MOORE ClearComm

ESSENTIAL CYBER DEFENCES FOR CHARITIES

Confidentiality of information in charities has always been of paramount importance. A breach affecting records of its data which could involve donors, children, ethnic and religious categories is typically very serious and would invite increased regulatory and public scrutiny with potential severe financial penalties.

The security threat from the simple use of e-mail and the web is very real, with phishing and ransomware attacks commonplace in today's internet-connected world. Successful cyberattacks range from the theft of sensitive information to long-term disruption to the operation of IT systems.

Maintaining a minimum level of cyber compliance across your charity's IT infrastructure is therefore absolutely key to not falling victim to a cyberattack. As technology constantly evolves becoming more ingrained into daily life, it is often difficult to know what this minimum level looks like in practice. The technical capabilities to strengthen cyber security defences is not always internally available within the charity.

For trustees, it can be challenging to determine whether the charity's infrastructure is adequately protected against the possible threat of a cyber-attack.

This issue facing the sector across the country led to the UK Government introducing the Cyber Essentials scheme. The scheme is designed to protect charities against 80% of the most common cyber-attacks which can impact charities of all sizes.

The five controls within the Cyber Essentials scheme are designed to protect your charity against these types of cyber-attacks and guard your internet connection, devices, data and services.

Basic Level Cyber Essentials certification is self-assessment and provides a basic level of assurance that the controls have been implemented correctly by the organisation.

Cyber Essentials Plus covers the same requirements but also includes an on-site audit and therefore provides the independent assurance of the effectiveness of these controls.

.

NOVEMBER

SPECIAL OFFER - NON PROFIT ONLY

£225

NORMALLY: £300

Sign up before 12th November 2021

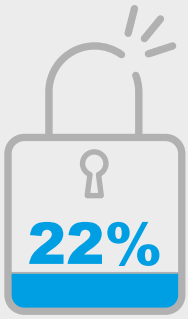
TO CLAIM THIS OFFER EMAIL:

info@mooreclear.com

CYBER ESSENTIALS

- Online self-assessment process
- Fast assessment
- Supported programme available
- Electronic certificate and report

EXPERIENCE OF BREACHES OR ATTACKS



of charities identified cyber security breaches or attacks in the last 12 months

£9,470

is the average annual cost for charities that lost data or assets after breaches

Among the 22% identifying breaches or attacks:

29%

needed new measures to prevent future attacks

32%

took up staff time dealing with breaches or attacks

21%

had staff stopped from carrying out daily work

39%

identified at least one breach or attack a month

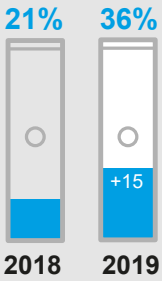
GDPR AND CYBER SECURITY

36%

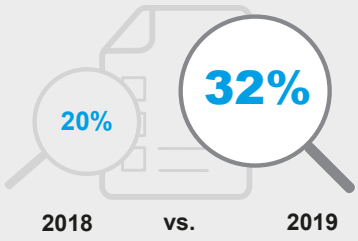
have made changes to cyber security because of GDPR

Among the 36%:

- **60%** created new policies
- **17%** had extra staff training or communications
- **4%** changed firewall or system configurations
- **10%** created new contingency plans



have cyber security policies in place.



have done a cyber risk assessment in the last 12 months

*Source: Information and infographics from Cyber Security Breaches Survey 2019 carried out by the Department for Digital, Culture, Media & Sport.
Ipsos MORI carried out telephone survey to 514 charities.

CONTACT US Call: +44 (0) 20 7566 4000 or email: info@mooreclear.com

MOORE ClearComm

www.mooreclear.com