ASIAN BANKING SCHOOL

Let's Talk Digital Series #16

Cybersecurity Challenges for Banks During the Pandemic

CYBERSECURITY CHALLENGES *FOR BANKS DURING THE PANDEMIC*

The COVID-19 pandemic has greatly impacted banking and financial services. On top of handling the direct economic impact of the pandemic, banks are now required to implement strategies to protect employees and customers from the virus that is spreading. Many of the banks are already encouraging employees to work remotely, and customers who are becoming increasingly cautious about spending time in public spaces will also need a way to conduct their banking without physical interaction.

This can be achieved through digitization of banking processes such as financial transactions processing, application process for new accounts, stock trading, and more. In fact, digital banking has become a sustainable business model that allows the financial industry to keep up in face of the pandemic, and many banks are now fast-forwarding their digital transformation plans to adjust to the new normal of 'Work-From-Home' and 'Contactless Banking'.

The accelerated adoption of digitization plans brings about new risks that will challenge the current defences in banks. Hackers are also actively looking for ways to take advantage of the pandemic as banks have to immediately implement plans for remote working and contactless banking in a short time and at a scale which they have not experienced before.

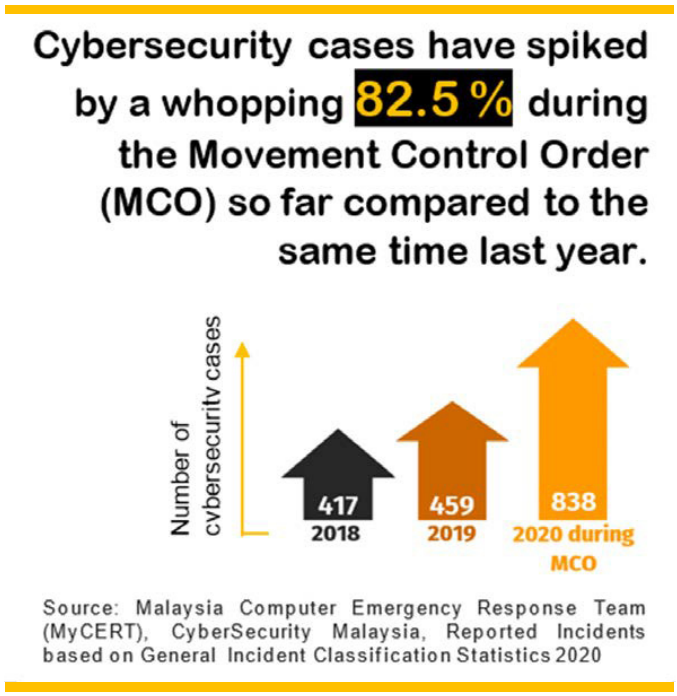

Figure 1: The number of cybersecurity cases reported in Malaysia from year 2018 to year 2020.

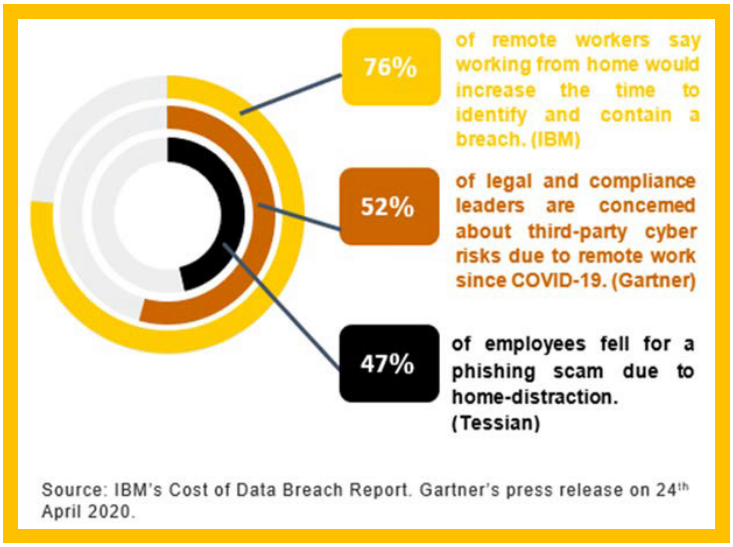

Figure 2: Cyber risk statistics during the pandemic.

Many organizations are raising concerns on the cybersecurity risks arising from the implementation of remote working policies that targets a large number of employees. In addition to risks from an internal perspective, banks have to also manage possible risks associated with the digitization of banking processes for their customers at an external perspective. Hence, banks need to start identifying the risks involved when adjusting to the new normal in light of the pandemic.

Figure 3: Common internal and external risks faced by banking institutions during the pandemic.

Banks should also consider implementing mitigation controls to manage the risks in conjunction with the adoption of remote working plans and contactless banking.

Figure 4: Suggested mitigation controls to reduce the impact of cyber threats

Banks will need to ensure that all required controls are in place when rolling out technologies for remote working. Employees that are working from home should be required to activate VPN and use MFA to access the internal network and any critical applications. In addition to patching the existing critical systems, technologies used for remote working should be constantly patched and updated to ensure that vulnerabilities are eradicated accordingly after discovery. The rollout for these updates can be planned to follow the criticality of the system and the severity addressed by the update to reduce network congestion.

As most banks employ a diverse number of vendors under their organizations, it is also crucial for them to ensure that vendors are practicing due diligence in ensuring adherence to good security practices. On top of stronger technology controls, banks should find ways to increase security awareness in bank employees and customers, particularly on social engineering due to the surge of COVID-19 campaigns during the pandemic.

The pandemic outbreak presents unique challenges and new means of effect given its global repercussions and potential duration. It has brought new challenges for digital banking services, and also an opportunity for banks to gain a deeper understanding of their own cybersecurity environment.

References

1. Malaysia Computer Emergency Response Team (MyCERT), CyberSecurity Malaysia, Reported Incidents based on General Incident Classification Statistics 2020. Retrieved from https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=b9018870-c2a0-4b64-912d-39f65600abb8
2. IBM Security, Cost of a Data Breach Report 2020. Retrieved from https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
3. Cybersecurity and the COVID-19 pandemic. Retrieved from https://www.lexology.com/library/detail.aspx?g=8b5940c3-55b2-4c48-982c-546e956906cd

ASIAN BANKING SCHOOL

This article is part of the Digital Banking Learning Series, 'Let's Talk Digital', an initiative by the ABS Center for Digital Banking. It is written by industry practitioners and are aimed at educating the general public on the intricacies of digital applications in banking and other related industries, including the latest insights and trends of Digital Banking.

As the industry's preferred partner in learning and development, ABS offers relevant training programmes that covers a comprehensive list of banking areas that are designed and developed in-house by our Specialist Training Consultancy Team or in collaboration with strategic learning partners that includes some of the top business schools in the world. It also provides specialised consulting services and tailored learning solutions to meet the specific needs of its clients.

For more information, visit our website at **www.asianbankingschool.com** or email us at **digitalbanking@asianbankingschool.com**