

Cyber security and data protection in the Not-for-Profit (NFP) sector

Dave Cartwright

Senior Consultant,
Information Security

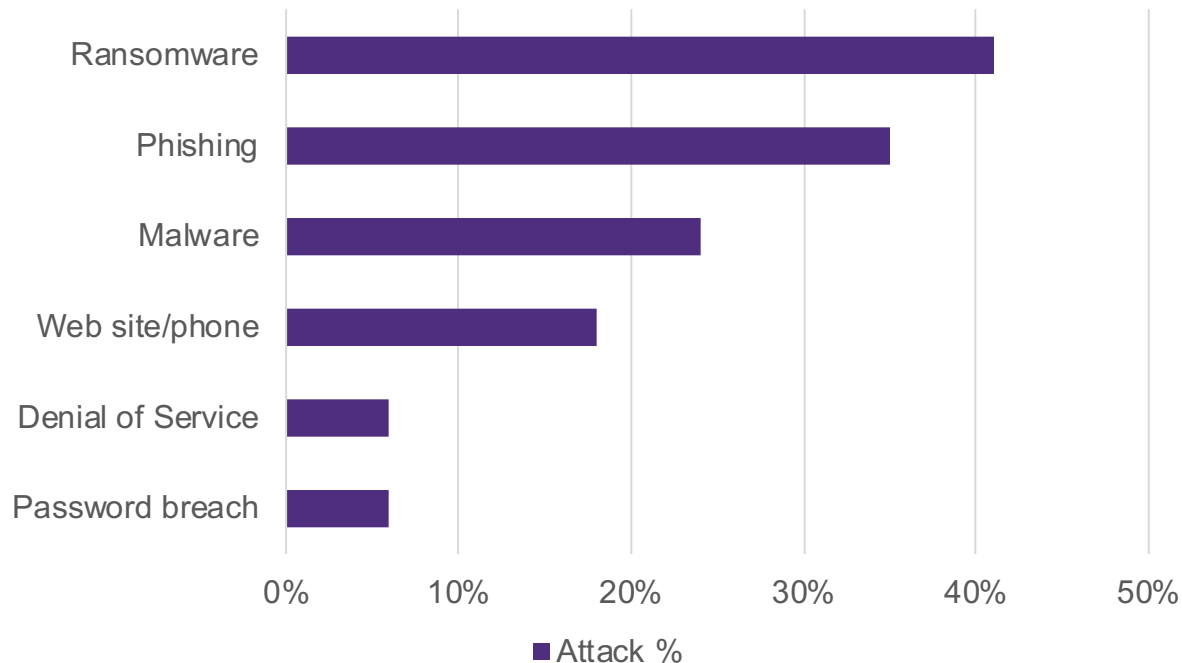


My background



The problem

Charities are subject to cyber attacks



Reality check

- Do charities need the risk of cyber attack?
 - To reduce cyber risk, you can reduce use of technology
- So do they need all this technology?
 - Could they limit their use of tech and reduce risk?

Reality check

- Less tech isn't an option for charities
- Lloyds research: charities with “high digital capability”
 - ... are twice as likely to save time and to increase donations
 - ... are ten times as likely to save cost
- So we need to understand the risks and deal with them



Why are charities special?

In some ways, they're not

- No more or less susceptible than others to indiscriminate attacks
 - Ransomware
 - Phishing
 - Accidental loss of equipment
- But in many ways, in fact, charities *are* special



Finances

- Budgets are limited
 - Even medium-sized charities can't afford several hundred ££ per day for advice/techies
 - IT equipment often purchased on a shoestring
 - And limited funds to manage, upgrade or replace it



Committee hold data themselves

- In fact, charities often have no technology at all
 - People use their own computers
 - Email goes to and from personal addresses
 - And is therefore mixed in with people's own private email
 - Charity records sit in people's houses

Internal technical and cyber skills

- Founders of charities are passionate about their subject
 - Sometimes some access to IT knowledge
 - Seldom any access to cyber or Data Protection expertise
- Not many charities recruit volunteers or committee members for their cyber or DP knowledge

People share credentials

- Single login for the cloud-based accounts package
- Shared login for the Gmail account they use for email
- Shared login for the WordPress Web site

Committee turnover

- Some committee members stick around for years
- But others don't
 - Family commitments, work, etc. have to come first
- When people leave the committee, data goes with them

Many charities hold sensitive data

- Could be “special category” personal data
 - Ethnic origin
 - Health data
- Could be other sensitive data
 - Financial information about donors
 - Data about children

Charity work is often part-time

- Doesn't necessarily lighten the load of obligations
 - The 72-hour breach deadline still applies
 - Do you even check the charity email in this time?
- Spare time is limited
 - Does anyone ever check systems?



There's a lot you can do without help

Don't fret that it's too difficult

- Some of the tech behind cyber security is complex
- But the principles are largely common sense
 - Protect data
 - Don't give it to people who aren't entitled to it
 - Store paper records securely
 - ... etc.

Tech skills more common than cyber skills

- There's usually someone who can make a PC or a Web site work
 - Or a handy teenager
- You can still do many of the basics yourselves
 - Non-techies can do Windows Update, anti-virus, etc.
 - These are as much tech skills as they are cyber skills

The vendors are beginning to help

- Example: small/home office routers
 - Ten years ago: router credentials were admin/admin
 - And it didn't force you to change it
 - Now you're forced to change the password at setup time
- Example: buying a new Mac
 - Prompts you for a strong password and to enable FileVault

There are some easy things you can do

- Check out Cyber Essentials
 - Five simple steps to protect against ~80% of attacks
 - Anti-virus software on everything
 - Keep apps and operating system up to date
 - Change default passwords
 - Principle of least privilege
 - A firewall on your Internet connections



Get a proper, separate email account

- Domains can cost a few pounds a year
- Email access is often thrown in with the domain name
- Keeps it separate from personal email
 - And you can delete accounts and mail when people leave

Keep your technology up to date

- Windows/MacOS updates
 - Both platforms can update automatically, so it's easy
- Anti-virus software
 - It'll update itself – set it to do so several times a day



Encrypt and protect your systems

- It's dead easy with MacOS – turn on FileVault
 - And use complex passwords
- Slightly less straightforward with Windows
 - Google for “free file encryption software”
 - Set a BIOS (boot time) password

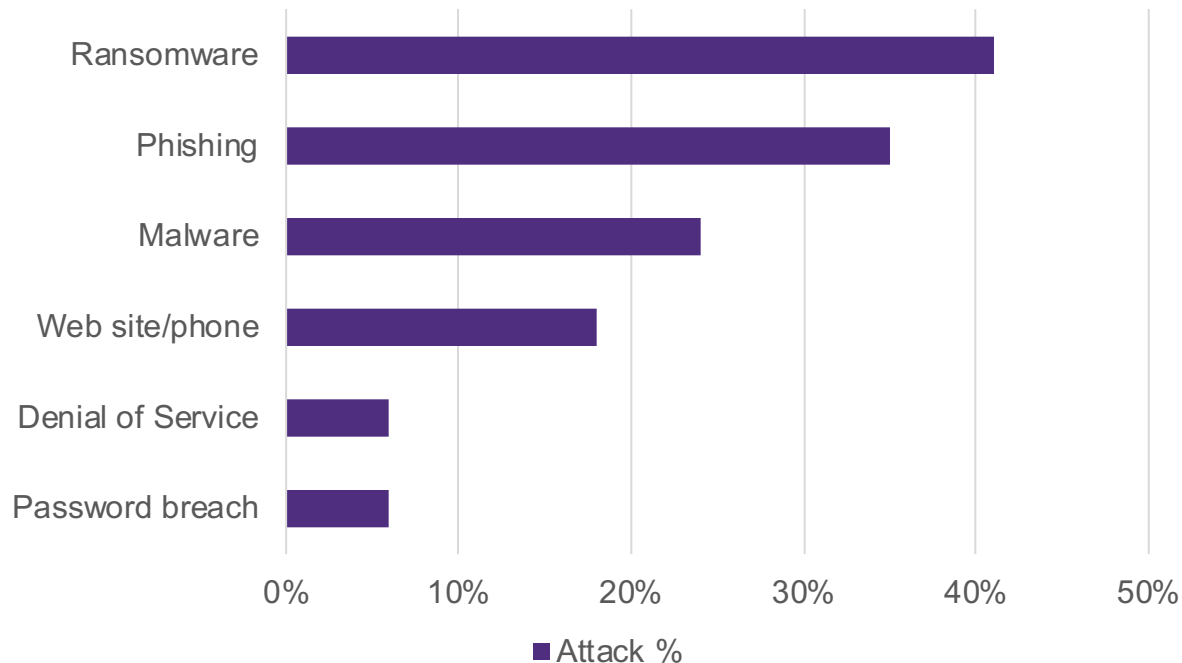


Be wary of cloud services

- By all means use iCloud, Google Drive, etc.
 - I use both so I have a backup of my stuff
- But be diligent
 - Use strong passwords – they're accessible from anywhere
 - MFA is a “must” with all cloud services
 - If you're sharing folders with others, set a time limit



Let's briefly revisit that graph



Data minimisation

- Don't store data that you don't need
- Keep personal data only where you need to
 - And restrict access to only the people who actually need it
- Don't take it with you unless you have to

Use the resources available

- Google is your friend
 - It's quick, free and comprehensive
- Use (but don't abuse) the ICO
 - They're not a replacement for a consultant
 - But they're more than happy to be asked stuff



A new resource you can call upon



Jersey Charitable Skills Pool

<http://www.jerseycsp.org.uk/>

What's the JCSP?



Jersey Charitable
Skills Pool

- A throwaway comment that became a charity
- A pool of cyber security resources
 - Like a “hardship fund” but gives time rather than money
 - Jersey companies give their staff time free of charge
 - Charities/NFPs can apply for resource



What's the JCSP?



Jersey Charitable
Skills Pool

- Opens for applications on 1 March
- We encourage you to share resource
 - e.g. training sessions for several NFPs at once

Growing organically



Jersey Charitable
Skills Pool

- Hopefully the beginning of something bigger
- We've deliberately kept the name general
 - Walking before we try to run ... but we intend to run later
 - Launching with cyber security, but intention to expand
 - Finance, publicity, etc.



References

- Lloyds Digital Business Index
 - <https://resources.lloydsbank.com/businessdigitalindex/>
- Ecclesiastical Charity Cyber Guide
 - <https://www.ecclesiastical.com/documents/charity-cyber-guide.pdf>
- NCSC CE page
 - <https://www.cyberessentials.ncsc.gov.uk/>





Jersey Charitable Skills Pool

<http://www.jerseycsp.org.uk/>

dsc@jerseycsp.org.uk