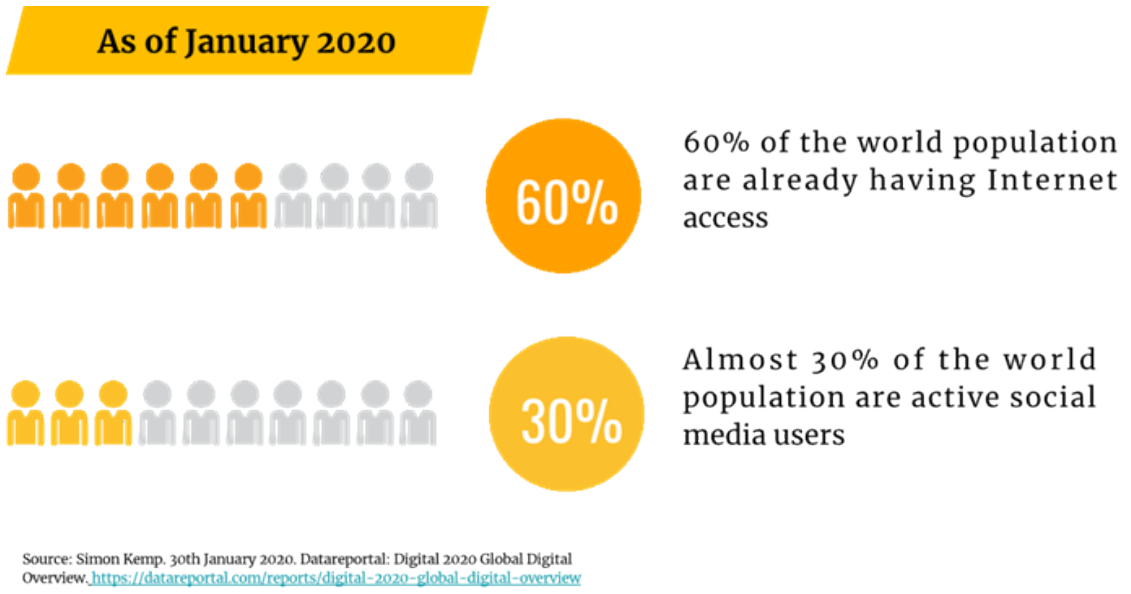
ASIAN BANKING SCHOOL

Let's Talk Digital Series #2

The Paradigm Shift of Cybersecurity in 2020

In the 21st century, computers and a plethora of Internet connected devices are dominating the modern society. I personally believe that we are living in one of the greatest times for mankind, where information is gold and virtually everything is accessible at the tip of our fingers.



Source: Simon Kemp. 30th January 2020. Datareportal: Digital 2020 Global Digital Overview. https://datareportal.com/reports/digital-2020-global-digital-overview

With integration of the Internet into our daily lives, what we used to know about business and life has drastically changed over the last two decades: the largest retail stores in the world today are no longer in physical forms, communications are no longer confined to telephones, private transportations are now shared, food are delivered to our doorsteps with just a click of a button. Our wealth is essentially just a set of digits recorded in our mobile phones.

Technologies are shaping our culture, life and even our behavior. Unfortunately, technology has not done much in helping us remodel how we perceive personal security, especially digital security while using the Internet.

CYBER CRIMINALS TODAY

When I first set foot in Makati City, the Philippines during a business trip back in 2004, I was told that the city has the lowest bank armed robbery rates in Asia. I have to agree, because everywhere I went, I can see armed guards operating at almost all business premises. Even the security guards at Starbucks were holding a double barrel shotgun. These are strong deterrent signs to anyone who has the slightest thought of doing something dumb.

Moving forward in time, some of the largest bank heists today are done purely online; it is clean, swift and efficient.

Many business operations have moved online, such as e-commerce stores, financial services, education, gaming, healthcare, call centers and so on. The trend also signifies the need for business owners to realize that they are now facing a whole new battle ground since catching a thief is no longer as simple as applying brute force.

A whole new set of strategies and tactics need to be redefined accordingly.

Throughout the articles of this series, I will be introducing concepts that may illuminate in high contrast against our conventional beliefs about Security, particularly Cyber Security.

PARADIGM SHIFT NO.1: "THE BAD GUYS ARE OUT THERE"

Ever since we were in our adolescence, we have all been taught the same doctrine that the "Bad guys" are out there. This belief is taught universally, regardless of your religion, creed, education level or culture. It is not too much to assume that we still have this same belief firmly injected into our DNA, even passing the same belief onto the next generations.

Source: Nucleus Cyber 2019 Insider Threat Report, conducted with Cybersecurity Insiders.

Our principal design for security is to put the focus on protecting us from External Threat. While the principal still holds true today, we are merely focusing on the threat of infiltration and missing out on a very important part: the Exfiltration – a scenario where the bad people have already come into our houses, and are moving our valuable information assets out from it.

The questions that we need to ask ourselves today is no longer about infiltration, it is more about our contingency readiness – are we capable to detect and respond if the enemies have already infiltrated our protected realm?

PARADIGM SHIFT NO.2: "I HAVE NO VALUABLE INFORMATION TO BE STOLEN"

Let's be honest, not every one of us think that we have information that is worth any value. Some of us just live by a simple Cyber Lifestyle: we use messenger to communicate with friends and family; we read our social media postings and shop online occasionally; some of us do not even trust online banking, so we do not even have any online bank accounts.

Now, if you fit into the profile above, you are already amongst the 5.19 billion Internet users who are subjected to online fraud and scams.

You may feel like you do not have any 'valuable' or 'sensitive' information to be stolen, however, people on your phones' contacts lists and social media accounts do: their names, phone numbers, and email addresses can all be used by Cyber criminals to formulate Cyber-attacks, especially online fraud.

PARADIGM SHIFT NO. 3 "MY COMPUTERS ARE STRICTLY USED FOR WORK ONLY"

This may be true. However, if your computers are connected to the Internet, you may have something that is equally, if not more valuable: your network bandwidth.

- Malicious hackers are hacking into computers to install backdoors that can be used to facilitate their attacks.
- These backdoors allow the hackers to take full control of the compromised computers and also control the computers to perform Cyber-attacks for them. When all these compromised computers are grouped together, the hackers can form a Bot-Net (a network of "Robots").
- The "Robots" infected computers can function as normal computers without the owners noticing any differences.
- These computers will also allow hackers to go in and out as and when they like; whilst listening for the command from hackers to launch Cyber-attacks against the target.

CONCLUSION

There seems to be a lot of information to be consumed at one go, I hope the examples above can give everyone a jolt in their common belief system of what Security is about.

In my following articles, I will continue to elaborate about the paradigm shifts we have to adapt to in order to meet the ever-growing Cyber Threats in our digital life.

Cybersecurity may seem to operate like conventional physical security, but the truth is that managing Cybersecurity is far more challenging in comparison.

Our assailants today are coming from all over the world. We are in a constant loop of a rat and cat chase; it will never end. We need to regularly assess our security postures to adapt to new technologies, to ensure that we are always staying ahead of Cyber criminals.

Let's start by changing the way we perceive Cyber Security, learn and adapt to the new digital paradigm of the 21st century.

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**