Month 10

Cyber Security – Threat or No Threat?

STEVE FRASER
—
Monahans

80%
of cyber-crime could be avoided if users were better trained.

A threat!

There is no doubt that cyber security is a threat to us all, whether small or large, profit making or not, a business or an individual. Unfortunately, charities can sometimes be seen as soft targets. A typical charity only spends 25% of what a similar sized business would spend on cyber security, despite the valuable data they hold.

While the growing threat of cyber-attacks might seem obvious, the need to protect ourselves against them is often overlooked or ignored. A successful cyber-attack can leave a charity open to blackmail and ransom demands and can result in financial losses and can damage reputation.

It is often the case that shortcuts are taken in protecting a charity against cyber-attacks due to cost restraints, and because the actual threat is under-estimated. However, some of the essential protections that can be put in place are neither expensive nor complicated.

The biggest risk?

It is often said that the biggest risk to an organisation is its own people. Certainly, it is estimated that 80% of cyber-crime could be avoided if users were better trained.

People are seen as a vulnerability that cyber attackers can seek to exploit. No matter what technology or security is in place, the major risk that will always remain is your individual users. It is essential that all of your users receive training covering cyber security and what the threats are so they are more aware of what to avoid and how to react to, for example, a suspicious e-mail.

So, how can you help your users to help you?

- Encourage users to lock their PC or laptop when it's unattended, and never leave them switched on at night.
- Make sure that any users out on the road are aware of the risks. It is staggering the number of people you can see on trains with confidential data on the screen in front of them!
- If an email looks suspicious, it probably is.
- If you receive requests for payments or the change of a bank account, don't react immediately. Take a step back and think about whether it's reasonable.
- Unfortunately, sooner or later a cyber-attack may be successful. If something happens, do your users fully understand the risk? Do they know how to react? Who to speak to? Are these processes part of your IT policies?

What are they after?

More often than not, the answer to that question is simple – your data. In the UK, it is estimated that charities hold data on three out of four people, data often of a financial, personal or medical nature. This data will be absolutely vital to their continuing operations, and its safety will be crucial to their reputation.

It is therefore essential that you understand where your data is. At first sight, this may sound a strange statement, surely it is saved safely on your server? However:

- How much data is used or saved to mobile devices?
- How often is data copied to a memory stick and used remotely on a lap-top?
- Are staff allowed to take data home to work on?
- Are there proper controls over the use, safety and deletion of this data?
- Is it properly protected and encrypted?
- Is shared data controlled in the same way?
- Are your processes fully understood and adhered to?

What else can you do?

There are some practical steps that can also be taken to help avoid damaging cyber-attacks.

- Charities cannot always afford the latest equipment and software, but it is still important that they have sound technical support available, either internally or through a third party resource.
- One of the vulnerabilities that a cyber-attack will seek to exploit is through your software, whether it is an operating system or an application. It is important that any software you use is kept up to date, with the latest version or update, and patches are in place. Try to avoid using out of date software, or software (particularly operating systems) which are no longer supported (for example, Windows XP) and are therefore no longer updated with the security patches. To ensure that your software is up to date, consider what automatic updates are available and how these might be applied, particularly to your operating systems.
- Have a think about how strong your access controls are. Who can access your systems? Who can access applications? Do they really need to access those applications? All these things should be considered and the appropriate protections put in place.
- I know that it can be a nuisance, but if you need to limit risk, then why let a user access a part of your system which has no bearing on their job?
- Whenever you can, make sure any passwords are “strong” passwords, whether it is for an encrypted device or to access a system or software. These passwords should, for example, include a range of characters from capitals to lower case, to numbers and special characters, such as exclamation marks. Also, make sure that procedures are in place to force password changes on a regular basis.

Checklist for the month

At the end of the day, trustees must recognise their responsibility to protect your organisations data, people, finances and reputation.

- Lead by example, from your board down.
- In compiling your risk register, has the risk of a cyber-attack and your reaction to it been fully considered?
- Review your systems, processes and procedures. Are they up to scratch?
- Are your users properly trained?
- Do you meet the essentials of cyber security?

Where can I get more information?

I appreciate that a lot of this sounds complicated, and maybe a little unnecessary. However, none of this needs to be complicated, a lot of it is just common sense and good practice, and is down to training and understanding the risk. Sadly, all of this and more is necessary if we’re to face the growing threat from cyber security, a threat which is predicted to increase significantly before it gets any better.

Try the governments simple self-assessment at

www.cyberaware.gov.uk/cyberessentials

If you have any questions arising from this article or would like to speak to a member of our team about how we can help. Please get in touch with your local MHA member firm.