National Cyber Security Centre
a part of GCHQ

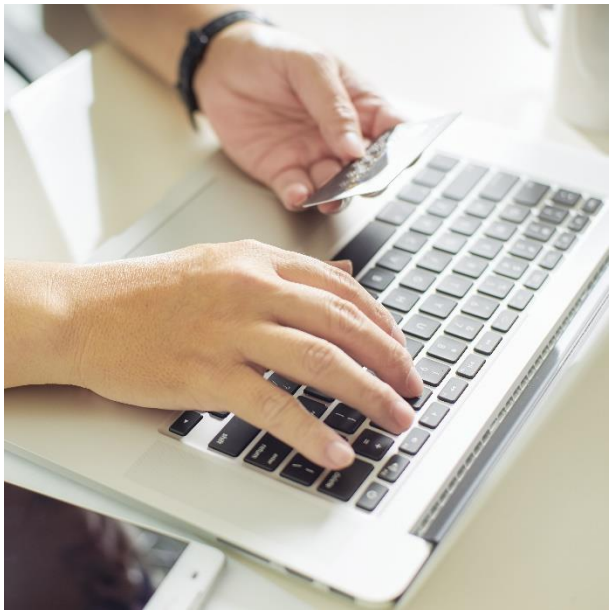
Cyber threat assessment: UK charity sector

February 2018





Contents



Key findings

UK charities hold funds, personal, financial and commercial data (and other information) that is of interest or monetary value to a range of cyber criminals and other groups. Some charities are aware their data is sensitive, valuable and vulnerable to attack. However, the National Cyber Security Centre (NCSC) believe that many charities - particularly smaller ones - do not realise this and do not perceive themselves as targets.

The scale of cyber activity against charities is unclear. Whilst some charities report cyber incidents externally, others may not for fear of reputational and/or financial consequences, or through uncertainty of how and where to register the offence. Under-reporting is hindering our understanding of the scale of the threat to the charity sector.

Malicious cyber activity against charities could impede their ability to deliver their services. It may also affect the integrity and reputation of an individual charity, and that of the sector in general. The culture of openness in the sector makes charities particularly vulnerable to some types of cyber criminal activity, such as cyber-enabled fraud and extortion.

We consider there is considerable variation in charities' understanding, approach to and application of, cyber security.

Smaller charities may not consider it a priority to commit resources to cyber protection, perhaps in the belief that cyber security will be expensive and divert money away from frontline expenditure. Or maybe they do not fully understand the threat.

Pending legislation (the General Data Protection Regulation), continuing high levels of cyber criminality and growing use of online business practices by charities mean investment in cyber security is increasingly imperative for the sector.

Scope of this assessment

This assessment has been produced to raise awareness of the cyber threat to the UK charity sector. It considers cyber criminals (and other groups that pose a threat to charities) their motivations and some of their methods. A forward look, anticipating how changes in the cyber landscape may affect charities, is also included.

This assessment does not give specific technical information on how charities have been targeted, evaluate infrastructure weaknesses of specific organisations, nor offer guidance on how to mitigate against cyber threats. Specific advice for the charity sector is now available to download from the NCSC website at www.ncsc.gov.uk/charity.

This report draws on consultation with experts within the NCSC, the Charity Commission for England and Wales and open sources. There may be cyber capabilities and/or activities being conducted by cyber criminals and other groups that have not been identified. We are not aware of comprehensive data on the scale and types of cyber incidents in the sector: judgements on the scale and types of cyber activity against the sector are therefore given with reduced confidence.

Sector definition

The range of activity by UK charities is broad and diverse, and benefits many sections of society, both here and overseas. Charities range from large, internationally recognised organisations to small, local community organisations.

For the purposes of this paper, the charity sector is defined as those registered with UK Regulators for the sector[1]:

- The Charity Commission for England and Wales is the Regulator of charities for that jurisdiction, with which there were 166,963 charities registered in June 2017.
- The Office of the Scottish Charity Regulator is the independent Regulator for Scottish charities: it has 24,078 charities currently registered. The Charity Commission for Northern Ireland is the independent Regulator for Northern Ireland charities.
- A process of formally registering the estimated 7,000 plus charitable organisations in Northern Ireland has been underway in recent years.

[1] The criteria for a charity to register with the Charity Commission for England and Wales is an income of £5,000 per year. Unregistered charities are subject to the same rules as those registered. Subject to certain conditions, some charities are also 'exempt' from registration, or are overseen by other regulatory bodies.

Who might target the sector, and why?

UK charities hold funds, personal, financial and commercial data and other information that is of interest or monetary value to a range of cyber criminals and other groups. The type and amount of information held varies according an individual charity's size, objectives, structure and contacts. Charities are subject to the same cyber vulnerabilities as other organisations and businesses that conduct financial transactions, and rely on electronically held data or information to conduct day-to-day operations.

Thirty charities interviewed for a recent government-commissioned report had collectively experienced a range of cyber breaches in the last two years including viruses, phishing emails, ransomware attacks, identity theft, website takedowns and variants of online financial fraud. The breaches resulted in loss of funds, data and website control. Although based on a very small dataset, the findings suggest that malicious cyber activity against the charity sector is varied and enduring.

Cyber criminals

Cybercriminals vary from advanced, professional groups to small-scale fraudsters. The technical skill required to commit cyber offences is decreasing, as the tools required are easily and cheaply available through online criminal forums. The growing availability of tools and services for hire (Crimeware-as-a-Service) such as malware and distributed denial of service (DDoS) is further lowering the entry barrier for would-be cybercriminals or those with low technical proficiency.

Cyber criminals are primarily motivated by financial gain. They may seek to directly steal funds held by charities used for running costs or to supply grants and enable frontline activity. Alternatively, cyber criminals may seek to capitalise indirectly through fraud, extortion or data theft.

Datasets containing personal details and financial information are an attractive target: such information will be sold in online criminal forums to enable fraudulent activity using those details. Charity datasets may contain personally identifiable information (PII) of donors, trustees, patrons, partners, paid staff and volunteers. Some large charities hold several million donor records. The data may also include payment details relating to donations including card details.

Ransomware and extortion

The outward facing nature of charities and a culture of trust in the sector makes them particularly vulnerable to criminality. Cyber crime malware campaigns often rely on social engineering techniques, typically deceiving end users into clicking on malware-infected links in (often plausible and well-crafted) phishing emails or visiting compromised websites.

Current techniques used by cyber criminals are more confrontational and extortive than in previous years. Charities may be targeted directly, be inadvertently affected by malware aimed elsewhere, or by mass indiscriminate campaigns seeking to exploit as many victims as possible. Malicious actors may not only steal or deny access to data; they may delete or change it.

Alternatively, attackers may steal and threaten to release data unless a payment is made (or another demand is met). Charities involved in the protection of vulnerable individuals or holding sensitive medical data could be particularly susceptible to this form of extortion.

Business email attacks

Cyber-enabled fraud aimed at tricking employees with financial authority into transferring money to criminals is increasing. A UK charity lost £13,000 after the email of its CEO was hacked and a fraudulent message sent to the charity's financial manager with instructions to release the funds.

There are several variations of this type of fraud. For the purposes of this paper, they are referred to as business email attacks. Criminals may initially compromise the email accounts (usually business rather than personal accounts) of a company's senior executives or finance or legal personnel. Spoofed emails are then sent ordering unsuspecting employees with financial authority to carry out money transfers that are diverted to the criminals' accounts.

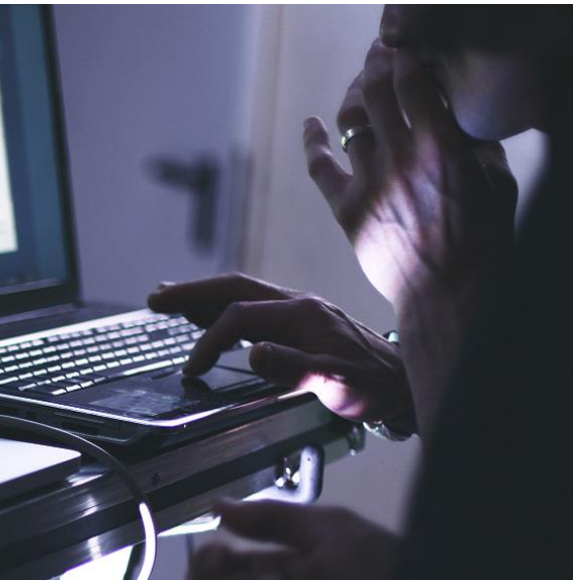
Criminals may succeed in prompting fund transfers using purely social engineering, but more developed campaigns combine the fraud with the deployment of malware to capture information that can be used to generate greater returns. According to their size and resources, charities have departments and/or individuals with authority or responsibility for transferring funds. Again, the culture of trust in the sector may make charities especially vulnerable to this type of exploitation.

Fake organisations and websites

Criminals exploit the credibility and appeal of charities to trick donors into giving money to what appears to be a legitimate charity. This is often achieved through the creation of fake organisations and accompanying websites. Some of these fraudulent websites are well designed, functional and look professional. Criminals react quickly to exploit disasters and global events to steal donations. Although not directly targeting charities by cyber means, this activity has potential financial and reputational ramifications for genuine charities. Criminals may also use the brand of a charity to add credibility in phishing campaigns.

Are cybercriminals the greatest threat to the charity sector?

The funds and types of data and other information held by charities are attractive targets for cybercriminals. Some reported cyber incidents in the sector have involved methods typically used by cybercriminals. 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.



Nation states

Nation states employ cyber capabilities to further their own national agenda and prosperity. Some charities operate through local partner organisations in the UK or overseas. Others play a role in helping formulate and deliver UK domestic and foreign policy. We assess this makes them potentially attractive targets for states who oppose or mistrust their activity.

Hacktivists

Hacktivist is a term used to describe hackers motivated by a specific cause, for example to further political or personal agendas or in reaction to events or actions they perceive as unjust. Hacktivists have successfully used DDoS attacks to disrupt websites, or have exploited weak security to access and deface them.

In 2012, a hacktivist gained access to the website of a UK charity, defacing it and stealing personal details. The charity received a substantial fine from the Information Commissioner for the breach. Although this incident was not recent, it illustrates the potential consequences for charities of a cyber breach.

The NCSC believe that the charity sector is not a priority target for hacktivists, but even a limited website takedown or defacement, could have financial, operational or reputational implications.

Insiders

An insider is someone who exploits, or intends to exploit, their legitimate access to an organisation's assets for unauthorised purposes. Insiders can pass on credentials to attackers (they may have been recruited by other actors, such as criminals or states), or conduct activities such as stealing data. They may be motivated by a variety of grievances, convictions or external pressures.

Insiders may include disgruntled current or former staff who have left an organisation but retained access to their former employers' computer systems. However, insider threats are not always malicious. Employee breaches of security procedures resulting from carelessness or ignorance can introduce vulnerabilities, for example introducing unauthorised software to a system or opening a malicious attachment.

Terrorists

For terrorist groups such as Daesh (ISIS), Al Qaeda and affiliates, website defacement and 'doxing' (publishing the personal details of victims online) are cyber methods most likely to be used. On most occasions, the data released through doxing is already publicly available.

Indirect attacks: suppliers and third parties

Threats may not come from direct attacks on charities. It is common, especially for smaller charities, to outsource the responsibilities for running, maintaining and securing their IT and data to specialist support companies. Charities may also share data with external organisations such as marketing companies. Cyber criminals and other groups may be able to gain access to charities' networks and/or information through these companies. Additionally, cyber criminals may be able to access UK-based charity systems through linked branches or projects in other countries where the security culture may be less stringent than in the UK.

Forward look

In common with other organisations, charities have a duty of care to safeguard their information. The General Data Protection Regulation (GDPR), which comes into force in 2018, will impose increased penalties on organisations that fail to adequately protect their data, and makes breach notification mandatory in some situations. Good security is essential for GDPR compliance. We consider that some UK charities are unprepared for the introduction of this important legislation, and do not understand the link with robust cyber security.

Cyber incidents now often feature prominently in media reporting. There is a growing awareness amongst businesses of the potentially major consequences of a significant data breach and a recognition of the need to allocate specific responsibility and accountability for cyber security.

For a charity, a cyber incident that renders funds or information inaccessible may ultimately affect its ability to deliver its services. The adverse publicity of a breach could affect the integrity and reputation of the particular charity and that of the sector in general. As charities compete for funds, a cyber incident may (at least in the short term) discourage donors, which could in the extreme pose an existential threat to a small charity.

Previous surveys on the charity sector have noted a broad lack of specialist staff with technical skills to cover cyber security (and issues with maintaining these skills in the sector), a low awareness of government support available and a low level of digital skills, exposing charities to further cyber risks. Addressing these issues is important, as the use of online business practices in the sector will continue to grow. For example, charitable donations are moving increasingly online as older payment methods such as cheques are used less.

Cyber criminals and other groups will continue to use tried-and-tested capabilities but will develop and refine methods in response to changes in defences etc. Spear-phishing will continue to be a highly effective infection tool: well-crafted bogus emails that enable social engineering and deliver malware will remain successful, despite measures to enhance employee awareness. Ransomware attacks will continue to target businesses and organisations, driven by the perception that such targets are likely to yield higher returns than the targeting of individuals.

Conclusion

The NCSC believe there is considerable variation in charities' understanding, approach to and application of, cyber security. Some charities are aware their data is sensitive, valuable and vulnerable to malicious cyber activity. We believe many, particularly smaller charities, do not realise this and do not perceive themselves as targets.

Charities are falling victim to a range of malicious cyber activity, but the scale of this activity is unclear due to under-reporting. Whilst some charities report breaches to the Charity Commission and/or law enforcement, other incidents may be only reported internally to trustees or IT providers and dealt with in-house. Incidents may not be reported externally for fear of reputational and/or financial consequences, or through uncertainty of how and where to register the offence.

Larger charities, especially those operating like major corporations are in a better position to allocate specific cyber security responsibilities and take a pro-active approach to cyber security. For smaller charities with resource constraints, and where individuals often perform multiple duties, this may not be deemed possible or necessary. Some charities may perceive cyber security as incurring major costs or be unable to commit resources to it for fear of criticism that money donated for their core services is being spent on 'administration' or because their budgets are ring-fenced.

Investment in cyber security is increasingly important for charities in order to protect their finances, information, operational capability and reputation. Such investment may not require a financial outlay or take a lot of time and may in the longer term prove cheaper than repairing the damage after a cyber attack. We encourage all charities, especially smaller ones, to make use of the NCSC's guidance on reducing the impact of cyber attacks, which is available from www.ncsc.gov.uk/charity .

National Cyber Security Centre
a part of GCHQ

Cyber threat assessment: UK charity sector

February 2018