Grant Thornton

Charity cyber security

Charity Chairs of Audit Committee virtual roundtable

Introduction

Grant Thornton recently held a virtual discussion for Chairs of Audit Committee (or equivalent), focussing on the charity sector and how cyber risk remains a threat, why it is a threat, and what can be practically and proportionately done to mitigate the risk. Held under Chatham House Rules, the discussion raised a number of themes and questions which are outlined in this document.

2023 National Cyber Statistics

Stuart Sivieri, Grant Thornton's Head of Cyber Operations, led the session with a short presentation, first discussing the 2023 National Cyber statistics from the National Cyber Security Centre (NCSC). Cyber was seen as a high priority for 82% of corporates, compared to 72% of charities in 2022, and for 2023 this dropped down to 71% of corporates and 62% of charities. But only 18% of charities overall are aware of the 'Small Business Guide' and 'Small Charity Guide' which are specific guidance documents created by the NCSC which offers key tips and facts to help charities and small businesses to protect themselves from cyber threats.

Why are charities a target?

A lot of cyber-attacks are 'faceless criminal acts' and the hackers may not know exactly what kind of organisations they are attacking, but once they have located vulnerabilities within the technology, hackers can then apply pressure to hold data to ransom and extort the organisation.

Some hackers do specifically target charities for a number of reasons:

- Charities hold a wealth of sensitive or valuable information that could lead to financial gain;
- Charities may feel reluctant to spend resources on cyber security enhancements, rather than front line charitable work;
- Volunteers and part-time staff are a large part of charity workforces and may not have the time capacity to fully understand cyber procedures;
- Many charities allow staff to use personal IT (Bring Your Own Device (BYOD)) which is harder to secure than centrally managed equipment; and
- The impact on a charity could be significant due to limited insurance coverage, limited funds and limited support from other agencies.

Cloud storage and access

To begin with, participants asked about the robustness of shared devices and cloud-based storage such as SharePoint. Over the last few years, one of the biggest changes in the IT landscape has been the migration from large server rooms to cloud servers which are hosted and secured by third-party organisations. A key theme around cloud servers is 'access control,' which deals with the governance and control of data, and how organisations should apply due diligence to prevent unauthorised access to data. Linked to this, and a factor that is often seen in charities, is 'shared credentials.' This is where an organisation has one username and one password to access a whole host of systems, and a number of staff or trustees have access to this.

Charities can obtain accreditation through 'Cyber Essentials,' a government-backed NCSC scheme which offers protection against a wide variety of common cyber-attacks. The accreditation is based on 5 pillars:

- Firewalls
- Service configuration
- User access control
- Malware protection
- Patch management

The accreditation helps organisations to understand how to manage areas like user access and ensure that there are robust internal controls and procedures in place to discourage hackers. Grant Thornton can assist organisations in achieving Cyber Essentials 1 & 2 – please contact our Cyber team for more information.

But a further participant noted that as charities continue to grow, the current security methods in place may not always be appropriate. With respect to BYOD, there are expensive solutions to ensure protection of those devices, but those solutions may not be in line with the overall strategy of the charity, or be a financially viable option. Indeed, a policy where only specific, up-to-date devices can access the system can create a vulnerability if not consistently applied, and there may be over-reliance on external providers where a third party is responsible for that secure connection.

Security monitoring and threat intelligence

The group spent some time discussing security monitoring and threat intelligence. Stuart explained that 'threat actors' often use legitimate accounts and tools to gain access to systems, meaning that from the outside, everything 'looks normal.' But Next Generation Antivirus (NGAV) is a new, smart technology which understands how the attack is happening, rather than just identifying the area of attack (which is what old antivirus software does). Security monitoring is still required, however. This relates to individuals reviewing metrics and data and identifying 'unusual' behaviours – for example system access at 3am on a Sunday may be unusual for a charity whose operations are largely 9-5 and office based. The security monitoring team would notice this, report it to the organisation and then actions can be taken.

Building on this, Stuart went on to explain to the group about managed detection response services. This involves the application of technology in line with prevention principles. For example, a 24/7, 365-days-a-year Security Operations Centre (SOC) provides monitoring, remediation and proactive threat hunting to identify and respond to cyber incidents.

The group then heard that there is threat vulnerability from the dark web. The dark web enables threat actors to sell stolen data to the highest bidder and more and more organisations are looking for support to monitor the dark web in order to pre-empt any attacks. Charities and businesses want to know if they are being targeted next, or if they have been targeted and any sort of data has been leaked onto the dark web. Threat intelligence enables these organisations to understand more deeply the risks to them, and if real time, if they are vulnerable to an attack.

A holistic approach by trustees

The discussion then moved on to tackle the topic of what trustees can and should be doing in their respective charities. One participant observed that in their charity, they are considering information and data governance as a whole, with the Audit and Risk Committee gaining assurance over their security by asking for a regular update relating to the cyber security framework.

Another member observed that for a lot of trustees, cyber security is a new concept and one that most do not have detailed experience of. Where there are trustees and staff who use technology for social media, emails and other more basic functions, there is a risk that personal devices used for operational purposes are not sufficiently protected. Policy implementation around saving documents to secure areas only (such as a SharePoint or Google Workspace environment) would mitigate the threat arising from documents held on personal devices with no protection. Stuart demystified the assumption that 'data is secure because it is in the cloud' as this is only the case where you have a 3rd party to protect the data, which is now required by law. Cloud providers now do have to provide some element of security to protect organisations' data.

Insurance

The group explored the topic of cyber insurance and the in-depth work and questions that need to be addressed before an insurance company would often even consider providing cover. Cyber insurance can be expensive, but the market has responded, and many providers have lowered premiums recently. Cyber insurance has lots of benefits including indemnity or liability costs that come from loss of data. Many elements of cyber insurance cover the ransomware negotiations and fees, legal costs. Because of these features, there is a huge appetite to obtain cyber insurance.

Another participant then raised the ethical quandary around paying ransom in the event of a ransomware attack. Participants discussed that whilst some organisations will pay a ransom to release their data, charities find themselves in a complex position where their charitable objectives mean that payment of ransom can potentially not occur. Participants further mentioned that paying ransom may, inadvertently, lead to financial support of organised crime or terror activities and create significant reputational damage.

Furthermore, payment of a ransom may be in breach of a charity's articles and therefore be a reportable matter to the Charity Commission. However, each charity would need to consider their situation and make a decision which is appropriate for them: if data were being held ransom in a care organisation, the board may consider a ransom payment in order to save lives and protect the people in its care. In any event, regular and thorough communication with the regulator would be essential for a charity being held to ransom to allow for a cohesive resolution.

Summary

Cyber risk remains a key threat to charitable organisations and the level of knowledge varies between different charities. From this session it was pleasing to learn that an array of charities are taking steps to protect themselves, through insurance, achieving Cyber Essentials accreditations, internal audits and internal policies and procedures. It is clear that there remains some uncertainty in the sector, especially where trustees do not consider themselves to be 'tech savvy' but an increasing awareness of risk around personal devices and cloud computing shows promising advancements in these areas.

Key Terms

BYOD (Bring Your Own Device)

The concept of employees using their personally owned device(s) for work purposes.

Cloud storage

A method of computer data storage in which digital data is stored on servers in off-site locations. The servers are maintained by a third-party provider who is responsible for hosting, managing, and securing data stored on its infrastructure.

Dark web

Refers to encrypted online content that is not indexed by conventional search engines. Accessing the dark web can only be done using specific browsers, such as TOR Browser.

Ransomware

A type of malware which prevents access to devices and the data stored on them, usually by encrypting files. A criminal group typically then demands a ransom in exchange for decryption.

Next Generation Antivirus (NGAV)

Uses a combination of artificial intelligence, behavioural detection, machine learning algorithms, and exploit mitigation, so known and unknown threats can be anticipated and immediately prevented.

Threat actors

Also known as malicious actors, are any person or organisation that intentionally causes harm in the digital sphere.

Contact us

If you have any questions or thoughts for future topics for discussion please contact us:

Stephen Dean
Director, Not-for-Profit Audit
T +44 (0)20 7728 2954
E stephen.t.dean@uk.gt.com

Paul Rao
Head of Not-for-Profit
T +44 (0)20 7865 2445
E paul.rao@uk.gt.com

Harriet Raine
Not-for-Profit Technical Manager
T +44 (0)113 245 5514
E harriet.g.raine@uk.gt.com

Stuart Sivieri
Associate Director
T +44 (0)20 7184 4538
E stuart.sivieri@uk.gt.com

GRANTTHORNTON.CO.UK

Grant Thornton