BOX 9
Implications of the COVID-19 on Technology Adoption and Cybersecurity

Introduction

During 2020, COVID-19 created an unprecedented change in the lifestyles of people around the world. Demand for traditional goods and services changed significantly with demand for Information Technology related services increasing rapidly. The adoption of these new changes has led to the creation of new markets and opportunities, which have both positive and negative impacts. Two such key issues, which have garnered attention among both organisations and the general public, in the current situation, are cybersecurity and cybercrime.[1]

New Information Technology-based Economic Activities

Mobility restrictions adopted by countries due to the pandemic had led to the emergence of several new trends in the carrying out of conventional economic activities. Some of the key trends, which are mostly dependent on information technology and related services, are listed below.

a) Work from Home (WFH)

During the first wave of the pandemic, most countries did not have significant prior experience or did not possess the readiness to face the novel circumstances arising from the pandemic. In order to curb the spread of the virus, the immediate response across countries was to impose varying degrees of mobility restrictions. The urgent manner in which these were undertaken necessitated the urgent transition of workers from physical places of work to 'work-from-home' arrangements. Neither workers nor organisations were equipped with the appropriate infrastructure for such working arrangements. This dearth was observed not only in terms of equipment, such as laptops, but also in terms of secure access to organisational systems and networks. In addition to the increased use of email and the internet, many organisations immediately adopted the use of Virtual Private Networks (VPN) for this purpose. Further, personal electronic devices were also being used for official work on a large scale within a very short period. Most of these personal devices were not secured adequately in line with industry accepted standards.

b) Online learning

Educational institutions experienced intermittent closures. Accordingly, all educational activities were shifted to online platforms with teaching staff delivering lessons through platforms, such as Zoom and Microsoft Teams. Assignments and other coursework were also shared through these platforms and others, such as WhatsApp, in order to improve the extent of outreach to students. Even pre-school children started having online learning sessions of 30 minutes to 1 hour. This provided the students the opportunity to use internet enabled mobile devices for longer durations than earlier without much restriction or supervision of their parents.

c) E-commerce

Many merchants who relied on conventional sales through physical outlets rapidly adopted online sales platforms. At the same time, customers also rapidly shifted to online shopping due to lockdowns and travel restrictions imposed to prevent the rapid spread of COVID-19. However, such a swift and widespread transition of sellers and customers to online platforms could not be handled by existing systems leading to system downtimes and interruptions. There was also a reduction in the usage of physical money, in light of the pandemic, thereby leading to a surge in online transactions.

d) Online financial services

Most banks and financial institutions (FI) encouraged their customers to use online financial services to minimise their visits to bank branches. This resulted in increased usage of online banking websites and mobile banking applications. People who possessed low levels of IT literacy also had to use these online financial services for their daily needs, and FIs had to relax some restrictions to widen the reach of these financial services.

e) Virtual meetings and conferences due to travel restrictions

With the pandemic induced travel restrictions and social distancing recommendations, many organisations had to shift in-person meetings and conferences to virtual platforms to ensure continuity, increased accessibility and inclusion. Although online meetings were not an entirely novel concept, it was a relative new experience for a substantial segment of workers. As different organisations used different tools for this purpose, it posed several challenges to data security. A wide range of confidential information including intellectual property and trade secrets had to be shared online and most meeting hosts and participants were not aware of security measures which were essential to preserve the confidentiality of meeting proceedings.

[1] Cyber security is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from attack, damage, or unauthorised access. Cybercrime is any criminal activity that involves a computer, networked device or a network. While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them, while others use computers or networks to spread malware, illegal information, images or other materials.

Cyber Criminal Activities amidst Pandemic-Induced Online Activity

a) Phishing emails

Work-from-home arrangements have provided several opportunities for cyber criminals to launch different types of cyber-attacks. Such attacks began with phishing or spam emails, which lure email users to disclose sensitive and confidential information to an unknown third party without their knowledge. Phishing emails have been created targeting a specific group of people or organisations. The sophistication of such phishing emails has increased to the extent that they can surpass spam filters. Through the collection of confidential information from these phishing mails, they were able to plan and execute cyber-attacks to business-critical systems and gain financial benefits.

b) Device sharing and free/cracked software

Many students have to use their parents' devices for their studies and cyber attackers have launched specific attacks targeting these students. Children tend to visit malicious websites, download and install free software and games to these devices. Such freeware come with malware used for different purposes, such as stealing information, key logging[2] and acting as bots[3] that initiate cyber-attacks on other devices connected to the internet.

c) Fake websites/apps

The boom of e-commerce has made it easy for cyber criminals to steal customers' sensitive data, such as credit card details by sending spam emails and setting up fake websites or mobile apps pretending to be an online store, banking website etc. Some organised criminals steal sensitive data from victims and create online banking profiles for accounts that belong to the victims and steal money from these accounts.

d) Loss of information security focus

With the sudden increase in demand for work-from-home arrangements, remote access and other needs, many organisations have lost focus on information security amidst trying to cope up with this surge in demand. When information security professionals also work from home and their focus is also diverted towards these new challenges, general work related to cybersecurity (system updates, patch management, log monitoring, and forensic investigation of security incidents) go unattended paving way for circumstances that provide a good opportunity for the cyber-attackers.

Way Forward

The pandemic could prevail for a while, but the implications of the pandemic would linger on for several years to come. Therefore, it is vital for organisations to have short-term, medium-term and long-term plans to progress in line with the new norms and enhance cybersecurity and cyber resilience.

a) Strengthen cyber resilience

Sophistication of cybercrimes is continuously on the rise and even organisations that have adopted very high levels of cybersecurity measures have not been able to assure that they are fully secured against cyber-attacks. It is believed that some malware can stay undetected in an organisation's network for very long periods, as much as 240 days before an actual attack. Therefore, most organisations tend to concentrate on achieving cyber resilience, which ensures that the organisation could resume its normal operations with minimal disturbances subsequent to any cyber-attack related disruptions to IT systems. Developments in the IT infrastructure industry, including cloud computing, have enabled businesses to achieve the required business resilience.

b) Business Continuity Planning (BCP) for pandemic-related circumstances

It is mandatory for many industries, including the financial sector, to plan, test and implement business continuity programmes. Many of these BCPs cover test scenarios, such as natural or man-made disasters, technical failures, etc. However, it was observed that pandemic related BCPs had not been implemented or tested in many organisations. A pandemic is a special scenario where physical accessibility to information systems is not possible due to lockdowns and thereby the potential unavailability of key personnel. Organisations may not have enough information security professionals to duplicate or share roles. If these employees are affected by these unusual circumstances, it would create a vacuum in that particular area of work. Therefore, it has become essential for organisations to include remote working arrangements and adequate human resources in their business continuity planning.

c) Allocate adequate budget

With the new norms of work-from-home, it has been extremely difficult for organisations to protect their information systems as done in the past through restricted access and other stringent controls. While allowing these new facilities, organisations should implement immediate and long-term plans to protect their IT assets. Cybersecurity comes with an enormous cost that even large-scale organisations struggle with when deciding on budget allocations for information security. Cooperation among organisations, within a specific sector, to share information security related resources would be beneficial for all in the long term. In

[2] The practice of using a software program or hardware device (keylogger) to record all keystrokes on a computer keyboard, either overtly as a surveillance tool or covertly as spyware

[3] A software program that can execute commands, reply to messages, or perform routine tasks, as online searches, either automatically or with minimal human intervention

the short term, organisations should increase their focus on maximising the usage of available cybersecurity resources to protect their IT assets.

d) User awareness

User awareness can be considered as the most important part of cybersecurity, as it is the users who create system vulnerabilities that pave way for the entry of cyber criminals to enter into the organisational systems. The demarcation between official and personal tasks seems to have disintegrated as observed in the use of personal devices for official work and vice versa. Hence, this too, is a risk to cybersecurity if such devices are not maintained properly with the required security features. Users are often unaware of these risks. This puts the onus of awareness on cybersecurity and staying safe on all individuals. Organisations must focus more on creating user awareness among employees. Schools and universities should also do the same.

e) Working closely with National Computer Incident Response Teams (CIRT)

Most of the countries have established National Computer Incident Response Teams (CIRT) that serve as the national focus point for coordinating cybersecurity incident responses to cyber-attacks within a country. Sri Lanka Computer Emergency Readiness Team Coordination Centre (Sri Lanka CERT) is the national CIRT for Sri Lanka and their mission is to protect Information Technology users in the public and private sector organisations and the general public by providing up-to-date information on potential threats and vulnerabilities and by undertaking computer emergency response handling services. Therefore, any individual or organisation can obtain their services and consultancy in relation to cybersecurity when required.

Conclusion

Cybersecurity should be made a topic of the boardroom and given extra attention considering the growing threats during the pandemic. While going through the second wave of the pandemic and with concerns of a possible third wave, every organisation should implement preventive measures for cyber-attacks while strengthening cyber-attack detection, response and recovery capabilities. It is the responsibility of every individual and management to protect themselves and their workplaces from cybercrimes in today's connected world. At the same time, a collective approach is required at organisational, sectoral, national and international levels to fight against cybercrimes and build a safer world for the present and future generations.