October, 2019

Be Fraud Aware: Lessons From Charity Awareness Week

On 24 October, our firm hosted the 'Be Fraud Aware' charity fraud prevention conference organised by ICAEW North West in Manchester. Here are some key takeaways from the event.

Kevin Lucas of ICAEW welcomed Alan Bryce, Head of Development, Counter Fraud and Cyber-Crime at the Charity Commission, to speak at the conference.

Mr Bryce unveiled two national surveys that have been undertaken by the Commission into charity fraud and cyber-crime this week. These are believed to be the biggest conducted anywhere in the world and which had asked charities about their perceptions as well as their most recent experiences of fraud and cyber-crime.

These surveys revealed that while over two thirds of charities think fraud is a major risk and 85% think they are doing everything they can to prevent it, almost half don't actually have any good-practice protections in place and less than 9% have a fraud awareness training programme for their people.

A key message from the surveys is that fraud awareness is critical for everyone who works within a charity, from trustees and senior management to staff and volunteers. Trust makes the Charity sector work, but it is being exploited every day.

Mr Bryce advised charities to refrain from simply putting lots of controls in place, as fraudsters know how to get around them and instead to focus on the robust and consistent application of a few key controls.

Mr Bryce suggested that organisations should ask for everyone who works for them to spend a little time - maybe even just a couple of minutes at a time - doing fraud awareness training.

He indicated that this helps organisations to establish and strengthen a 'fraud aware' culture, one of openness and honesty where people feel able to hold up their hands and admit to making mistakes - and to learn from them. Fraud will always happen, so the best strategy is to be as prepared as possible to deal with it and not to pretend that this risk can ever be eliminated completely.

In light of this research, the Commission has asked charities to share their stories and to report fraud to the authorities. It has also reminded charities to raise serious incidents of fraud with the Commission itself, so it can share learning with the sector via more regulatory alerts and fulfil its statutory objectives and strategic priorities.

Mr Bryce closed his speech by offering some practical tips to help charities reduce the risk of fraud...

- Back up your data each day.
- Avoid public Wi-Fi: Can you really be sure that you're not making yourself vulnerable to a fraudster sitting next to you in a coffee shop with a piece of technology in their bag setting up a fake site to harvest your data?
- Read the National Cyber Security Centre Small Charity Guide to Cyber-Security (which provides useful guidance for charities of all sizes).
- If you're going to write down your passwords then do it in a good old-fashioned notebook rather than online as this reduces the chances of your codes being cracked.
- Use the practical checklists from the Commission's recently-published surveys to prevent fraud and cyber-crime.

Helen Williams, a Cyber Protection Officer from North West Regional Ogranised Crime Unit (NWROCU), was next to speak. She revealed that the average age of a cyber-criminal is fourteen, news which was met with a collective intake of breath from a somewhat more mature audience.

The North West Regional Organised Crime Unit (NW ROCU) provides specialist capabilities to tackle serious and organised crime that crosses borders in the region. It is a collaboration between the six North West police forces in Cheshire, Cumbria, Greater Manchester, Lancashire, Merseyside and North Wales. The Unit has a dedicated cyber-crime team who work proactively and reactively on significant cyber-crime investigations with other national and international partners to identify and prosecute cyber criminals who are active or impacting upon the North West.

Echoing Mr Bryce's earlier comments, Ms Williams noted that the majority of cyber-crimes can be prevented by taking basic security measures and that, from an anti-fraud perspective, *less is more* when it comes to engagement with social media. LinkedIn is often used by social engineering fraudsters to impersonate and trick colleagues into giving away sensitive information. She advised that those who work for charities should keep any personal information listed on their social media profiles to a minimum in order to reduce the risk of this type of fraud.

Illustrating her point, she ran a short film by Cifas (the UK's leading fraud prevention service), called *Data to Go*, showing just how much personal information can be harvested in the amount of time it takes for a barista to take, make and deliver a coffee order. Click this link to watch the clip.

Ms. Williams then offered more valuable advice for preventing fraud...

- Only consider using public Wi-Fi if you can route usage through a virtual private network (VPN).
- Invest in your own mobile smartphone charger and avoid plugging into public charging points, as with the latter you can never be sure what you are tapping into.
- Check whether your email addresses have been subject to data breaches by using https://haveibeenpwned.com/

A Partner in our Charity sector team, Robert Nieri, was invited to close the conference, and he reiterated the message that charities need to develop a strong culture of fraud awareness.

It's advisable for charity trustees to set the tone that everyone follows, not only putting in place internal financial controls but implementing and monitoring them.

But every colleague has a part to play in preventing fraud and cyber-crime – a healthy degree of "*professional scepticism*" and the ability to challenge colleagues is called for here. It pays to implement a culture where every colleague, at every level, feels comfortable calling out concerns or suspicious behaviour, where appropriate by invoking whistleblowing procedures.

From a charity governance perspective there are a number of simple yet effective steps charities can take to make themselves more resilient to the threats of fraud and cyber-crime, including:

- Creating and implementing an anti-fraud policy.
- Devising a fraud action response plan which sets out appropriate measures to take in the event of a fraud being discovered.
- Taking advantage of free of charge fraud awareness guidance made available online, in particular by the Fraud Advisory Panel.
- Ensuring pre-recruitment checks are carried out on prospective trustees, staff and volunteers.

October, 2019

If you would like to discuss how your charity might want to review its governance to help protect itself from fraud and cyber-crime, then feel free to get in touch with Robert Nieri for a no-obligation, confidential chat.

Robert Nieri

Partner – Charity

Brabners LLP

Robert Nieri
Partner

T: 0161 836 8814 / +44 7767 673 219
E: robert.nieri@brabners.com

Brabners