COVID-19 CYBER SECURITY THREATS TO MSMEs

The novel coronavirus (**COVID-19**) pandemic is an unprecedented health and economic crisis, affecting the lives and livelihoods of workers, as well as the continued operations of businesses globally. Micro-, small- and medium-sized enterprises (**MSMEs**) and their workers, as well as entrepreneurs and the self-employed, are among the hardest hit. It is imperative that urgent and decisive action is taken by all stakeholders to combat the economic repercussions of COVID-19 and safeguard the current and future functioning of the global economy.

The International Chamber of Commerce (**ICC**), the institutional representative of more than 45 million companies in over 100 countries, has launched a campaign to "Save Our SMEs" to (i) shine a spotlight on the devastating impact of COVID-19 on small businesses and their employees; (ii) ensure effective policy and fiscal responses at both the international and national levels; and (iii) provide resources and tools to small businesses to help them navigate the unprecedented economic shock unfolding before us.

COVID-19 DISRUPTIONS INCREASE RISK OF CYBER-ATTACKS ON MSMEs

To ensure business continuity, protect workers and continue to serve customers during the COVID-19 pandemic, many organisations are moving substantial parts of their operations online. In the wake of the crisis, there has been an upsurge in the use of online and digital tools, primarily to support communication. This creates new opportunities for malicious actors to take advantage of the disruptive effects of the crisis and target MSMEs for cyber-attacks.

Even before the current crisis, MSMEs were increasingly the target of cyber-attacks due to the lack of resources to implement comprehensive cyber security solutions. A recent report suggests that small businesses are the target of over 40%of cyber-attacks with an average loss per attack of more than US$ 188,000.[1] Cybercriminals have been capitalising on the piecemeal tools used by MSMEs to protect their operations[2] and using MSMEs as the "weakest link" to exploit their connections to larger companies in the supply chain. In 2019, it was estimated that one out of five SMEs had fallen victim to a ransomware attack.[3] Phishing attacks have also reached their highest level in three years with small organisations receiving malicious emails at a higher rate.[4]

Large-scale adoption of work-from-home technologies, heightened activity on customer-facing networks, and greater use of online services by MSMEs in response to the COVID-19 lockdown measures have exacerbated these risks, putting immense stress on cyber security controls, which cybercriminals have been quick to exploit. Now, with heightened security risks, it is vital that companies be able to identify cyber security threats and effectively manage their information systems during the current crisis, as part of their business continuity plans.

[1] Verizon, *Data Breach Investigations Report* (2019).

[2] Symantec, *Internet Security Threat Report* (Vol 24, February 2019).

[3] Datto, *Datto's Global State of the Channel Ransomware Report* (2019).

[4] APWG, *Phishing Activity Trends Report* (Q3, 2019).

KEY CYBER SECURITY RISKS FOR MSMEs IN THE CONTEXT OF THE COVID-19 CRISIS

The following section provides a typology of current cyber security risks and sets out concrete steps MSMEs can take to enhance the security of their operations.

> **Phishing and Business Email Compromise attacks using COVID-19 as bait**
Phishing and Business Email Compromise schemes often proliferate in the aftermath of crises to exploit fear and confusion. In the wake of the COVID-19 crisis, there has been a surge of malicious emails using basic social engineering techniques to lure users into providing valuable information under false pretences. Cybercriminals will often pose as a legitimate agency or a trusted source such as the World Health Organization and local authorities to coax individuals into sharing sensitive data.

> **Malware distribution using COVID-19 as bait**
Similarly, malicious actors are using COVID-19 as a lure to distribute malware and interfere with business networks. Cyber security firms have identified multiple malware families, including ransomware and spyware, using COVID-19 related themes to infect a device and gain unauthorised access to the network. This can compromise sensitive data and cause extensive damage to an MSME's IT systems.

> **Remote working and supply chain threats**
Securing the infrastructure for remote working remains a challenge for many MSMEs. Usage of applications for remote working was rife before the COVID-19 crisis but as workers increasingly use personal devices to ensure business continuity, many communications are now taking place outside company firewalls. This can significantly increase cyber security risks for MSMEs as applications for remote working are often the target of malicious actors. MSME dependence on outsourced tools and web-based services can increase risk overall.

> **Heightened vulnerability due to lack of awareness**
Cyber security threats very often remain under the radar and by far the greatest risk for MSMEs is the lack of awareness or underappreciation of cyber security threats. In the current environment, where MSMEs are squarely focused on tackling operational stresses, addressing liquidity issues and securing the health and livelihoods of their workforce, cyber security threats may be underestimated. Below, we suggest several easy steps that can quickly help increase MSME cyber security resilience.

EASY STEPS FOR MSMEs TO PROTECT THEIR BUSINESS FROM CYBER SECURITY THREATS DURING THE COVID-19 CRISIS

> **Raise awareness within the organisation—employees are the first line of defence against cyber-attacks**
In 2018 over 50% of security incidents were a result of human error rather than a deliberate attack.[5] In addition, many security incidents that result from a deliberate attack can be avoided if individuals take appropriate steps. Employees must understand their daily responsibilities in handling, protecting and supporting company data and networks. This includes simple steps such as selecting strong passwords and ensuring responsible email use. Importantly, employees should be made aware of possible scams and malware in order to recognise, refrain from sharing, and report malicious material in a timely manner. MSMEs should also implement company-wide policies that create a culture of information security which bans use of unlicensed software, updates all software regularly to help patch security flaws and establishes safe browsing and social media rules.

[5] Kaspersky, *The State of Industrial Cyber Security* (2019).

ICC has partnered with the Cyber Readiness Institute (**CRI**) to offer advice and training for MSMEs, from quick tips and guidelines to a comprehensive cyber resilience training programme, available free of charge in seven languages (Arabic, Chinese, English, French, Japanese, Portuguese and Spanish).

- **Strengthen remote access management policy and procedures**
  MSMEs must contend with an increasingly complex remote access environment, in light of the rapid rise in teleworking and the proliferation of devices (phones, laptops, tablets, whether they are company-owned, personal, shared, public or a combination thereof), as well as the different ways to connect to the Internet (home or public wi-fi, company provided hotspot) and to access company data (Virtual Private Network, cloud-based technology or other). It is therefore important for MSMEs to set out clear guidelines for their employees with respect to proper use of remote access. As a general rule of thumb, company-issued devices should be preferred to personal or public devices. Similarly, private networks and company-issued hotspots should be preferred to public networks, barring the use of a VPN. Cloud-based systems, centralised file-sharing systems or a dedicated file sharing site with company oversight should be used for accessing and sharing documents.

  ICC and the CRI have also partnered to offer an online training webinar for SME managers and employees to better align remote working with cyber security requirements. The online training webinar is built on a series of CRI quick guides on how to secure remote workforce.

- **Secure supplier portals and other external facing systems**
  It is crucial that MSMEs map out, assess and manage all entry points with the underlying objective of making information systems impervious to outside tampering. Quick practical steps include updating and patching software, updating passwords and encouraging multi-factor authentication. This also entails greater communication with business partners to secure networks across the supply chain. Showing leadership in cyber security can increase overall resilience across the supply chain and bolster MSMEs' credentials with existing or potential business partners.

- **Update incident response plans in a more distributed environment**
  Because of the evolutive nature of cyber threats, even well protected companies can experience security breaches. Businesses operate in an environment where risk can be minimised but not entirely removed. A quick response is critical in order to mitigate and, where possible, fence off the disruptive effects of an attack. Successful incident management includes a clear communication strategy with both internal and external stakeholders as well as support from specialised third parties to help contain and remedy the incident. MSMEs should also proactively engage with law enforcement and specialised oversight agencies to help tackle increasingly sophisticated cyber threats.

  With respect to cyber-attack risk in the current crisis, we also advise MSMEs to follow government guidance and recommendations issued by national Computer Emergency Response Teams, and urge policymakers to provide up-to-date and comprehensive information on the locally specific cyber security threats businesses face.

The ICC Cyber Security Guide for Business offers a comprehensive approach to sign-post effective action and help guide discussions for management and information technology teams. The document features a security self-assessment questionnaire and a set of five principles to reduce risk associated with cyber security incidents. The principles are supported by a checklist of six essential steps every company should take to set managers on a course towards information security excellence. Importantly, this guide can help companies engage with business partners and wider networks to assess and better secure all points of entry.

Finally, we encourage MSMEs to actively engage with the many ICC initiatives on cyber security. The ICC Commission on Digital Economy brings together companies of all sizes to assess cyber threats and offer tailored recommendations to tackle this multifaceted issue with an emphasis on adaptive and flexible solutions.