# The very real cybersecurity threat to charities' reputations

A joint paper from

falanx Cyber

smartdesc SMART DECISIONS

# "We were devastated by this attack"

In March 2022, staff emails and phones suddenly stopped working at the large Scottish charity SAMH (Scottish Association for Mental Health). Gigabytes of sensitive charity data had been uploaded to the dark web. This included names, home and email addresses, and passport scans belonging to donors and volunteers.

SAMH had fallen victim to a deadly cyber-attack by the cybercriminal gang RansomEXX. The impact was considerable - hindering the charity's efforts to continue supporting those in need. But with online fundraising now firmly at the fore, the effect this had on the charity's reputation was even greater.

Speaking of the attack, SAMH's Chief Executive Billy Wilder stressed his disbelief that this had happened to a charity. 'We are devastated by this attack. It is difficult to understand why anyone would deliberately try to disrupt the work of an organisation that is relied on by people at their most vulnerable.'

Unfortunately, such attacks on charities are not uncommon; third sector organisations are often 'soft' targets for criminals.

But why are charities targeted? And what can they do to mitigate against cyber threats and reputational risks?

# Valuable data, limited cyber expertise, stretched budgets – a perfect storm

The latest figures from the Department for Digital, Culture, Media & Sport's annual Cyber Security Breaches Report 2022 show that the incidence of attacks on charities is converging with those on UK businesses:

- In 2018, 19% of charities and 43% of businesses reported they had been attacked
- This has now risen to **30%** of charities reporting attacks in 2022

Targeting a charity is appealing to an attacker: they hold valuable financial, personal and commercial data that the attacker knows will give them leverage, whilst also having limited IT budgets and often non-existent in-house cyber security expertise.

The Cyber Security Breaches Report makes it abundantly clear that charities are increasingly seen as 'soft', attractive targets for hackers; they are either playing catch up, not prioritising risks, or are simply unaware of the threat.

On the cybersecurity threats that charities face , Amie McWilliam-Reynolds, Assistant Director Intelligence and Tasking from the Charity Commission, observed:

*'Online financial transactions, and online working generally, present a great opportunity for charities – whether in engaging supporters, raising funds, and streamlining their operations. But online financial transactions and the collection and storage of personal data also harbour risk, and we are concerned that some charities may be underestimating that risk, and are therefore exposing their charity.'*

# Why charities are a target

A charity's digital footprint is similar to that of those in the private sector; nine in ten businesses have at least one of the following, as do eight in ten charities:

- A digital bank account
- Personal information about customers held electronically
- Network connected devices
- Facilities to order, book or pay online

In addition to this, 44% of charities allow people to donate on the web and 42% have beneficiaries that can access services online.

## Easy infiltration and a lack of cybersecurity prioritisation

Many charities have a much wider (and less well policed) attack surface – the possible points of entry of exit by unauthorised access. The third sector generally relies more heavily on BYOD (Bring Your Own Device) than commercial companies, with 64% of charities reporting staff using their own devices regularly compared to 45% of businesses. As a result, cybersecurity updates and monitoring are more difficult to carry out, and charities are more susceptible to cybersecurity breaches.

Criminals are also aware that risks are much less likely to be assessed and responded to at board and senior management level among charities. Almost a quarter of all charities never update their senior management on cybersecurity actions taken. A similar amount - 26% - do not have a board member who is accountable for cybersecurity.

## Federated charities and the increased risk to reputation

Smaller charities are much less likely to have the resources for addressing cybersecurity threats.

But many charities in the UK, including Mind, Carers Trust and YMCA, operate with a federated structure where a network of smaller, independent local charities is overseen by a national charity.

Such smaller organisations offer an easy route in for hackers. And, should they successfully breach a branch and steal supporters' personal data, then the effects would not just be localised. The national charity that heads the federation could suffer a severe loss of reputation, causing potential supporters to think twice about donating and sharing their details.

## Extended threats to charity networks

Loose links in the chain may not just come from federated structures. All charities have a wider supply chain where data and access to networks is shared. However, according to the Breaches Report, only 4% are actively doing anything to assess the risks that arise from their wider supply chain.

As a recent example, the International Committee of the Red Cross (ICRC) was victim of an attack in which personal data and confidential information on 515,000 vulnerable individuals was stolen from a third party supplier.

# Strategy, monitoring and detection: how charities can secure themselves and their brand reputation

The main victim of a breach, wherever it occurs, is your charity's reputation.

At a time when charities are facing both an expansive attack surface and a weak cybersecurity focus from senior managers, the two most effective solutions to reducing this risk to reputation come from the hiring of a Virtual CISO (Chief Information Security Officer) and MDR (Managed Detection and Response).

A cost-effective way to ensure that charities can benefit from board-level expertise, and strategic cybersecurity guidance is to hire a Virtual CISO (or vCISO). Sometimes referred to as a CISO-as-a-Service, this is where you partner with an outsourced security expert (or team of security experts) to guide and direct your cybersecurity priorities and protection. Smartdesc's vCISOs typically work alongside existing internal IT teams on a part-time basis, acting as in-house, impartial and trusted advisors; driving the cyber strategy forward through deep collaboration with all levels of your business.

Charities can access immediate help from highly experienced vCISOs through Smartdesc's Information Security Manager service. With their in-depth understanding of IT security, combined with a sole focus on the Not for Profit sector and being NCTO-approved IT providers to the sector, they ensure cyber security improvement projects are led from the front and make sure your attack surface is monitored  reducing the time it takes to detect and respond to threats.

Falanx Cyber MDR service offers continuous protective monitoring of your network by the latest tech and a team of UK security-cleared analysts. While risks are investigated and prioritised, proactive hunting will discover existing threats to, or weaknesses in, your network. And this includes identifying threats from your third-party network. MDR covers your entire IT environment and endpoints. This makes it ideal for dispersed networks as it enables visibility of any activity anywhere that could threaten your organisation. This visibility allows you to confidently focus on other strategic tasks, rather than fighting cybersecurity fires.

**Charities, like yours, are on cybercriminals' radars. Falanx Cyber and Smartdesc are IT experts uniquely placed to overcome the cybersecurity challenges in your sector.**

**Between us we work with over 80 charities including Mind, Shelter and YMCA to identify weaknesses, prevent attacks and improve overall IT strategy. Speak to us today to learn more about enhancing cybersecurity at your organisation.**

## About Smartdesc

Smartdesc is an IT Service Provider and NCVO Trusted Supplier who specialise in helping charities improve their IT effectiveness. We partner with household names such as Mind, Terrence Higgins, WaterAid and the YMCA to improve their IT systems, cut costs, reduce cyber security risk, and optimise hybrid working via Microsoft 365 and Teams.

www.smartdesc.co.uk
0203 440 2445

## About Falanx Cyber

Falanx Cyber is a provider of cyber security services that identifies areas of cyber risk and deliver end-to-end managed services to alleviate those risks. We specialise in Managed Detection and Response (MDR) and Incident Response services from our 24/7/365 Security Operations Centre (SOC) in Reading, UK. Combined with our security testing and advisory services we focus on improving our clients' cyber resilience, and ultimately enabling them to withstand, cyber-attacks.

Falanx Cyber is part of Falanx Cyber Security, a publicly listed business traded on the AIM stock exchange.

www.falanxcyber.com
020 7856 9450

Falanx Cyber holds, operates to, and delivers its cybersecurity services in accordance with the following certifications and accreditations:

QMS ISO 20000-1:2018 REGISTERED
Certificate No:383902021

QMS ISO 9001 : 2015 REGISTERED
Certificate Number: 383882021

QMS ISO 27001 : 2013 REGISTERED
Certificate Number: 383882021

CYBER ESSENTIALS CERTIFIED PLUS

CREST. VA PEN TEST

falanx Cyber | Crown Commercial Service Supplier

smartdesc SMART DECISIONS

falanx Cyber