Summary of Proceedings

Digital Security and Data Protection in SMEs

How to ensure SMEs are less vulnerable for a post-COVID digital world?

Digital for SME 'D4SME' Global Initiative webinar – 29 October 2020

The issue: Emerging digital technologies are opening tremendous market opportunities for SMEs and creating entirely new industries, but, in turn, raise vulnerability to digital security risks. As small and medium-sized enterprises (SMEs) connect to the digital world and move towards new digital solutions, they will need to effectively manage cyber-risks to reap the benefits of the digital transition. In the context of the COVID-19 pandemic, more businesses have been forced to operate online than ever before, and their reliance on digital infrastructure, cloud computing and software has increased, as the intensity of cyber-attacks.

Many SMEs lack the awareness, resources or expertise to assess their digital risk exposure and to implement appropriate prevention and remediation measures which are more common among larger. The risk is particularly pronounced in sectors where SMEs tend to process significant volumes of personal – and valuable – data, such as professional services, healthcare and retail trade.

1. Context and Introductory Remarks

Ms Lucia Cusmano – Deputy Head of SME and Entrepreneurship Division, *OECD Centre for Entrepreneurship, SMEs, Regions and Cities (CFE)* explained how although SME digitalisation has the potential to increase efficiency and productivity, there is a need to accelerate the SME digital transformation and close the gap between large and small firms. Barriers to SME digitalisation such as lack of skills and resources, as well as regulatory complexities, existed before the COVID-19 pandemic. Whilst COVID-19 is forcing many SMEs further along their digital journey, it has also exacerbated the former gaps and risks. SMEs have been prompted to use digital tools and move operations on digital platforms without further preparedness as regards the digital security risks they could incur. The D4SME initiative in the context of the pandemic is focussing on how this accelerated digitalisation of SMEs can increase their resilience and long-term growth perspectives. Helping SMEs better manage digital security risks has appeared as an important area for public policy attention.

The discussion was moderated by **Ms Sandrine Kergroach, Senior Economist of the OECD Centre for Entrepreneurship, SMEs, Regions and Cities (CFE).**

2. Panellist Key Takeaways

Mr Benjamin C. Dean - Cyber Catastrophe Research Lead, *Hiscox* shared some insights from the forthcoming OECD CFE report on "Digital Security and Data Protection in SMEs". Mr Dean highlighted that SMEs have a smaller attack surface than larger firms because of their size, because they tend to be less digitalised and because they are often less profitable target for cyberattacks. Smaller firms have less sophisticated in-house capacity for managing digital security risks. They are less likely to have employees in the enterprise who are aware, skilled and dedicated to this task. Rather, SMEs tend to outsource digital security solutions and management. In addition, SMEs are connected to many organisations, in supply chains, markets and business transactions. SMEs under attack can therefore become a platform for accessing a greater number of and larger players. Digital security management in SMEs must therefore be considered as part of a larger ecosystem. In the context of COVID-19, SMEs are increasing their exposure to cyber-risks as they shift rapidly a

majority of their operations online. At the same time, SMEs may be less well prepared to adapt to this fasting changing context compared to large firms.

Mr Aviv Abramovich - Head of Security Services, *Check Point (Israel)* explained that financial gain is the primary motivation behind digital security attacks targeting firms of all sizes. Mr Abramovich explained that the first point to take into consideration is that attackers use tools of the same level of sophistication independently from the fact that the target is a small or a large firm. He then highlighted that in the context of the COVID-19 pandemic, there has been a strong correlation between the increased digitalisation of business practices and the intensification of cyber-attacks. Finally, he noted that the digital environment has become more complex (e.g. business operations shifting online, individuals using their mobile phones and tablets more). All these trends have created new vulnerabilities that hackers can exploit.

Mr Abramovich concluded by pointing out that the digital insecurity created by COVID-19 and these new complexities has only deepened the divide between small and large firms. Larger firms often have dedicated digital security departments in defending against these threats whilst SMEs do not. As the digital business ecosystem becomes increasingly interconnected, this vulnerability makes SMEs "weak links" in the networks and the easiest access points for hackers to target larger firms.

Mr Steffen Mauer – Co-founder and CTO, *ATLAS Intelligence Gmbh (Germany)* emphasised the complexity of the Information Technology (IT) ecosystem and the lack of experts in digital security services. This widening skill gap puts businesses at a loss of where to find individuals with appropriate skills. Mr Mauer advocated for an upgrade in how skilled personnel are educated to ensure programmers have the appropriate practical skills. He highlighted how academic institutions can play an important role in this upskilling by engaging with code experts in academic research.

Mr Mauer added that he believed the greatest digital security risks to SMEs to be those associated with human error, such as how individuals interact with their personal or work emails. These behavioural risks are harder to control at an organisational level. He also observed that in his direct experience many smaller firms that purchase digital security software, often do not have the knowledge on how to best use and configure them.

Ms Annika Linck - Project Manager, *European DIGITAL SME Alliance* indicated that one of the main challenges for SMEs in achieving a robust digital security strategy is the lack of internal resources and expertise. She emphasised how the heterogeneous nature of SMEs also presents a challenge as digital security solutions need to be tailored to the different levels of digitalisation amongst small firms. Ms Link stressed three levels where capability gaps should be addressed: organisational capability, individual capability and the ecosystem. She suggested that awareness campaigns on the importance of digital security practices need to be targeted not only at the organisational level (executive level, HR, finance department) but also to the business ecosystem at large. Ms Link emphasised how the digital business ecosystem is highly connected and there is an important role to be played by digital front runners or 'enablers' to assist the SME "missing middle" to achieve more secure cyber practices, for instance through business partnerships. Similarly, she highlighted how there is a place for intermediaries such as chambers of commerce, sector associations and service providers like accountants and insurance, as well as local authorities to work with legislators and strengthen the ecosystem.

Ms Jessica Hunter - Cyber Security Services Division, *Australian Cyber Security Centre (Australia)* shared details on the Australian Cyber Security Strategy. She emphasised how the strategy includes policy instruments that specifically target SMEs as a vulnerable group. According to an Australian Cyber Security Centre (ACSC) national survey conducted in 2019, SMEs spend much less than is optimal on their digital security strategy, with over 50% indicating they would not spend more than 250 euros annually. The survey also indicated that many SMEs overestimate their ability to respond to attacks and often outsource ICT security management. Ms Hunter further echoed other

panellists call for an emphasis on awareness. She also mentioned the need to get more evidence and a better understanding of the digital security issue.

The ACSC chose to tailor a specific strategy for SMEs as they believed that by simplifying technical terminology smaller firms would be able to better understand the threats. The strategy also has a focus on software solutions, skills and pragmatic procedures. For the ACSC it is important to not just offer guidance on *what* SMEs should be doing, but *how* they should implement a digital security strategy. The ACSC strategy for SMEs notably works with other actors in the ecosystem, providing efforts for matchmaking between digital security providers and the SMEs. Ms Hunter shared policy examples such as tailored tool kits (e.g. to assess maturity levels) and grants for SMEs spent at private sector cyber security firms. Ms Hunter explained how there is also a local dimension to the strategy through regional hubs which can engage in face-to-face interactions and act as intermediaries to raise awareness amongst SMEs.

Ms Hunter advised that when policy makers are developing a digital security strategy for SMEs it is critical to include SMEs in the discussion early on in the strategy consultation; stressing that it is important that policy makers recognise SMEs as equal a threat as other groups and clearly define the important role that SMEs play in the broader ecosystem.

3. Open Q&A Discussion

Are cloud services safer from attacks?

- Mr Abramovich explained that although cloud services provided by multinational tech companies have high levels of digital security, they are not completely 'safe.' Mr Abramovich referred to the 'Shared Responsibility Model' in which SMEs are also responsible for part of their security and pointed out that there are a number of tools available in the cybersecurity industry to ensure cloud platforms are configured correctly.
- Mr Dean suggested that cloud services might be safer than traditional systems but at a greater ecosystem level if all small firms are dependent on the same provider there is a risk of catastrophic disruption if the cloud platform is compromised.

Does the Australian government provide training in cybersecurity or funds organisations providing it to SMEs? Does it have a proactive policy outreach to SMEs?

- Ms Hunter explained that the Australian government funds training programs for SMEs through regional hubs. These, 'Joint Cybersecurity Centres' offer in-house training to SMEs such as training to executives who are creating the digital security strategy for their business. The Australian government also funds industry bodies to produce tailored training for SMEs and offers sector specific advice.

What would be one piece of pragmatic advice you would offer an SME starting out on their digital journey?

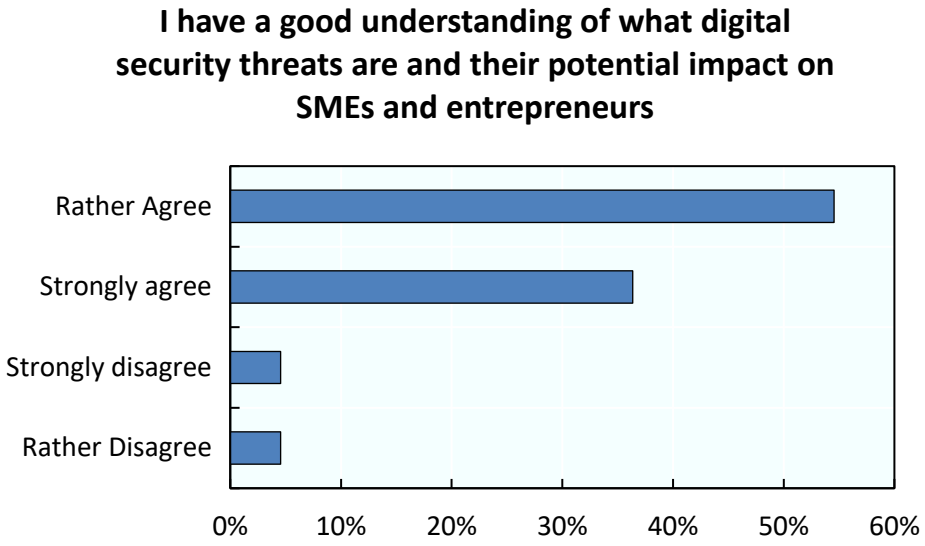
- Mr Mauer suggested that the big cloud services are a good place to start. He explained that when you do not have the skills or employees to take care of ICT it is wise to turn to a big provider to be productive.

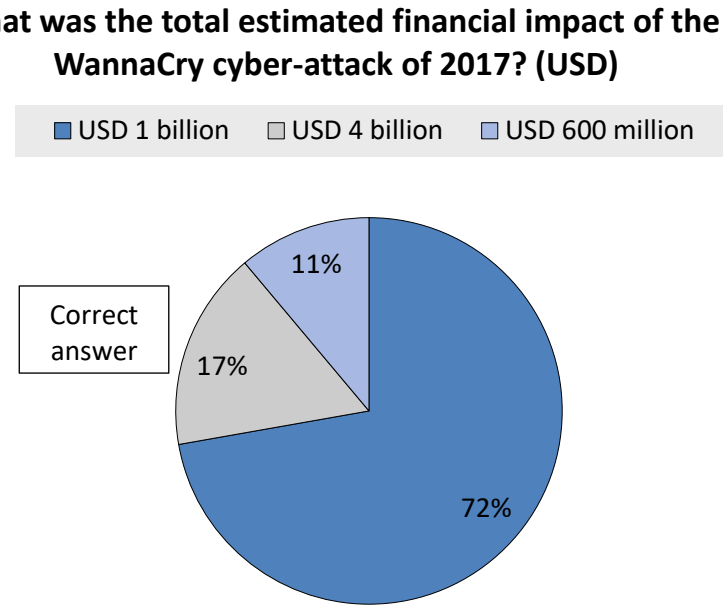
Mr Laurent Bernat - Cybersecurity Policy Analyst, *OECD Directorate for Science, Technology and Innovation*, rapporteur of the session, highlighted what he saw as the main takeaways from the discussion, bringing to the table some of the insights from the activities of the OECD *Working Party on Security in the Digital Economy*. Mr Bernat observed how the digital security of SMEs is becoming a strategic policy priority, a trend that is bound to accelerate in the context of COVID-19. He highlighted that as we are only at the beginning, policy makers and practitioners alike should take the time to understand the various facets of the challenge in order to develop balanced policy. He underlined the complexity of digital security which can be daunting for many SMEs who need to sufficiently understand the technical security aspects in order to make informed risk management

decisions which can have serious economic consequences on their business. Mr Bernat explained that many countries have put in place national Cyber Security Strategies and that a key policy challenge is to integrate SMEs into these strategies and then to turn the strategies into action. He stressed that cross-cutting co-operation within governments and a multi-stakeholder dialogue are key to make progress in this area.

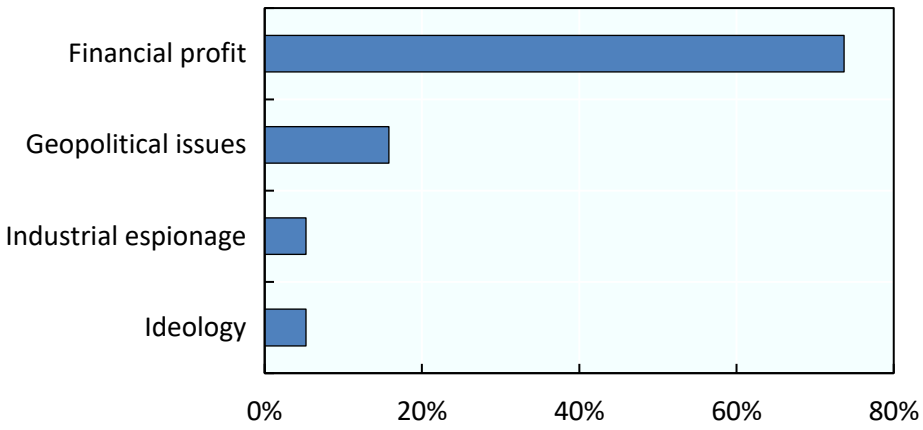
4. Audience Live Polls

All graphs represent the percentage of responses from the 70 participants to the specific question.

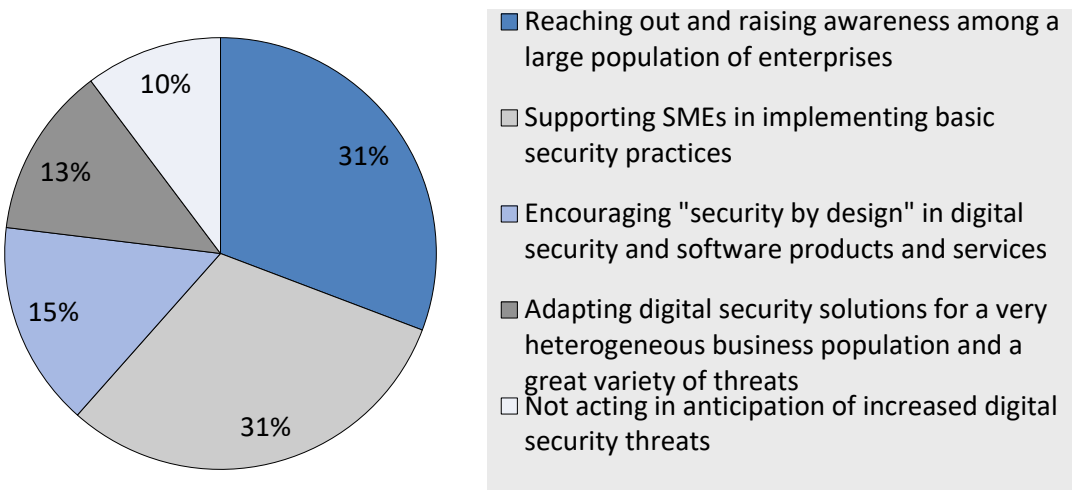




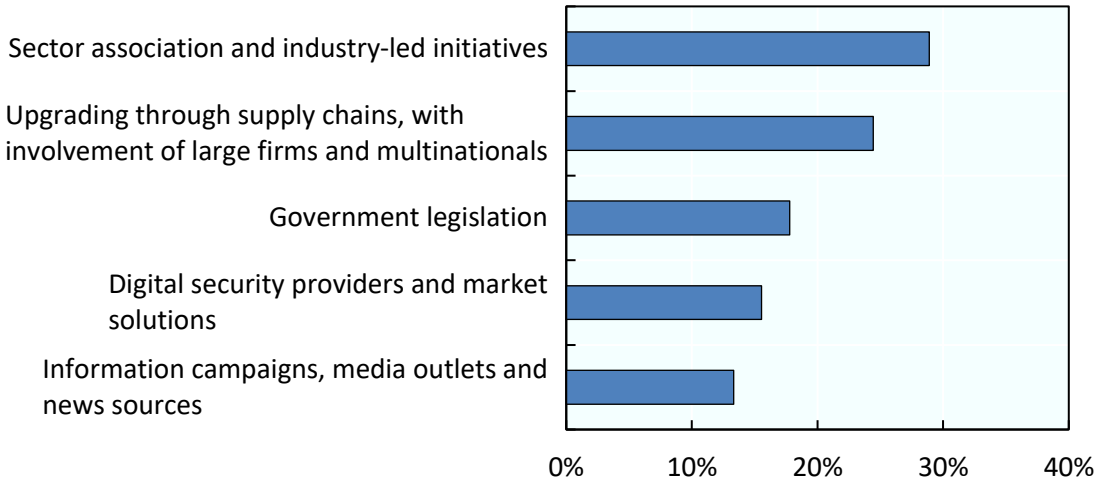
What do you see as the main motivation behind cyber-attacks?



In your views, what are the main challenges ahead with regards to SME digital security? (multiple choice)



In your view, what are the key channels to improve SME digital security and data protection?



Read More

The Digital for SME 'D4SME' Website is constantly being updated with relevant information of SME digitalisation and upcoming activities surrounding the initiative: https://www.oecd.org/going-digital/sme/

The OECD COVID-19 portal, provides analysis of the impact of the COVID-19 crisis and reports on policy responses, including a note on SME policy responses https://www.oecd.org/coronavirus/en/

OECD contacts

For more information on the D4SME Initiative please contact marco.bianchini@oecd.org, Madison.lucas@oecd.org