Disruption to operations
  - Lack of compliance with legislation and funding requirements (leading to fines, loss of funding etc.)
  - Reputational damage

Our approach

- In 2019 we appointed an external Data Protection Officer (DPO) and established a cross-functional working group.

- Working group comprised:
  - Senior Information Risk Office (sponsor)
  - Business Assurance / Governance
  - External DPO
  - IT
  - Finance
  - HR
  - Marketing
  - Operational representatives

- Data protection audit undertaken in 2019 to review compliance against GDPR / DPA 2018

Information Security Audit

- In Spring 2020 we commissioned Adapta to undertake an independent review of the Charity's information security.
- The review took a pragmatic risk-based approach and included:
  - Interviews with staff who hold significant responsibilities for information security
  - Interviews with a cross-section of other staff who access and process confidential information
  - Detailed review of technical and non-technical background information
  - Review of policies, procedures and management controls

Results and progress to date

- A report was developed with a range of recommendations to help move us to a more compliant position with respect to Cyber Essentials, ISO 27001, the Data Protection Act 2018, GDPR and recognised good practice in information security

- The recommendations were RAG rated against likelihood and impact in line with our risk register and were prioritised accordingly

- These were developed into action plan to be delivered by our working group

Key learnings and recommendations

1. Get sponsorship from the top
2. Build the business case and do not rely on fear tactics (what's in it for them?)
3. Take a cross-organisation approach (not just IT)
4. Create realistic timeframes and prioritise carefully
5. Be prepared to translate issues for a range of audiences to make things meaningful
6. Communicate widely and deliver appropriate training (no one size fits all)

THANK YOU

Registered Charity number: 213121

Breakout Room Discussions

What worries you most about information security in your organisation (or, if you prefer, what do you think are the biggest information security risks to NfP organisations generally)?

What steps could an organisation take to improve its information security posture, without necessarily incurring significant cost?

Re-convene for feedback from each group.

Poll, Thanks & Goodbye!

Upcoming events…

Answer Time: Information security – 21 April

www.adaptaconsulting.co.uk/adapta-events

If you would like further information or any advice regarding your own specific issues, then please do contact the Adapta team at hello@adaptaconsulting.co.uk

adapta
processes, people and technology

INSTITUTE OF CONSULTING
RECOGNISED PRACTICE