It's Small Charity Week from 19th to 24th June 2017, which raises awareness of the work of smaller UK charities and some of the issues they face. One area of growing concern for smaller charities is fraud and cyber-crime especially given the high profile cyber-attack on the NHS in May.

The latest figures from The Office for National Statistics[i] show that cybercrime and fraud is on the rise. According to the Crime Survey for England and Wales there were 3.6 million incidences of fraud and 2 million computer misuse offences.

Charities are as vulnerable as businesses, and are increasingly targeted by cyber criminals because they often hold a lot of data about stakeholders and donors. Last year the Institute of Directors[ii] warned that businesses and charities were not taking cyber security seriously enough. They highlighted a 'worrying gap' between awareness of the risks and business preparedness.

Estimates of the scale of charity fraud vary hugely, but the most conservative estimates put it at hundreds of millions of pounds each year. Whilst charities cannot eliminate fraud, they need to understand the fraud risks they face, including the growing threat and risk of cyber-crime.

Smaller charities especially, who may not have as robust controls as larger organisations need to put measures in place to reduce the risk of cyber-crime and reduce their potential losses. So, what can charities do to prevent themselves being victims of cyber-crime?

Fraud and cyber-crime is made possible because of poor controls, however, it's usually how the controls are used in practice that is the issue. Charities need to think objectively about their risks and develop appropriate controls, as part of their overall risk policy.

The types of cyber-crime charities could fall victim to include hacking, phishing scams, ransomware and mandate fraud and charities need to identify all areas of weakness that could be exploited by online criminals.

To reduce risk, organisations should check their technology systems and ensure they have the most up-to-date firewalls and security systems installed. As the Charity Commission[iii] suggests, they should always install software updates as soon as they become available, as they will often include fixes for critical security vulnerabilities.

Regular data backups of important files, using an external hard drive, memory stick or online storage provider should also be made, ensuring no device is not left connected to prevent malware infections spreading. That way if an organisation were to experience an attack they will have retained most of their data.

Education is paramount in the fight against cyber-crime and the risk policy should include advice for employees about not clicking on emails or links they are unsure about. This is one of the main ways computer viruses or attacks happen, so making sure everyone understands this is essential.

There should also be a policy about employees using personal devices and connecting them to the internal network. With employees increasingly using smart phones and tablets in the workplace to access company data, this can compromise data security. This needs to be managed and perhaps restricted if it's considered too much of a risk.

When it comes to managing fraud, charities must ensure they verify all changes to key contacts and that important instructions, including changes to payments, bank details and addresses are made in writing and followed up by a phone call to the contact.

These are just some ways smaller charities can protect themselves and prevent themselves becoming a target of cyber-crime. While no charity can ensure they will be 100% safe, they can help mitigate the risks with a well-thought out risk policy that is fully ingrained in the workplace culture.

[i] http://www.bbc.co.uk/news/uk-38675683

[ii] http://www.charitydigitalnews.co.uk/2016/03/04/charities-need-to-get-real-about-cyber-security/

[iii] https://www.gov.uk/government/news/regulatory-alert-charities-at-risk-of-cyber-attack

Comments (0)