BUSINESS IN THE COMMUNITY The Prince's Responsible Business Network

BRIEFING

HOW LARGE BUSINESSES CAN SUPPORT SMES WITH CYBER SECURITY

This briefing contains insights from a roundtable with BITC members discussing how larger businesses can support smaller businesses with cyber security.

Context

Economies are now reliant on safe and reliable connectivity. The internet enables collaboration, connects businesses to customers and employees, and generates growth. Unsurprisingly, 9 in 10 enterprises in Europe make use of a fixed broadband connection to access the internet.[i]

However, increased reliance on the internet also means that businesses are now exposed to cyber crime. This presents a major issue to businesses with more than 80% of UK businesses experiencing a cyber attack in 2021[ii] at an annual cost of £21 billion.[iii]

The Covid-19 pandemic has made exposure to cyber-crime worse due to increases in the number of people 'working from home.'[iv]

Research has also shown that these issues are made more acute for small businesses because:

- They are more vulnerable due to lack of budget, resources, and expertise relative to large corporates.[v]
- They are more reliant on personal devices and phones to conduct business.[vi]
- They are often targeted as a means to infiltrate large businesses with sophisticated security.[vii]

INSIGHTS FROM OUR GUEST SPEAKERS

Nominet, Ellie Bradley, Managing Director

Nominet runs the registry of internet domains containing the domain extension ".uk", which includes large and small businesses and government organizations. Nominet gives a protective DNS service from cyber attacks for UK Government for 6 million public sector workers and around 900 national organizations.

Nominet works proactively with law enforcement authorities to reduce risks for all businesses from fraud, malware distribution, and other cyber-crimes. Prevention is a key strategy for Nominet and all domain registrations are checked through at the point of application in order to avoid supplantation of government websites, including protecting the public from misleading information related to the pandemic. Nominet also has a focus on education helping SMEs to get their business online and using social media, while also signposting towards resources that relate to cyber security.

Cyber Resilience Centre (CRC) for London, Simon Newman, Interim CEO

At present, all types of cyber crimes are increasing and the latest data[viii] shows that 4 in 10 businesses suffered at least one cyber attack or breach in the last 12 months. Phishing remains the most common

HRH THE PRINCE OF WALES ROYAL FOUNDING PATRON type of attack, with impersonation identified as another of the most disruptive forms of attack.

Despite the spike in cyber crime, a recent ONS survey[ix] shows that although 53% of respondents reported receiving a direct online threat, only 3% reported clicking on it. This shows people are acting more cautiously; however, only a small percentage are reporting cyber attacks to the police. Reporting will be key to increase understanding and help to inform policy; without data it is not adopt measures or address these problems in the right manner.

The good news is that most cyber crime can be prevented. The focus for CRC is "Getting the Basics Right" for every organization, even with simple actions such as using strong passwords, anti-virus software and awareness; however, the most important step is to create the right culture within the organization and among staff.

Supply chains are becoming a key target as they can be an effective way to access large organizations. To combat this, large organizations need to take responsibility and support SMEs in addition to the Government to implement policies to ensure individuals from every organization can take responsibility on this issue.

National Cyber Security Centre (NCSC), Anonymous Speaker

NCSC is the UK's technical authority for cyber threats providing support to public, private and not-for-profit sectors. Insights from NCSC's last annual review report[x] shows their active work in this space:

- NCSC ran 2.3 million cyber enabled campaigns - 442 phishing campaigns using NHS branding were taken down.
- NCSC have also offered support to nearly 800 business with significant incidents.

UK systems and professionals are gaining a better understanding of the risks for business and how they impact on activity. Cyber crime can have a large financial impact on organizations through financial theft, loss of investors, interruption of service and supply attrition.

The NCSC is helping businesses through its resources, including the Small Business Guide, Exercise in a Box and Cyber Essentials (full list at the end of this briefing).

NCSC also has a subscription centre[xi] which allows organisations to receive the latest news and information from NCSC, including a Small Organisation Newsletter.

Verizon Enterprise Solutions, Alistair Neil, Director of International Security Solutions

Verizon, the largest mobile phone carrier in the US, has been gathering information related to cyber security and data breaches for over 15 years, working along law enforcement authorities, tech companies and academia to develop a common language on this issue.

Their latest report[xii], which had 87 contributors from 82 countries has 5 key take aways:

- There are 4 core pathways for cyber crime: credentials, phishing, exploiting vulnerabilities and botnets.
- Ransomware has become industrialized and is the biggest single threat.
- Supply chain breaches can multiply threats.
- Error continues to be a dominant trend and is related to misconfigured cloud storage, using unprotected printers at home, etc.
- The human element continues to drive breaches. Although reporting and awareness is getting better.

The most common threats to SMEs last year were ransomware, use of stolen cards and phishing. Basic security recommendations should be followed by businesses to help mitigate these threats, having a plan is critical and using the NCSC's 'Exercise in a Box' is highly recommended. Having a quick response action plan, where everybody in the organizations knows their role and has a common understanding, can also dramatically diminish the scale of impact.

Sebastian Kobelt, Sebastian Kobelt Chocolatier and Pâtissier

Sebastian Kobelt works with hundreds of businesses to supply chocolate to the hospitality sector both directly and via online channels. Therefore, the security of confidential data is a crucial part of his business operations. Key cyber security measures taken by his business include:

- Developing a secure invoice system and online shop to keep data secured.
- Training employees to minimize the risks with regular checks including changes to passwords, backing-up files, anti-virus use by approved suppliers, advice on avoiding email attachments, and controls for social media use and direct messages.

Sebastian highlighted that having someone to turn to, either individuals or other businesses, that you can trust for advice around cyber security is critical.

TOP TIPS FOR LARGE BUSINESSES

Share resources: Share guidance and resources, such as those available from the NCSC website, including:

- Cyber Aware: a behaviour change campaign seeking to encourage the public and SMEs to implement basic cyber security measures
- Small Business Guide: this includes a self-assessment tool and further guidance for SMEs to improve their cyber security with five easy-to-implement measures
- Response & Recovery Guide: for when a cyber attack does occur
- Exercise in a Box: a practical scenario-based exercise to understand and rehearse responses
- Top Tips for Staff: free cyber security training for staff
- Cyber Essentials: a certification recommended for all businesses that want to work with the government. It shows how to address basic cyber security and prevent the most common attacks; and also gives CyberLife insurance of £25,000 for an eventual attack giving organisations a better chance to have a well-connected and safe supply chain.

Offer support: offer advice or mentoring to your SME customers or supply chain to enable them to implement effective cyber security measures.

Offer funding support: Cyber security measures can be costly for some SMEs. Larger businesses funding certifications, such as Cyber Essentials, and training for SMEs could be an investment for the security of your own supply chain, as it is more valuable to mitigate risks and could save the potential costs associated with a data breach or ransomware threat in the supply chain.

Broaden your training: It may be worth offering internal training for your own staff and including SMEs as part of this programme to build a culture of awareness.

Establish joint responding mechanisms: Should a cyber attack occur, acting fast is crucial. Helping SMEs to create rapid and efficient ways for communication in case of breaches could minimize any potential harms and benefit all.

Report fraud: Encourage SMEs to report cyber attacks to Action Fraud. The more data and insights there are, the better users can be protected, and criminals caught.

FURTHER INFORMATION

BITC members can now access the briefings from the previous BITC Small Business Support Roundtables , which provide expert advice and guidance for businesses to support their supply chain and SMEs in other pertinent areas:

- Large Businesses Supporting SMEs Taking Climate Action outlines the main discussion points of the Climate Action roundtable so BITC members can better understand how they can support SMEs with practical actions they can take to start their journey towards net zero.
- Large businesses supporting wellbeing in their supply chain briefing contains insights from a roundtable where BITC members discussed how larger businesses can support SMEs with wellbeing for business owners and their employees.

ENDNOTES

[i] The Telegraph (2019), *The connections driving business*, available at: https://www.telegraph.co.uk/business/future-technologies/connectivity-technology/

[ii] CyberEdge Group (2022), *2022 Cyberthreat Defense Report*, available at: https://cyber-edge.com/cyberthreat-defense-report-2022/

[iii] Detica / Cabinet Office (2011), *The Cost of Cyber Crime*, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf

[iv] PwC (2020), *Embracing the new normal: responding to cyber security challenges during the COVID-19 crisis*, available at: https://www.pwc.com/jg/en/issues/covid-19/cyber-security-challenges-during-the-covid-19.pdf

[v] Canon, *Why small businesses are at a higher risk of cyber-attacks*, available at: https://sg.canon/en/campaign/business-insight/tips/why-small-businesses-are-at-higher-risk-of-cyber-attacks

[vi] Deloitte (2022), *Impact of COVID-19 on cyber-security*, available at: https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

[vii] Economic Times (2020), *SMEs emerge as easy prey for cyber-attacks as large firms beef up security*, available at: https://economictimes.indiatimes.com/tech/tech-bytes/smes-emerge-easy-prey-for-cyber-attacks-as-large-firms-beef-up-security/articleshow/79924436.cms?from=mdr

[viii] Department for Digital, Culture, Media & Sport (2022), Cyber Security Breaches Survey, available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

[ix] Office of National Statistics (2022), Crime in England and Wales: year ending December 2021, available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/latest

[x] National Cyber Security Centre (2021), NCSC Annual Review 2021, available at: https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021

[xi] National Cyber Security Centre, Subscription Centre, available at: https://ncsc-production.microsoftcrmportals.com/subscribe/

[xii] Verizon (2022), 2022 Data Breach Investigations Report, available at: https://www.verizon.com/business/resources/reports/dbir/