Association Network

CYBER PROTECTION

Professional Guidance: IT 1
Original Publication Date: April 2019©

HOW SAFE IS YOUR ASSOCIATION?

THE SCALE OF THE PROBLEM

- Cyber attacks are a relatively new threat to associations but… they are real and a growing problem which is getting worse
- Don't think that it is only the corporate giants who are the chosen targets of the hackers; every business and association is exposed to some sort of indiscriminate or targeted attack
- In 2017 over 875,000 SMEs were affected by cyber attacks with costs incurred ranging from £10K to £2.5m
- It is a threat which cannot be ignored
- The average cost of a data breach is £36K and nearly 70% of businesses rate cyber security as a high priority
- However only 51% have taken action to identify cyber risks. Less than 30% have formal cyber security policies and only 10% have plans in place to deal with an attack
- After the USA, Britain is the most targeted country in the world with 1 in 10 businesses being targeted. Of these attacks 43% were aimed at small businesses including trade and professional associations

THE THREATS

The most common types of attacks are:

- **Spear Phishing** - apparently legitimate emails leading to a revelation of confidential information
- **Denial of Service** - blocking access to stored data
- **Trojans** - hidden malicious software which may seem legitimate
- **Ransomware** - blocked access to data until monies are handed over
- **Social Engineering** - tricking individuals into divulging confidential information

In 2018 the most common type of attacks were viruses, spyware and malware (68%) and impersonation of the organisation (32%). Despite the scale of these threats it is estimated that almost 70% of phishing emails are opened!

In addition to the professional hackers, your association may be vulnerable due to your suppliers having inadequate security, employee error or even a malicious employee.

Association Network

CYBER PROTECTION

Professional Guidance: IT 1
Original Publication Date: April 2019©

THE POTENTIAL IMPACT ON YOUR ASSOCIATION

- **Operational** – loss of service and IT failure
- **Intellectual Property** – Loss of confidential and commercial data
- **Financial** – loss of revenue and potential ransom payments
- **Regulatory** – legal sanctions and regulatory fines
- **Reputation** – Loss of confidence by members, partners and the general public which can take years to recoup

A TWO-WAY DEFENCE - WHAT ASSOCIATIONS CAN DO

Instigate a thorough review of current IT strategies

- Do you allow staff access to association IT systems for personal use?
- Draw up comprehensive defensive IT strategies and invest in staff training to increase awareness of the threats and the association's potential vulnerabilities
- Talk to your IT provider. Discuss any concerns about current systems and seek reassurance that your association is as protected as it can be. This is not a "one-off"; systems require regular review
- It may be worth partnering with another provider to see if they can hack into your systems. Take nothing for granted
- Many small associations do not have in-house IT experts and for them, it is even more important to invest in ensuring that protection is as comprehensive as possible

INSURANCE

Check your association's insurance policies. Is cyber security specifically included?

If not, then get cover as soon as possible. Many insurance companies now offer bespoke insurance products and it is money well spent investing in cover for your association. Make sure that your broker is fully aware of the scale and nature of your association and the potential threats to it.

A good cyber security insurance policy will:

- Provide a rapid 24/7 response if you are attacked to minimise the effects
- Identify, contain and restore your systems as quickly as possible
- Deploy legal and PR teams to minimise the damage as far as possible
- Liaise with media and partner organisations who may have been compromised by the attack

CYBER PROTECTION

Professional Guidance: IT 1
Original Publication Date: April 2019©

- *Assist with investigations instigated by the regulators*
- *Compensate your association for loss and costs arising from the breach of commercial and personal information*
- *Cover loss of revenue due to business interruption and/or cyber extortion*

SUMMARY

Cyber security is a growing problem for organisations and it cannot be ignored; to do so is a dereliction of duty by the governing body which could result in heavy financial penalties. Be aware of the threats and consequences of a cyber attack to your association. Thoroughly review your in-house policies and liaise with your IT support providers to ensure that you are as protected as possible. Keep systems and browsers patched. Back up your data to more than one source, one of which should be off site or cloud based. Test your backups regularly.

A good source of more in depth advice is available via www.cyberessentials.ncsc.gov.uk

Review your existing insurance and, if it is inadequate, invest in comprehensive insurance cover which takes account of your association's own vulnerabilities in the event of an attack.

For more advice and where to find further information, please contact:

Richard Frost, Director, Association Support
www.associationsupport.co.uk