Business at OECD Policy Brief: Covid-19 and Digital Security

July 2020

Introduction

In the Covid-19 crisis the security of digital technologies delivering critical infrastructure and essential services in response to the pandemic across sectors has become a major concern.

Since the onset of Covid-19 there has been an increase in malicious activity including hacking, phishing, malware, piracy and counterfeiting.[1] This has presented significant risks to health systems, Government, business and people, impeding activities to mitigate the Covid-19 crisis For example, health services are connected through the *Internet of Things* (IOT) to ensure coodination of medical services, treatment, diagnostics and care. A medical ventilator, critical for many being treated for the virus, may require up to one million lines of code. Systems must be reliable and safe.

Vulnerabilities are exacerbated in places and for people with low digital literacy, and small and mid-sized businesses seeking funding or loans may be particularly vulnerable to phishing and other scams. The pattern of malicious cyber activity has been shown to match the worldwide spread of Covid-19, including an exponential increase in fraudulent or abusive activities online:

- Trendmicro reports 907K spam messages are related to COVID-19 in 1st Quarter 2020. Spam has increased 220 times from February to March 2020, and 48K malicious URL hits were related to COVID-19 in Q1, an increase of 260% from February to March. [2]
- Large-scale spam campaigns using Covid-19 as a handle are attempting to spread ransomware, steal data or install banking malware.
- E-mail phishing campaigns try to get users to connect to fraudulent web pages offering downloads of comprised documents about Covid-19.
- A growing number of state-sponsored groups are now using the subject of Covid-19 to conduct various types of espionage.[3]

Digital Security is a "borderless" issue, requiring a combination of inter- and intra- sector and country collaboration as well as private-public partnership is needed to effectively address threats. A strategic approach is required to move this collaboration beyond the law enforcement, intelligence agency and Information Security 'circles of trust' that exist today, which predominantly focus on operational and tactical threat information sharing. [4]

There is also concern that governments may stockpile or exploit vulnerabilities during the Covid 19 crisis and beyond. Thus, policymaking and conduct in this area should be mindful to ensure democratic market-based economy standards. This concern is shared by essential

[1] https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

[2] https://resources.trendmicro.com/rs/945-CXD-062/images/Trend-Micro-Research-COVID19-Threat-Brief-Summary-13April.pdf

[3] Thales Cyber Threat Intelligence team. https://www.thalesgroup.com/en/market-specific/critical-information-systems-and-cybersecurity/news/covid-19-new-weapon-cyber

[4] Citi, Note on Cyberisk and Security.

businesses or firms as they reopen and may collect medical data on their workers (temperature, symptoms, whether they've had Covid-19, been hospitalized, etc.) but not having certainty how the data is kept and for what duration and security of the data storage.

Strengthening Digital Security during the Pandemic and in the Recovery Beyond

Strengthening trust, enhancing resilience and protecting healthcare are business priorities for digital security in the Covid-19 crisis. Secure data systems will be critical also for future preparedness and the resilience of our societies and economies.

- **Strengthening Trust - Invest to strengthen digital infrastructure and enable trust:**
    - Need for deployment of standardized, interoperable, global certification schemes, which is glabally becoming a prioity including for products without cryptography
    - Need to ensure clear parameters and timelines around the application of rules in time of emergency – exceptional cicumstances may imply that for periods of time during the emergency exemption from rules for digital security and data protection
    - Governments should not stockpile and/or exploit vulnerabilities in the Covid-19 crisis and beyond.
    - Concern that the partnership between private cybersecurity researchers, businesses, and public law enforcement are at risk to disparate interpretations of new and existing data protection laws

- **Enhancing resilience**
    - Ensure acknowledgement that security of consumers and business alike are impacted with the rise of e-commerce in the crisis
    - Address the lack of common industry definitions standards and incentives for proactive detection and mitigation of exploits before circumstances become exceptional
    - Concern that there is a lack of vulnerability disclosure point(s) of contact for security researchers to handle and inform only the relevent people in a data breach situation.
    - Urgent need to equip organizations and people with the necessary skills to identify and protect themselves against digital security risks

- **Protecting Healthcare:**
    - Need to reinforce the security of health systems, including diagnotics, treatment and remote consultation to ransomware against cybersecurity attacks

- Ensure the security of Artificial Intelligence (AI) algorithms in development of treatments and diagnostics

Business is working to provide solutions to enhance digital security through:

Overall security ecosystems:

- Development of solid coordinated vulnerability disclosure practices;
- Public private partnerships to deliver more reliable secure digital information systems;
- Focus on improving operational resilliency by managing cybersecurity through interoperable, risk-based frameworks;
- Application of blockchain technologies accross sectors

Enhancing Trust:

- Innovations to advance privacy preserving machine learning, to deliver better data security especially important in context of health care applications
- Development of homomorphic encryption allowing for encryption of data in AI systems and cloud services (as if the data were plain text).

Applications in Healthcare:

- Development of encryption tools for use by doctors and medical professionals in sharing medical data.
- Developing tools to address and protect the security of network devices like gateway and virtual private network (VPN) appliances from ransomeware attacks in the healthcare sector.[5]
- Application of blockchain for example to track infectious disease outbreaks, secure medical supply chains and support more effective crisis management[6]

Policy issues for digital security - in light of Covid-19 and beyond:

- **Importance of an integrated multistakeholder policy approach:** Promotedigital security frameworks including the OECD Guidance on digital security risk, Privacy, AI and Enhanced Access to and sharing of data.

- **Public private partnership:** Policy should support public private partnerships to advance digital security objectives. Policies and regulations adopted in during emergency

[5] April 1, 2020, Microsoft works with healthcare organizations to protect from popular ransomware during COVID-19 crisis: Here's what to do, Microsoft Threat Protection Intelligence Team , Microsoft Threat Intelligence Center (MSTIC)

[6] Ahmed Banafa, https://www.bbvaopenmind.com/en/technology/digital-world/blockchain-technology-and-covid-19/

situations must be transparent and understandable for all to respond effectively.. Criticality risk/benefit balance must be re-evaluated to find quick and timely solutions including regulatory sandbox approaches.

- **Investment in digital infrastructure:** Prioritize investments in digital infrastructure, promote capacity building and R&D, supported by coherent regulations for digital security?

- **Information sharing – multilateral approach:** Adopt best practices that allow for voluntary, meaningful information sharing programs through a multilateral approach, to help anticipate, mitigate, or manage networks to meet changing demands. This includes to ensure that solutions are technically feasible, achievable, not cost-prohibitive and donot result in unintended economic or commercial consequences.

- **Leverage internationally recognized cyber risk management frameworks and their standard taxonomies and terminology:** Such frameworks, including ISO/IEC 27103, provide a foundational security baseline that facilitates interoperability and cross-sector and cross-border coordination.

- **Workforce:** Adopt a clear and consistent definitions of an "essential critical infrastructure workforce" in times of confinement due to a global crisis to ensure continued security, availability and maintenence of digital systems whilere-emphasizing the importance of cross-border policy/legal interoperability.

- **Training and skills:** Need to equip organizations and people with the necessary skills to identify and protect themselves against digital security risk. "Social Immunity" has to be developed even in cyberspace by facilitating public understanding of potential risks in cyberspace, and develop resilience against incidents including the COVID-19 related malicious campaigns.

- **Democratic values:** Concern that governments do not stockpile or exploit vulnerabilities in the Covid 19 crisis and beyond. Standardization must be mindful of democratic market-based economy. and no data must be controlled on behalf of nondemocratic sovereignty.

OECD Role:
Business looks to OECD for evidence based analysis and global standards to enhance digital security in context of and recovery from the Covid-19 crisis:

- Working with business at OECD (BIAC), OECD should build the evidence base for digital security guidance and best practice, and serve as a lead organization for international co-operation on digital security together with relevent organizations and business.

- The review of the OECD Guidance on Digital Security Risk should take into account the valuable experiences learned from the Covid-19 crisis

- The OECD Global Forum on Digital Secuirty and Prosperity, should reinforce the importance and value of multistakeholder cooperation to mitigate global digital security risk , including with OECD non-member economies and relevent international organizations as well as G7 and G20.

Business looks forward to continued work with OECD to address these issues towards a more secure digital economy. The following annexe provides examples of business action and solutions towards a more secure digital transformation.

Annexe: Business examples

A compilation of business examples can be accessed here and on the *Business at OECD* Webiste Covid 19 Page. (link to be added)

BUSINESSatOECD

***Business at OECD* (BIAC)**
13-15 Chaussée De La Muette
75016 Paris
France
contact@biac.org | @BusinessAtOECD | www.businessatoecd.org

Established in 1962, *Business at OECD* stands for policies that enable businesses of all sizes to contribute to growth, economic development, and societal prosperity. Through *Business at OECD*, national businesses and employers' federations representing over 7 million companies provide and receive expertise via our participation with the OECD and governments promoting competitive economies and better business.