BUSINESS IN THE COMMUNITY

The Prince's Responsible Business Network

HRH THE PRINCE OF WALES ROYAL FOUNDING PATRON

Headline Findings

WOULD YOU BE READY FOR A CYBER ATTACK?

December 2018

YouGov® What the world thinks

BUSINESS IN THE COMMUNITY

The Prince's Responsible Business Network

WOULD YOU BE READY FOR A CYBER ATTACK? HEADLINE FINDINGS

Overview of the results from a baseline survey conducted by YouGov in November 2018 on behalf of Business in the Community to understand the barriers to small and medium-sized businesses implementing adequate cyber security measures.

Introduction

I am delighted to present these initial findings on small and medium-sized businesses'* current cyber security awareness and implementation. The findings provide critical insight into where we can support smaller businesses to be safer online and ensure that businesses stay in business. According to the Cyber Security Breaches Survey 2018 (DCMS), the average cost of a breach to a small business is £894 and for a medium-sized business it rises to £8,180. We are committed to finding easy-to-implement and cost-effective solutions that reduce the likelihood of data breaches and cyber-attacks and increase online security, in order for smaller businesses to get back up and running should the worst occur. Thank you to those businesses who completed the survey. I look forward to presenting the full report to you in the new year.

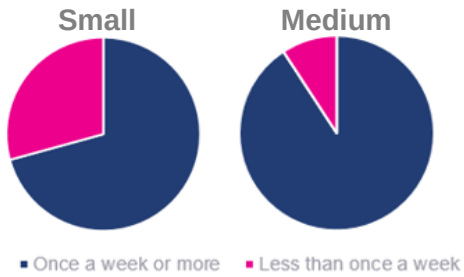
Yours faithfully,

Daniel Lawrence

(Chair of the Cyber Resilience Sub-Group, a part of the Business Emergency Resilience Group at Business in the Community & General Manager of Threat Intelligence & Investigations at BT)

*Where the results of small (50 employees or fewer) and medium-sized (50 to 249 employees) businesses are combined, they are referred to together as smaller businesses.

Back-up of Essential Data



82% of medium-sized businesses back up essential data at least once a week, compared to 65% of small businesses. Of these, 62% of medium-sized businesses and 46% of small businesses back up essential data every day. 10% of small businesses never back up essential data, in comparison to 1% of medium-sized businesses.

Updating anti-virus software, anti-malware software and firewalls

68%

of smaller businesses automatically update anti-virus software when a new update/patch is released.

Most smaller businesses update their essential anti-virus software, anti-malware software and firewalls automatically. Less than 17% of smaller businesses do not know when they update each of these programs or do not use them at all.

HRH THE PRINCE OF WALES ROYAL FOUNDING PATRON

BUSINESS IN THE COMMUNITY

The Prince's Responsible Business Network

Existing cyber security measures

30%

of small businesses do not have any cyber security strategies in place, compared to 4% of medium-sized businesses.

In the last 12 months, 40% of small businesses have not undertaken any cyber security action (policies, insurance, staff training etc.), compared to 8% of medium-sized businesses. Only 27% of all smaller businesses have introduced compulsory strong passwords and a password management policy; 25% have reviewed user accounts to make sure users can only access files that they have permission to; 22% have identified, documented and fixed hardware and software vulnerabilities; 20% have reviewed third-party providers' security capabilities (e.g. providers of anti-virus software).

35%

of smaller businesses have a basic data protection policy.

27%

of smaller businesses have invested in strong passwords and a password management policy in the last 12 months.

Reasons for investing in cyber security

Two-thirds (66%) of smaller businesses have taken at least one cyber security action. The main drivers for these actions were:

- Introduction of General Data Protection Regulation or other industry compliance standards (44% of those who have taken action)
- Hearing about cyber security in the media (24% of those who have taken action)

Investing in employee cyber security training

85% of all smaller businesses have not invested in cyber security training for employees in the last 12 months. 58% of all smaller businesses do not know why they have not invested in employee cyber security training, thought it is not necessary or have no reason.

26%

of smaller businesses do not think it is necessary to invest in employee cyber security training and the same for cyber insurance.

Investing in cyber insurance

Only 6% of smaller businesses have invested in cyber insurance in the last 12 months. 63% of smaller businesses said they do not know why they have not invested in cyber insurance, they believe it is not necessary or have no reason.

What can you do to protect yourself?

The full report will have more recommendations on how to protect your business. In the meantime, we highly recommend checking-out the National Cyber Security Centre's Cyber Essentials and implementing their five steps:

1. Use a firewall to secure your Internet connection
2. Choose the most secure settings for your devices and software
3. Control who has access to your data and services
4. Protect yourself from viruses and other malware
5. Keep your devices and software up to date.

All figures, unless otherwise stated, are from YouGov Plc. Total sample size was 1,003 adults. Fieldwork was undertaken between 12th - 20th November 2018. The survey was carried out online. The figures have been weighted and are representative of British business size.

HRH THE PRINCE OF WALES ROYAL FOUNDING PATRON

BUSINESS IN THE COMMUNITY

The Prince's Responsible Business Network

Hannah Tankard
Programme Manager
The Prince's Business Emergency Resilience Group

Business in the Community
137 Shepherdess Walk
London N1 7RQ

www.bitc.org.uk

HRH THE PRINCE OF WALES
ROYAL FOUNDING PATRON