Business at OECD Intervention

Thursday, 30 April 2020

Business at OECD Intervention - Delivered by Makoto Yokozawa, Business at OECD CDEP Co-chair

General points

- Business at OECD would like to thank the OECD CDEP Working Party on Security in the Digital Economy (SDE) for organizing this session. In the Covid-19 crisis, where we have seen an acceleration in the uptake of digital technologies and unfortunately also malicious activity.
- Digital security is a top priority issue for business, and business is leading solutions in partnership with governments and other stakeholders.

Risk situation

- Significant shift in global traffic patterns in this crisis – driving demand for connectivity and bandwidth given the swift move to telemedicine, telework, online education....
- Key technologies that have supported this shift have been network, cloud, content and collaboration tools.
- In light of Covid 19 there has been an increase in malicious activity including, hacking, phishing, malware... Users easily open uncertified files, which are pretending to be important messages regarding COVID-19.
- Trendmicro reports 907K spam messages are related to COVID-19 in 1st Quarter 2020. In 2020 Spam has increased increased by 220 times from February to March, 48K malicious URL hits were related to COVID-19 in Q1, and increase by 260% from February to March. ¹
- These activities present significant risks to public health, economies and society, and impede efforts to mitigate the crisis.

Business example – Enhancing digital security in the transition to telework

The ability to rapidly - but securely - transition a workforce to remote work is a critical component of business continuity. The following are three security best practices highlighted by our members in this context:

1. Manage risk by balancing operational needs with appropriate secure connection types following risk assessments by experts
   a. To conserve critical VPN capacity, organizations may reserve the most secure connections for those who require them. When VPN connection is not needed, encourage employees to use (secure) administrative access via portals and/or cloud applications.
   b. Knowledge and experiences must be shared in order to quickly respond to the specific threats in these COVID-19 situation.

2. Apply layered security controls
   a. Leverage tools such as multi-factor authentication and data-at-rest encryption for assets out of corporate control (e.g., desktop computers normally in company facilities). Bring your own device (BYOD) guidelines will have to be revisited.
   b. Readiness and resilience must be reconsidered to meet hidden risks in this situation, including the sharing/portability of experience/knowledge in the organization-specific security management.

3. Ensure communications and training
   a. Conduct telework-specific training regarding cyber threats, and regularly communicate remote work risks and best practices (including updating and patching home computers) to all employees connecting remotely.
   b. The importance of skill development are not limited to employees. Users and consumers are equally requested to consider the risks hidden in the COVID-19 related malicious campaigns.

We also wish to flag a number of policy issues:

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

- Importance of an integrated, multistakeholder policy approach to enhance digital security including the OECD Guidance on digital security risk, Privacy, AI and Enhanced Access to and sharing of data. And the situation requests quick and practical outcomes for short term responses.

- Public private partnership: Policy should support public private partnerships to advance digital security objectives. Regulations must be reconsidered to be much more transparent and understandable for all, if society needs to be regulated in the emergency situation. Critically risk/benefit balance must be re-evaluated to find quick and timely solutions including regulatory sandbox approaches.

- Investment in digital infrastructure: The need to prioritize investments in digital infrastructure, promote capacity building and R&D, supported by coherent regulations on digital

- Training and skills: Need to equip organizations and people with the necessary skills to identify and protect themselves against digital security risk. “Immunity will be required even in cyberspace to be resilient for COVID-19 related malicious campaigns.”

- Information sharing – multilateral approach: Adoption of best practices that allow for voluntary, meaningful information sharing programs through a multilateral approach, to anticipate, mitigate, or manage networks to meet changing demands.

- Workforce: The need for clear consistent definitions of essential critical infrastructure workforce in times of confinement to ensure continued security, availability and maintenance of digital systems.

- Concern that governments do not stockpile or exploit vulnerabilities in the Covid 19 crisis and beyond, and standardization is a product of democratic market-based economies.

We will provide additional input on the digital security issue in writing following this meeting
Business at OECD Member Company Intervention – Kathryn Condello, Century Link

There has been a significant shift in the global traffic patterns over the past few months driving demand for connectivity and bandwidth. The primary ICT entities that supported this shift have been the network, cloud, content, and collaboration providers. These providers have bi-lateral business relationships with each other and work together in the regular course of day-to-day business.

The dynamic nature of these global traffic shifts, however, led to increased voluntary information sharing and operational coordination between these providers that organically evolved the relationship toward multi-lateral discussions. This multi-lateral approach was undertaken to ensure that Industry could anticipate issues and more quickly respond, mitigate or manage our respective networks to meet the changing demands. This same multi-lateral coordination was leveraged to identify and communicate limiting factors to government decision-makers and align government policies as much as possible to mitigate those concerns.

While the global traffic and usage patterns have changed significantly, this usage did not outpace the US networks’ ability to respond. This led to a largely seamless experience for the end user. Governments should adopt best practices that allow for voluntary, meaningful information sharing programs and engage with the business community to ensure that solutions directed at the ICT community are technically feasible, achievable, not cost-prohibitive and does not result in unintended economic or commercial consequences.

Additional references

Regarding Video Conferencing: As a follow up to the final discussion on video conferencing......

https://www.hstoday.us/subject-matter-areas/cybersecurity/to-zoom-or-whatsapp-nsa-lays-out-security-details-of-videoconferencing-services-for-teleworkers/?fbclid=IwAR1a1dlzowLPIHWgjDljzCLuPcILKQqH_iIVMNqIbumeFAQKZc6x5B_ew

Members have suggested the following reference – US National Security Agency guidance as a reference for consideration as OECD looks at the issue of guidance for the security of video conference tools.