BUSINESS IN THE COMMUNITY
The Prince's Responsible Business Network

HRH THE PRINCE OF WALES
ROYAL FOUNDING PATRON

Full Report

WOULD YOU BE READY FOR A CYBER ATTACK?

March 2019

YouGov®
What the world thinks

WOULD YOU BE READY FOR A CYBER ATTACK? FULL REPORT

TABLE OF CONTENTS

WOULD YOU BE READY FOR CYBER ATTACK?

FOREWORD

Business in the Community is delighted to present this report, which confirms where we all can play a role in better online security and how we – business leaders, think tanks, government – can achieve this. We encourage CEOs and business owners of all sizes to take actions after reading this report. If you are a small business owner, we hope it inspires you to implement the recommendations to be safer online. For larger businesses, we hope you will consider joining our call to action. By working together, we will be a step closer to achieving the National Cyber Security Centre's vision to help: "make the UK the safest place to live and do business online".

Business owners have a lot of responsibility besides the all-important day job. There are additional extras, some compulsory, some nice to have, like getting tax returns in, passing health and safety checks, understanding data protection guidelines and colleague engagement. Unfortunately, we also know that a disruption of any form could put many small businesses out of business. According to the Cyber Security Breaches Survey 2018[i], the average cost of a cyber breach to a small business is £894 and for a medium-sized business it rises to £8,180. Other reports, such as one commissioned by Barclays[ii] suggest that this figure could be much higher. With costs like this, a cyber breach could spell the end for a business.

This report was commissioned by business leaders wanting to understand current cyber security practices of small and medium-sized business. The results show we can all play a role to help improve the cyber security and resilience of small and medium-sized businesses. We can help your business to be safer online, to protect invaluable customer and supplier data, to save costs, and to prevent heartache. We thank those businesses who took part in the survey for giving us this valuable insight. Business in the Community is committed to finding easy-to-implement and cost-effective solutions that reduce the likelihood of data breaches and cyber attacks and increase online security, so that businesses can get quickly back up and running should the worst occur.

> **By working together, we will be a step closer to achieving the National Cyber Security Centre's vision to help: "make the UK the safest place to live and do business online."**

Danny Lawrence (Chair of the Cyber Resilience Sub-Group, Business Emergency Resilience Group, Business in the Community).

Mike Still (Chair of the Business Emergency Resilience Group, Chair of Scotland Advisory Board and Trustee, Business in the Community).

Hannah Tankard (Programme Manager – Response & Recovery, Business in the Community).

[i] Department for Digital, Culture, Media and Sport. 2018. Cyber Security Breaches Survey: Statistical Release. London.
[ii] Barclays. 2018. Barclays launches major drive to help SMEs tackle cybercrime.

The results of our research show variations between the cyber security levels of different sized businesses, business sectors and sometimes regions too. Across different cyber security and resilience areas, small and medium-sized businesses have demonstrated where they have or have not been investing time, money or human resources into their own cyber security.

What is striking is the evidence that size does matter: small businesses are not investing as much time or money into their own cyber security as medium-sized businesses. From a supply chain perspective this is concerning: previously reported cyber attacks, such as that experienced by Ticketmaster[i], have shown that smaller, third-party suppliers have sometimes been the cause for cyber attacks at larger organisations. Moreover, we know that small and medium-sized businesses have fewer resources in place to deal with cyber attacks. Should a breach occur it could spell the end of a small or medium-sized business' ability to do business.

There are some differences between sectors. Service industries, such as the IT and telecoms and legal sectors, are more likely to have invested in cyber security measures than, for example, the construction and transportation and distribution sectors. Addressing the cyber security of weaker sectors would enable entire supply chains across the country to be more resilient.

The regional data also shows some disparities across several of the survey questions. Of note is that businesses in Wales stand-out as reporting having fewer cyber security measures in place and being less likely to update anti-virus, anti-malware and firewall software than other regions. Given that geographical boundaries do not affect the online space, it is vital that every region of the United Kingdom has good cyber security.

Business in the Community strongly believes that everyone needs to take action to reduce the likelihood of cyber breaches happening to small and medium-sized businesses, as well as having measures in place to reduce the impact should a breach occur.

As shown in our recommendations and top tips, small and medium-sized businesses can take steps today to mitigate cyber risks; simultaneously we also believe that larger businesses, with the resources available to them, can better support their supply chain and small and medium business customers. We are seeking everyone's support in helping the United Kingdom to be as secure online as possible.

[i] Friday R. 2018. The Ticketmaster hack is a perfect storm of bad IT and bad comms. Wired.

COULD ALL YOUR HARD WORK BE HACKED DOWN TOMORROW?

INTRODUCTION

Cyber attacks may not be on the top of your priority list. However, cyber-related incidents are more common than you think. We may think large businesses have all the requisite controls necessary to deal with a cyber disruption, yet businesses of all sizes are at risk. Moreover, small businesses do not always realise they can be the gateway to big businesses' data loss; a breach in a supply chain or the loss of customers' data could spell the end for many small businesses.

Big businesses, even those previously affected by cyber attacks, such as TalkTalk, Dixons Carphone, Ticketmaster UK and British Airways, have the people, resources and financial robustness in place to deal with breaches. Would your small business have the capacity to deal with a cyber breach? What could your company do now to prevent yourselves being affected by a phishing attack? (If you are not sure what a phishing attack is, see the glossary at the end of the report.) How are you ensuring that your business complies with the General Data Protection Regulations (GDPR)?

Business in the Community (BITC) commissioned a YouGov survey to understand the current cyber security practices of small and medium-sized businesses across a variety of areas. This report has several purposes: firstly, it is a chance to present the findings and provide an insight into where small and medium-sized businesses are investing their resources in terms of cyber security. We show overall results and then how these are broken down by business size, by sector and by location. We have also taken the opportunity to share existing easy-to-implement advice and tips through-out the report on recommended cyber resilience measures.

Secondly, the report will inform the work of the Cyber Resilience Sub-Group, as part of The Prince's Business Emergency Resilience Group (BERG) campaign at BITC. These findings will allow the group to focus on developing appropriate cyber security products and services for small and medium-sized businesses that will be user-friendly and cost-effective. This aligns with BERG's vision to help businesses to be prepared for, respond to and recover from crises, including cyber incidents. Additionally, it aligns with BITC's vision that a responsible business is a successful business.

Last but by no means least, we have a call to action whereby we are asking larger businesses to better support their small business customers and supply chains to implement cyber security measures. Afterall, we know that larger businesses will be better protected themselves if their supply chain is cyber secure.

KEY FINDINGS

CURRENT CYBER SECURITY STRATEGIES

Ideally all businesses would have the most common recommended measures in place. These include using a firewall to secure internet connections and limiting the number of users with administrative privileges. It also means keeping administrative activities separate from standard accounts. Other recommended measures include implementing a data protection policy and having a response and recovery plan in case a cyber breach should occur. Despite these recommendations, our survey found that many small and medium-sized businesses do not have many, if any, measures in place. For example, even with GDPR being implemented in May 2018, **only 35% of small and medium-sized businesses have a basic data protection policy;** only 29% have a policy for controlling access to systems. Of great concern is that 25% of small and medium-sized businesses do not have any cyber security strategies.

BY SIZE

When broken down by size, the differences between cyber security measures in place between small and medium-sized businesses are quite distinct. For example, **30% of small businesses do not have any cyber security strategies in place, compared to just 4% of medium-sized businesses.**

Across the options of cyber security strategies listed in the survey and presented on the graph on the next page, medium-sized businesses are more likely to have measures in place than small businesses. The most noticeable difference was that over 50% of medium-sized businesses have a policy for controlling access to systems that are limited to certain employees, compared to only 23% of small businesses. Other areas where there were large differences include: data breach notification, incident response, and an internal and external communications process should a cyber-attack occur; someone responsible for cyber security; and an up-to-date cyber security policy, signed off by a senior member of staff (i.e. a formal policy for responding to a cyber security breach).

BY SECTOR

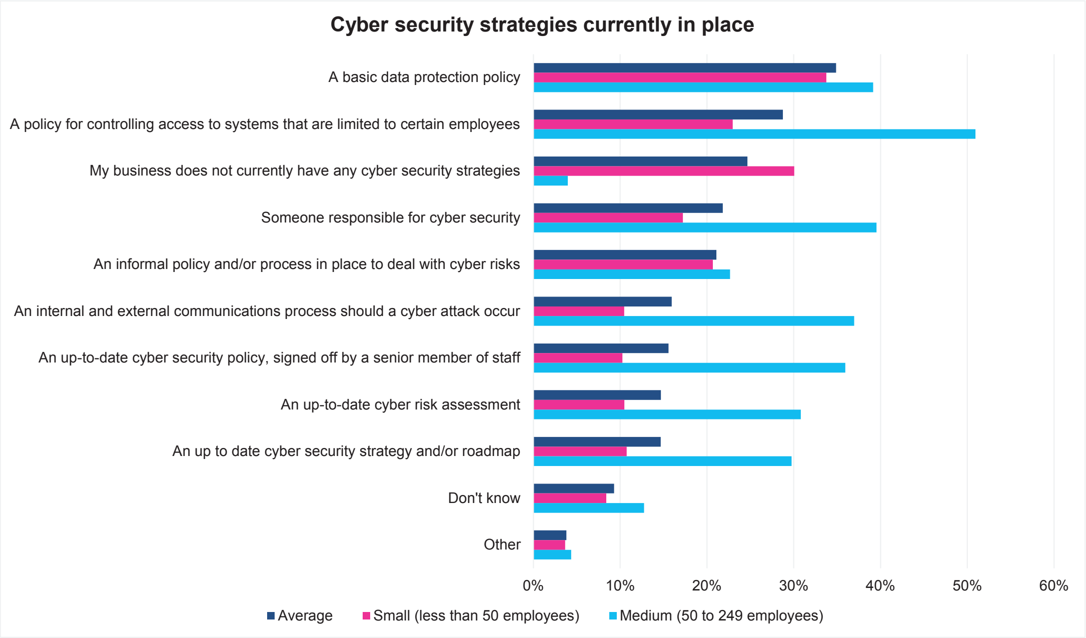
The following indicates overarching trends for cyber security measures that small and medium-sized businesses have in place by sector. The sectors highlighted were the best and worst for number of cyber security measures in place.

- The legal* and IT and telecoms sectors have the most measures in place with only 8% of both sectors indicating they have no measures.
- Retail (43%), construction (39%), and real estate* (36%) have the fewest cyber security measures in place.
- Of note was that the transportation and distribution* sector was the least likely sector to know what, if any, cyber security measures were in place (34%).

BY LOCATION

The following indicates overarching trends for cyber security measures that small and medium-sized businesses have in place by region. The regions listed are the best and worst regions for number of cyber security measures.

- 18% of business in London and 20% of businesses in both the East of England and East Midlands indicated they have no cyber security measures in place.
- In contrast, 40% of businesses in Wales* and 32% of businesses in the North East* indicated that they have no measures in place.



TOP TIPS

We highly recommend adopting the following five key simple steps, listed as the NCSC's minimum number of things a business should do to be more cyber resilient:

1 Use a firewall to secure your Internet connection – most devices have built in firewalls

2 Choose the most secure settings for your devices and software

3 Control who has access to your data and services – using passwords and specific user accounts

4 Protect yourself from viruses and other malware – using anti-virus software and staff training

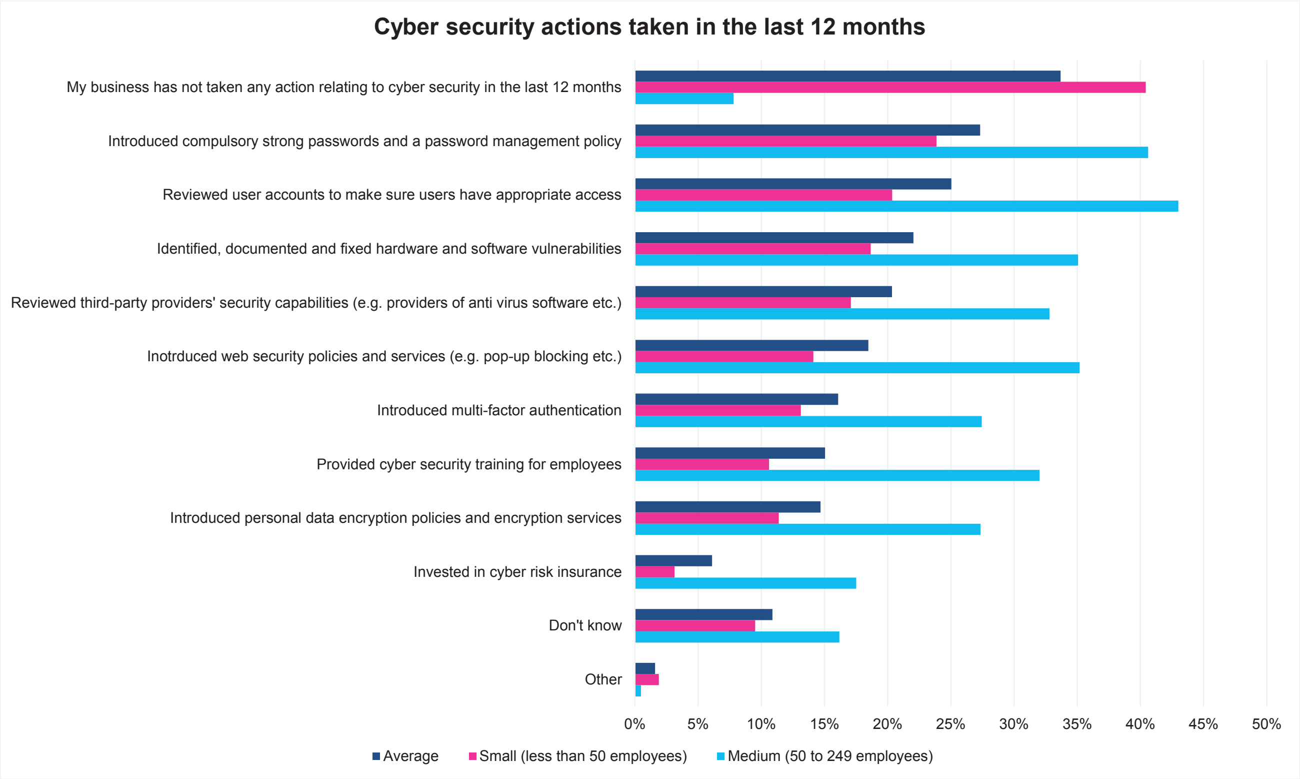
5 Keep your devices and software up to date – using auto-update mechanisms

CYBER SECURITY ACTIONS TAKEN IN THE LAST 12 MONTHS

Once a business has cyber security measures in place, it is important they are kept up-to-date, from reviewing policies to updating software and training employees. From the survey, however, we know that this is likely to not always be a priority for smaller businesses. For example, 34% of small and medium-sized businesses indicated not taking any cyber security actions in the last 12 months and 11% did not know if they have taken any actions. Of the actions that were taken in the last 12 months, the most common were: introduction of compulsory strong passwords and a password management policy (27%); review of user accounts to make sure users have appropriate access (25%); identifying, documenting and fixing hardware and software vulnerabilities (22%); and reviewing third-party providers' security capabilities (e.g. providers of anti-virus software) (20%).

BY SIZE

There is a difference in terms of actions taken by small and medium-sized business. For example, in the last 12 months **40% of small businesses have not undertaken any cyber security action** (policies, insurance, staff training etc.), compared to only 8% of medium-sized businesses. Across all the cyber security measures listed, except for 'other', medium-sized businesses were more likely to have implemented measures than small businesses.


Cyber security actions taken in the last 12 months

BY SECTOR

The individual cyber security measures taken vary by different sectors and are too numerous to list individually. Here we indicate the best and worst performing sectors with respect to cyber security strategies implemented in the last 12 months.

- The legal* and IT and telecoms sectors were the most likely sectors to have implemented measures, with only 18% of both indicating having taken no actions.
- **The retail (49%), hospitality and leisure (45%) and construction (43%) sectors were least likely to have taken any cyber security measures in the last 12 months.**

BY LOCATION

The individual cyber security measures taken by region varies too much to list individually. Here we indicate the best and worst performing regions with respect to cyber security strategies implemented in the last 12 months.

- London (25%), East Midlands (25%) and the North East* (26%) were the regions most likely to have implemented cyber security actions in the last 12 months.
- The South West (44%), Yorkshire and the Humber (43%) and Wales* (43%) were the regions least likely to have taken any cyber security actions in the last 12 months.

TOP TIPS

The NCSC advises that all businesses should have an overall security policy that includes cyber security and resilience. To ensure compliance with your policies across your organisation it is advisable to have mandatory and regular training for all employees that explains the latest and best practices for being safe online. This will ensure cyber security and resilience is embedded as part of the culture of the workplace and will reinforce that everyone has a role to play.

REASONS FOR INVESTING IN CYBER SECURITY

Of those businesses who have taken action in the 12 months preceeding November 2018, the reasons for implementing cyber security actions are varied. The most common reason by a large margin (44%) was the introduction of GDPR. **The other main reasons were: hearing about cyber security in the news (24%); a contractual agreement with supplier(s) or contractor(s) (15%); on advice from a professional organisation (14%); and knowing another person/organisation that has been negatively affected by a cyber security breach (14%).**

TOP TIPS

Being aware of current advice is critical to keeping a business as secure as possible online. Follow organisations like the NCSC on social media channels such as Twitter for up-to-date alerts on current cyber threats. It is also worth considering how much you spend on assets for employees: for example, what do you currently spend on mobile phone contracts?
How does this compare to how much you spend on employee security and resilience?

BY SIZE

There are no major differences behind the reasons why a small or medium-sized business may have taken cyber security actions in the last 12 months. The greatest difference was that medium-sized businesses are more likely to have been advised by a professional organisation (21%) than a small business (11%) to take actions. The second greatest variation was that medium-sized businesses were more likely to have (knowingly) experienced a previous cyber security breach (16%) than small businesses (7%).

BY SECTOR

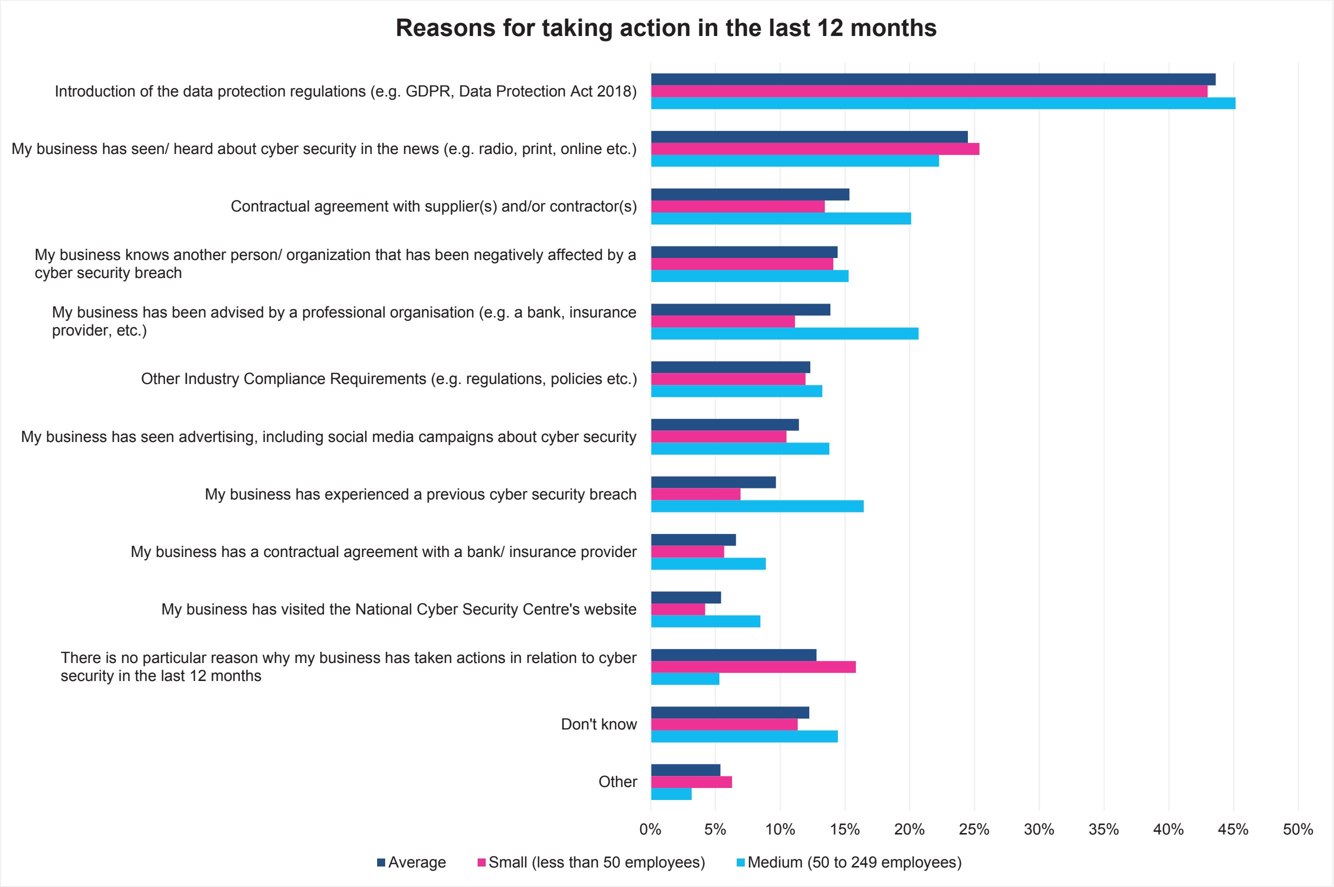
Of the two reasons that particularly influenced decision making in the last 12 months by sector:

- The legal* (36%) and medical and health services* (37%) sectors were more likely to have taken action because they had seen and heard about cyber security in the news. The least likely were finance and accounting (16%).
- The legal* (70%) and medical and health services* (68%) sectors were more likely to have implemented cyber security measures due to the introduction of GDPR. This contrasts with construction (16%) and education* (34%) sectors.

BY LOCATION

Of the reasons for implementing cyber security actions in the last 12 months by region:

- Those businesses in the North East* (54%) and East Midlands* (53%) were more likely to due to the GDPR. This compares to businesses in Wales* (22%) being least likely due to GDPR.
- Businesses in the North East* (31%), East of England* (29%) and South West (29%) were more likely to have seen and heard about cyber security in the news. This compares to the least likely areas being the North West (20%), South East (21%) and Scotland* (21%).
- Businesses in the North East* (19%) were most likely to have seen social media campaigns; the least likely region was the South West (5%).
- Those in Scotland* (19%), London (16%), West Midlands (12%) and the North East* (12%) were most likely to have implemented actions due to previous cyber breach experience; this compared to only 2% of businesses experiencing cyber breaches in East Midlands* and none in Wales*.
- 20% of businesses in London had received advice from a professional organisation, which contrasts to 9% in the South West.
- Businesses in the North East* (15%) were more likely to have a contractual agreement with a service provider; this compares to none in East of England and South West areas of England.



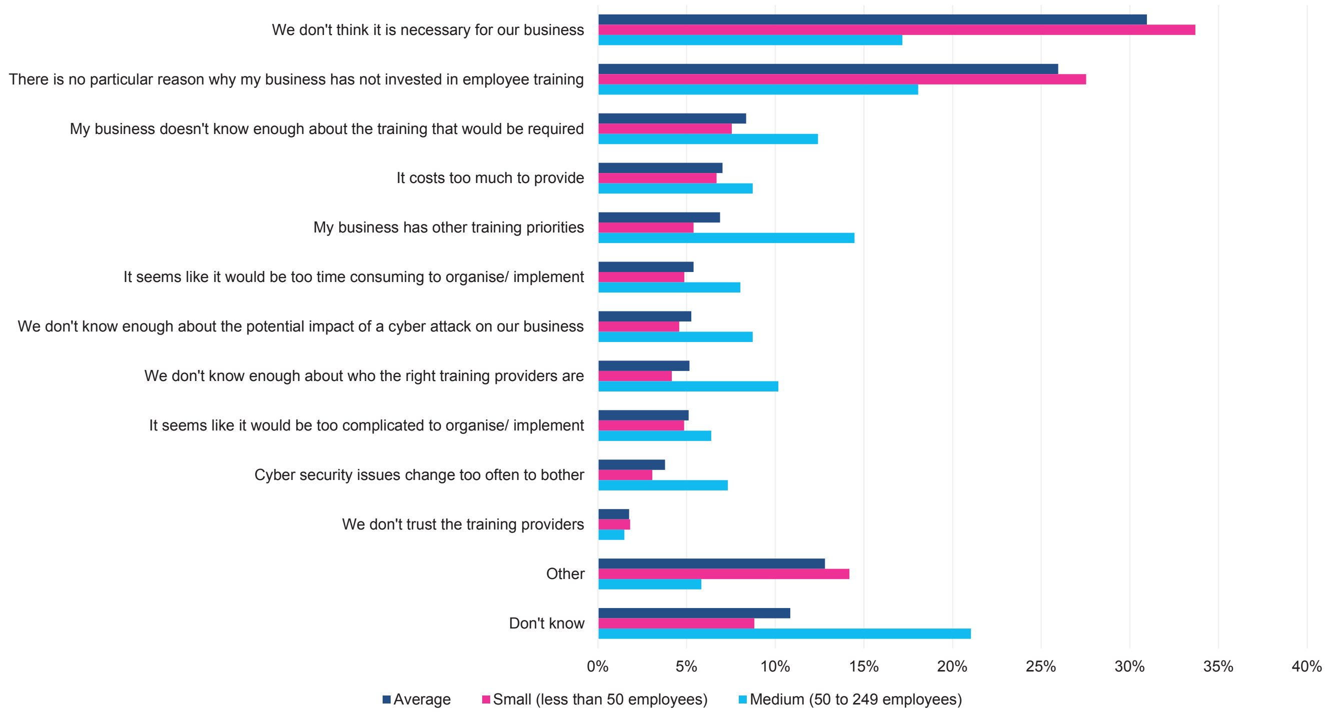
CYBER SECURITY TRAINING FOR EMPLOYEES

Cyber security and resilience is not just the IT team's responsibility. Every employee has a role in maintaining the security of company information, both online and offline. Employees are still a major reason why businesses are affected by cyber breaches, often falling prey to simple hacking techniques such as phishing and scams. Of those businesses who have not provided cyber security training for employees in the last 12 months, the main reasons for not providing training are that small and medium-sized businesses think it is not necessary for their business (31%) or have no particular reason (26%).

BY SIZE

When this is broken down by size, **small businesses were more likely to think it is not necessary (34%) or have no particular reason (28%)** compared to medium-sized businesses (17% and 18% respectively). However, medium-sized businesses were more likely to not know why they have not invested in cyber security training for employees: 21% compared to 9%. Medium-sized businesses were also more likely to have not invested in employee cyber security training due to: not knowing enough about the trainings that would be required (12%); having other training priorities (14%); thinking it is too difficult to implement (8%); not knowing who the right training providers are (10%); believing that cyber security issues change too often to bother (7%); indicating that it costs too much to provide (9%); and not knowing about the impact of a cyber-attack on their business (9%).

Reasons for not investing in employee cyber security training



BY SECTOR

The following are the main reasons why different sectors have not invested in employee cyber security training. This list does not include all sectors.

- **The retail (46%), hospitality and leisure (40%), education* (33%) sectors were most likely to think it is not necessary.**
- The construction (36%), finance and accounting (33%) and real estate* (41%) sectors were most likely to have no particular reason for not investing in cyber security.
- The transportation and distribution* (29%) sector was most likely to not know why they have not invested in cyber security.
- The transportation and distribution* (13%) and real estate* (14%) sectors were most likely to think that it would be too complicated to provide.
- The medical and health services* (24%) sector were most likely to have other reasons for not implementing cyber security.

BY LOCATION

Of the two main reasons for not investing in cyber security for employees by region:

- Yorkshire and the Humber* (41%), West Midlands (40%) and South West (37%) regions were most likely to think that cyber security training for employees is not necessary for their business.
- Small and medium-sized businesses in London (30%) were most likely to say there is no particular reason why they have not invested in cyber security training, followed by East Midlands* (28%), South West (27%) and North West (27%).

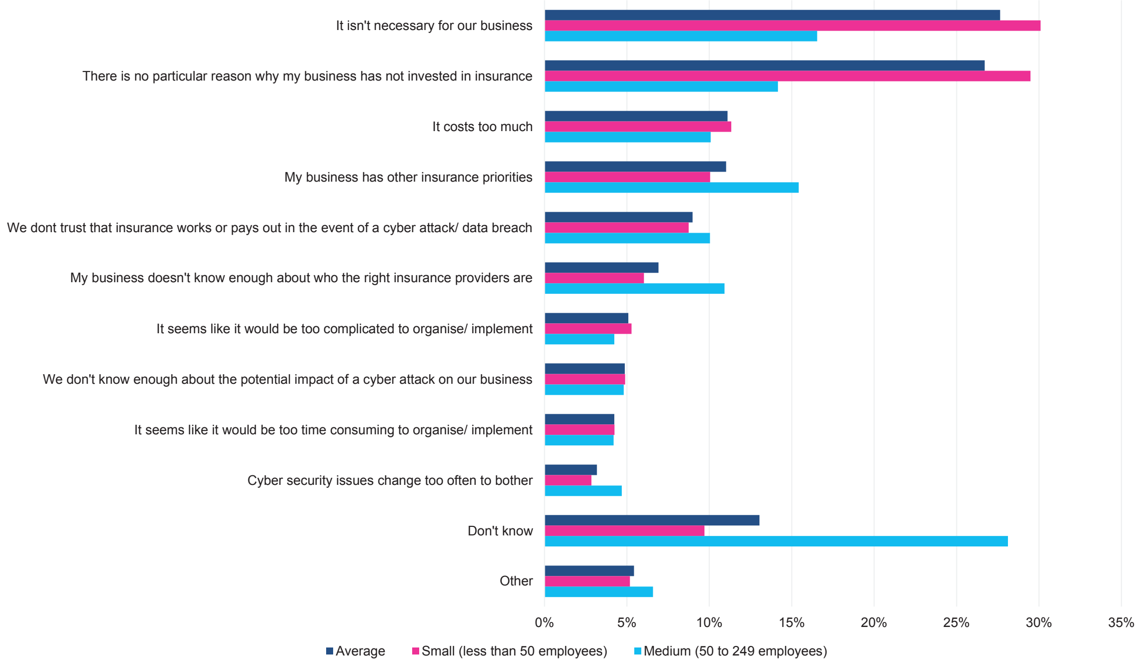
TOP TIPS

It is critical for all businesses to have the right training in place so that employees know how to be safe online, what to look for to prevent an attack and the immediate steps to follow should an attack occur. As with a business' cyber security policy, staff training needs to be regular, frequent and personable, preferably embedded as part of a business' values and not treated as an add-on. As a starting point, the NCSC has staff awareness and training guidance, and Barclays Digital Eagles, as an example, have free resources.

INVESTMENT IN CYBER INSURANCE

Even when you have cyber insurance in place, your business should still exercise good cyber practices. Cyber insurance can, however, give your business a safety net should a cyber incident occur. Of those businesses who have not invested in cyber insurance in the last 12 months, **the main reasons were either thinking that it is not necessary (28%) or having no particular reason (27%)**. Other reasons for not investing in insurance were: don't know (13%); it costs too much (11%); and business has other insurance priorities (11%).

Reasons for not investing in cyber insurance



BY SIZE

When this is broken down by a business size, 29% of small businesses were more likely to have no particular reason for investing in cyber insurance in the last 12 months compared to 14% of medium-sized businesses. Small businesses were also more likely to believe that it is not necessary for their business (30% compared to 17% of medium-sized businesses).

BY SECTOR

The following are the main reasons why different sectors have not invested in cyber security insurance in the last 12 months:

- **Retail (36%), hospitality and leisure (36%), education* (36%) and construction (34%) were most likely to believe that it is not necessary.**
- Finance and accounting (37%), construction (34%), medical and health services* (33%) and real estate* (32%) were most likely to have no particular reason for not investing in cyber security.

- Medical and health services* (25%) noticeably stand out as most likely to have other insurance priorities.
- IT and telecoms (24%) and legal* (17%) sectors were most likely to not trust that insurers will pay out in the event of an attack.
- Transportation and distribution* (34%) and media, marketing, advertising, PR & sales (22%) were most likely to not know why they have not invested in cyber security.

BY LOCATION

The following are the main reasons why businesses in different regions have not invested in cyber security insurance in the last 12 months:

- Businesses in Scotland* (40%), Yorkshire and Humber* (33%) and South West (32%) were most likely to believe that cyber insurance is not necessary.
- Businesses in Wales* (37%), Yorkshire and Humber* (34%), West Midlands (29%) and South West (29%) were most likely to have no particular reason for not investing in cyber insurance.
- 21% of businesses in the North East* were most likely to not trust that insurance works or pays out in the event of a cyber-attack claim.
- Businesses in London (19%) and East Midlands* (18%) were most likely to not know why they have not invested in cyber security.

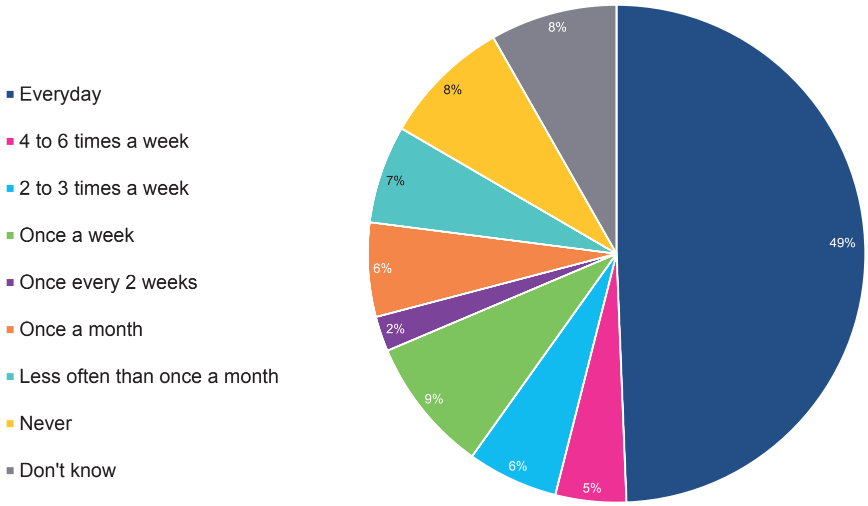
TOP TIPS

The Association for British Insurers (ABI) suggest that cyber insurance could help your business cover the cost of business interruption from a cyber attack from such things as loss of customer data, as well as repairing or replacing damaged equipment. Cyber insurance gives you access to specialists who can at short notice help to stop an attack and get back to business quickly. Insurance could also help with managing your company's reputation should a breach occur and paying any fines associated with a breach.

BACK-UP FREQUENCY OF ESSENTIAL DATA

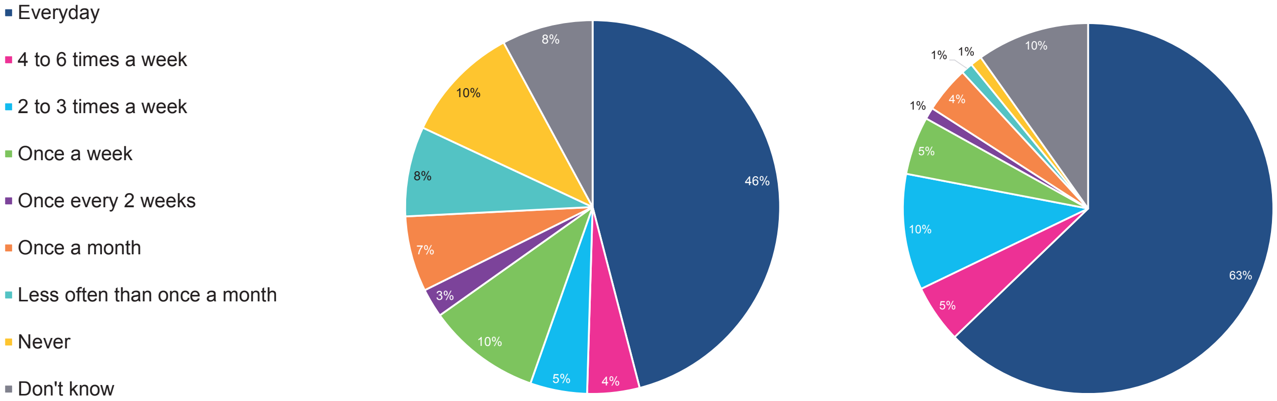
Losing your latest data and documents could be extremely disruptive for your business. The results showed that most small and medium-sized businesses are aware of this and are backing-up essential data: 49% of small and medium-sized businesses back-up data daily and 19% once a week or more. On the other hand, 8% of small and medium-sized businesses never back-up data and the same number do not know when, or if they back-up their essential data.

Back-up frequency for small and medium-sized businesses



BY SIZE

82% of medium-sized businesses reported backing 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.

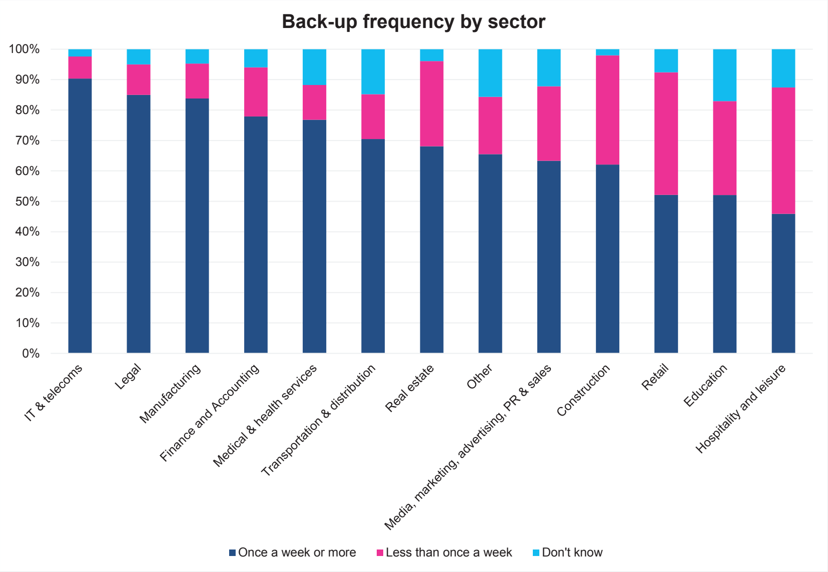

Back-up frequency for small businesses

Back-up frequency for medium businesses

BY SECTOR

IT and telecoms (90%), legal* (85%) and manufacturing (84%) sectors were more likely to back-up essential data more than once a week.

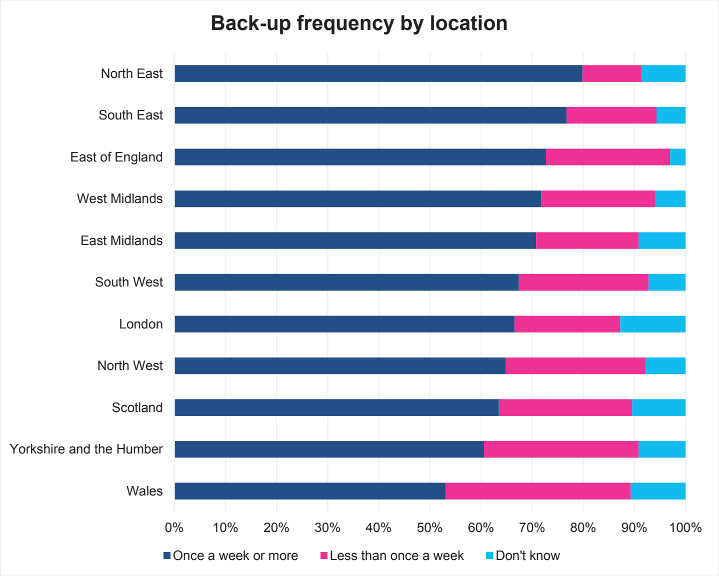
The hospitality and leisure (46%), retail (52%) and education* (52%) sectors were least likely to back-up essential data once a week.



BY LOCATION

The North East* (80%), South East (77%) and East of England (73%) were the most likely regions to back-up essential data once a week or more.

Wales* (53%), Yorkshire and the Humber (61%) and Scotland (63%) reported backing up essential data least frequently.

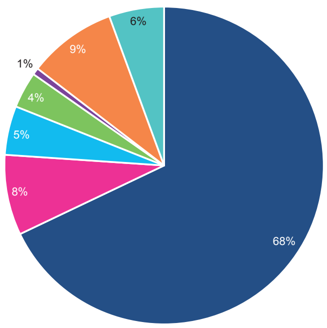


TOP TIP

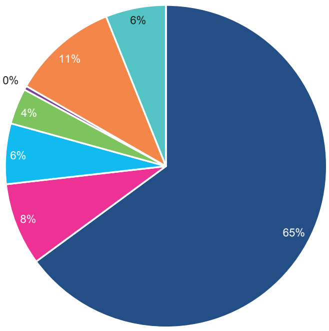
The NCSC advises automatically backing-up data. Ideally this would be done in more than one place (e.g. using a cloud provider) so that you always have the latest files available.

UPDATING ANTI-VIRUS, ANTI-MALWARE AND FIREWALLS

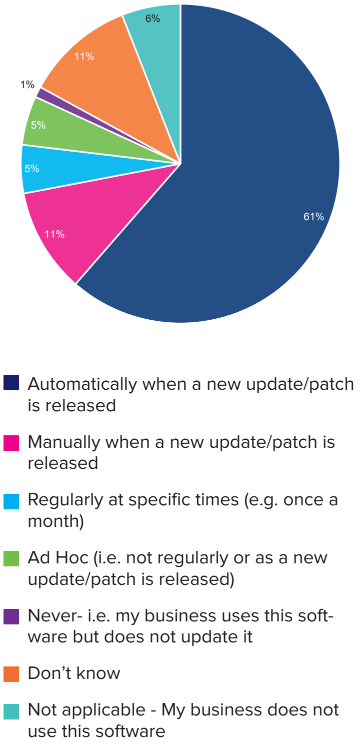
Anti-virus update frequency for small and medium-sized businesses



Anti-malware update frequency for small and medium-sized businesses



Firewall update frequency for small and medium-sized businesses



If your business does not have the latest software installed, you could be at greater risk of a cyber-attack. Most small and medium-sized businesses update their essential anti-virus software, anti-malware software and firewalls automatically: 68% automatically update anti-virus software when a new update/patch is released; 65% update anti-malware automatically when a new update/patch is released; and 61% update firewalls automatically when a new update/patch is released.

17% or less of all small and medium-sized businesses reported not knowing when they update each of these programs or do not use them at all.

BY SIZE

There is limited difference between small and medium-sized businesses as to when they update their anti-virus, anti-malware or firewall software. The most noticeable difference were that medium-sized businesses are more likely to update software manually when a new update/patch is released than a small business. For example, 16% of medium-sized businesses reported updating firewalls manually compared to 9% of small businesses. In addition, medium-sized businesses were more likely to not know when they update software.

BY SECTOR

The following indicates how often businesses update anti-virus, anti-malware and firewall software across sectors. The sectors presented are the two that update most frequently and the two that update least frequently. Across all three different cyber security measures, the hospitality and leisure sector is in the top two for not updating as frequently as other sectors.

UPDATING ANTI-VIRUS SOFTWARE AS SOON AS NEW UPDATES/PATCHES ARE RELEASED (AUTOMATICALLY OR MANUALLY):

- The IT and telecoms (85%) and legal* (85%) sectors were most likely to update anti-virus software automatically or manually as soon as an update/patch is released.
- The transportation and distribution* (63%) and hospitality and leisure (67%) sectors were least likely to update automatically or manually as soon as an anti-virus update/patch is released.

UPDATING ANTI-MALWARE SOFTWARE AS SOON AS NEW UPDATES/PATCHES ARE RELEASED (AUTOMATICALLY OR MANUALLY):

- The IT and telecoms (82%) and medical and health services* (81%) sectors were most likely to update anti-malware software automatically or manually as soon as an update/patch is released.

- The transportation and distribution* (56%) and hospitality and leisure (65%) sectors were least likely to update automatically or manually as soon as an anti-malware update/ patch is released.

UPDATING FIREWALL UPDATES/PATCHES AS SOON AS THEY ARE RELEASED (AUTOMATICALLY OR MANUALLY):

- Medical and health services* (81%) and IT and telecoms (78%) sectors were most likely to update firewall software automatically or manually as soon as an update/patch is released.
- The hospitality and leisure (62%) and other (66%) sectors were least likely to update automatically or manually as soon as an anti-malware update/ patch is released.

BY LOCATION

The frequency of how often small and medium-sized businesses update anti-virus, anti-malware and firewall software does vary by region. Top for updating anti-virus and anti-malware software as soon as a new update/patch is released (automatically or manually) was the East of England, with more than 80% of all small and medium-sized business doing so. East of England, alongside Scotland, West Midlands and the North East*, was also top for updating firewalls as soon as a new update is released, again with 80% of businesses reporting doing so

Noticeable across all three measures is that small and medium-sized businesses in Wales* were least likely to update as soon as a new update is available (automatically or manually), with less than 61% reporting doing so.

TOP TIPS

Software updates fix any security holes and bugs in your software and ensure that you reduce the likelihood of being compromised by hackers.
The NCSC advises updating software as soon as a new patch or update is available. The best way to achieve this is to do this automatically. However, some businesses may wish to do so manually. If the latter is preferable for your business, it is advisable to set notifications from your software providers so that you know when there is a new update and to not ignore these.

RECOMMENDATIONS FOR SMALL BUSINESSES

TAKE BITC'S READINESS TEST:
(www.wouldyoubeready.org.uk) At the end of the test you can download a PDF which contains useful tips and signposts to resources, as well as choose to opt in to a small business resilience community to receive future resilience communications.

IMPLEMENT THE NCSC'S CYBER ESSENTIALS:
These are the recommended minimum number of actions you need to take to help make your business more cyber resilient.

1. Use a firewall to secure your Internet connection – most devices have built in firewalls.

2. Choose the most secure settings for your devices and software.

3. Control who has access to your data and services – using passwords and specific user accounts.

4. Protect yourself from viruses and other malware using anti-virus software and staff training.

5. Keep your devices and software up to date – using auto-update mechanisms.

The NCSC has further guidance in their Cyber Security: Small Business Guide. This can be downloaded at https://www.ncsc.gov.uk/smallbusiness

BACK-UP YOUR DATA:
Back-up your business-critical data as often as possible, preferably automatically and in more than one place https://www.ncsc.gov.uk/guidance/backing-your-data.

UPDATE YOUR SOFTWARE:
Update software such as anti-virus, anti-malware and firewalls as soon as a new patch is released, preferably automatically, to stop hackers exploiting security weaknesses and bugs in older versions of the software: https://www.cyberessentials.ncsc.gov.uk/advice/.

HAVE A SECURITY POLICY:
Develop a security policy that includes cyber security. This needs to be shared with all new and existing employees and the appropriate regular training provided. This policy should include disciplinary procedures to discourage abuse of the policy: https://www.ncsc.gov.uk/guidance/10-steps-user-education-and-awareness.

TRAIN YOUR EMPLOYEES:
Staff need regular cyber security training to ensure their cyber awareness knowledge is up-to-date, so that they can conduct their work safely online, so they know what to look for to prevent an attack and the immediate steps to follow should an attack occur. Training needs to be appropriate to the user and how they use technology within the workplace. For example, the IT team of an organisation is likely to need more in-depth training then a standard technology user. Find guidance here: https://www.ncsc.gov.uk/guidance/b6-staff-awareness-and-training. Barclays Digital Eagles (https://www.barclays.co.uk/digital-confidence/eagles/) also have free resources.

BE ALERT: Keeping up-to-date is important to make sure you are aware of what is happening in the cyber security world. We would recommend following the NCSC's Twitter feed to be keep alert on current cyber threats: https://www.ncsc.gov.uk/threats

INVEST IN CYBER INSURANCE: Cyber insurance is not intended to replace good cyber security practice but rather be a back-up in case there is disruption to your businesses or there are costs involved with data loss or replacement of equipment. Cyber insurance also gives you access to specialists who can at short notice help to stop an attack and get back to business quickly. It can also help with managing your company's reputation should a breach occur and paying any fines associated with a breach: https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/business-insurance/cyber-risk-insurance/

CALL TO ACTION FOR LARGER BUSINESSES

We are asking larger businesses, with the resources and expertise they have internally, to support their small business customers and supply chains in implementing cyber security and resilience measures so that everyone is more secure online. Not only will this benefit your customers and suppliers, but it should improve the resilience of your supply chain from a cyber security perspective.

Some ideas of how you can support your supply chain are listed here:

USE SOCIAL MEDIA TO MAKE AN IMPACT:
Raise awareness using resources, such as BITC's Would you be ready? campaign. As a result, your small businesses customers and supply chains will see consistent business and government-backed messaging. The campaign uses impactful stills and videos designed to drive small businesses to BITC's Readiness Test (www.wouldyoubeready.org.uk). This quick test uses scenario-based questions to prompt businesses to think about their resilience; at the end of the test businesses can download a PDF, which sign-posts to resources.

PROMOTE THE NCSC'S CYBER ESSENTIALS AND CYBER SECURITY: SMALL BUSINESS GUIDE:
This means that small and medium-sized businesses are receiving the same, reliable, consistent messages from businesses, which are ratified by government. Cyber Essentials promotes simple but effective security controls that are the recommended minimum number of actions that all businesses should implement to protect themselves from cyber security threats.

PROCURE INTELLIGENTLY:
As part of your procurement process, consider tendering for new contractors and suppliers who are Cyber Essentials Certified. For existing contractors and suppliers, you could offer to support them to become certified.

PROVIDE BUSINESS SUPPORT: Support can be given in a variety of ways. It could be hosting resources on your own website or sign-posting to relevant partner cyber security information. It could also be more bespoke, such as providing workshops for your small business customers or tailored advice for the different sectors across your supply chain.

Should you wish to have more in-depth training on how to better support your supply chain and small business customers, BITC offers a Resilience Workshop for BITC Members. This covers a range of common UK disruptions, including cyber, extreme weather and infectious diseases.

GLOSSARY

SOCIAL ENGINEERING: Manipulating people into carrying out specific actions, or divulging information, that is of use to an attacker – phishing is a prime example.

PHISHING: Untargeted, mass emails sent to many people requesting sensitive information (e.g. bank details) or tricking them to visit a fake website. A Smish is an SMS message on a mobile device.

SPEARING AND WHALING: Targeted phishing where the email is designed to look like it is from a trusted source. Whaling is the sophisticated targeting of senior executives.

DATA BREACH: The accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. A data breach must be reported to the Information Commissioners' Office within 24 hours of having been identified.

MALWARE: A generic term for any malicious software that lets attackers monitor your activity and obtain your details when you log in, often without your knowledge.

WORM: Self-replicating malware that duplicates itself to spread to uninfected computers.

TROJAN: A type of malware that is often disguised as legitimate software but provides a backdoor into a device or system for cyber criminals.

ROOTKIT: Malware designed to provide an attacker with administrator access to a computer without being detected.

RANSOMWARE: Malware designed to block access to a computer system or data until a sum of money is paid to the attacker.

WATER-HOLING: Setting up a fake website (or compromising a real one) in order to exploit visiting users.

BAITING: A portable electronic storage device such as a USB stick left outside an office aiming for an employee to find it and plug it into their computer out of curiosity and compromise their computer or system.

DENIAL OF SERVICE: A cyber attack that disrupts an organisation's network so that it is unavailable to its intended and legitimate users, usually by overloading the service using malware bots.

ACRONYMS

BITC: Business in the Community

BERG: Business Emergency Resilience Group

GDPR: General Data Protection Regulation

NCSC: National Cyber Security Centre

SURVEY RESPONDENTS' PROFILE

All figures, unless otherwise stated, are from YouGov Plc. Total sample size was 1,003 adults. Fieldwork was undertaken between 12–20 November 2018. The survey was carried out online. The figures have been weighted and are representative of British business size. Where total responses on a question do not add up to 100%, this may be due to multi-coding or rounding to whole figures. In the report, figures for sectors and regions denoted by an asterisk (*) are based on fewer than 50 responses. Whilst this isn't statistically robust, the figures represent an indication of the views of this group. The tables below show percentage and raw values of respondents for each category.

Organization size			
	Small (less than 50 employees)	79%	799
	Medium (50 to 249 employees)	21%	204
Total		**100%**	**1003**

Work industry			
	Manufacturing	10%	105
	Construction	10%	97
	Retail	12%	119
	Finance and Accounting	10%	99
	Hospitality and leisure	10%	96
	Legal	4%	40
	IT & telecoms	12%	125
	Media, marketing, advertising, PR & sales	8%	82
	Medical & health services	3%	26
	Education	3%	29
	Transportation & distribution	3%	27
	Real estate	2%	25
	Other	13%	133
Total		**100%**	**1003**

Region			
	North East	3%	35
	North West	10%	102
	Yorkshire and the Humber	8%	76
	East Midlands	5%	55
	West Midlands	8%	85
	East of England	7%	66
	London	17%	170
	South East	19%	193
	South West	10%	98
	Wales	5%	47
	Scotland	8%	76
Total		**100%**	**1003**

ACKNOWLEDGEMENTS

Business in the Community would like to thank the following organisations for their support with the development of this report: Association of British Insurers, Aviva, Axis Capital, Barclays, British Insurance Brokers' Association, BT, Department for Digital, Culture, Media and Sport, Federation of Small Businesses, Fujitsu, HSBC, HSB Engineering Insurance, National Cyber Security Centre, Nominet, Royal Bank of Scotland, Sedgwick, 10x Banking and Trustify.

BUSINESS
IN THE
COMMUNITY

The Prince's
Responsible
Business Network

HRH THE PRINCE OF WALES
ROYAL
FOUNDING
PATRON

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

Chairman: Jeremy Darroch

Business in the Community is a registered
charity in England and Wales (297716)
and Scotland (SC046226). Company
limited by guarantee No. 1619253.