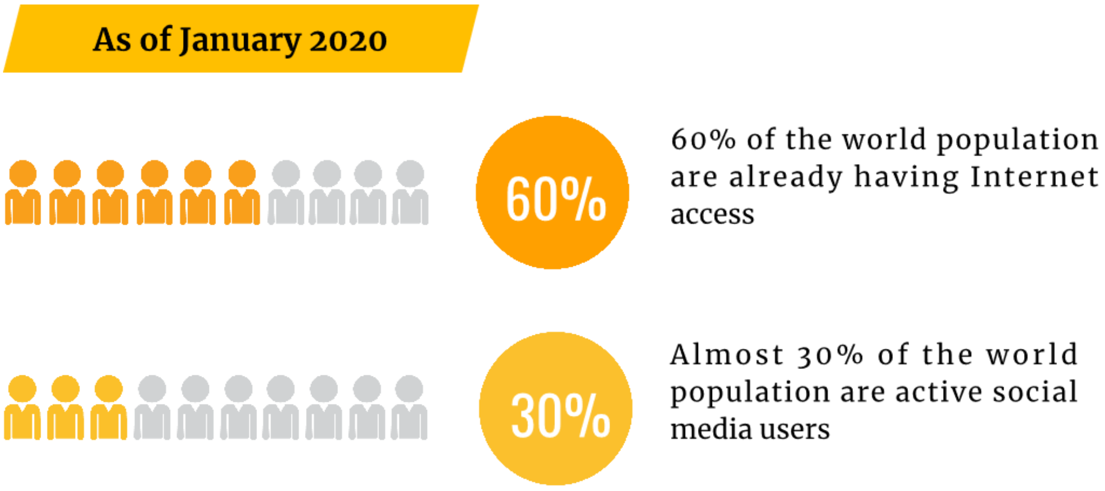
PART 1 OF 2

THE NEW CYBERSECURITY PARADIGM SHIFT IN 2020

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



As of January 2020

60% of the world population are already having Internet access

Almost 30% of the world population are active social media users

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

With the integration of Internet into our daily life, what we used to know about business and life have 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 essentially just a set of digits recorded in our mobile phones.

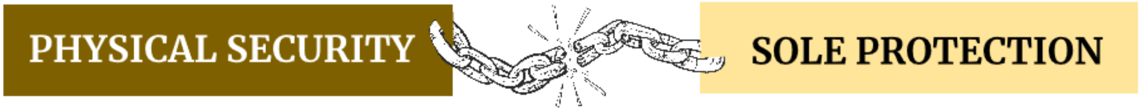
Technologies are shaping our culture, our life and even our behavior. Unfortunately, technology has not done much in helping us to re-model how we perceive personal security, especially our digital security when we are using the Internet.

CYBER CRIMINALS TODAY

When I first step 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 all most all business premises. Even the security guards at Starbucks are holding a double barrel shotgun. These are strong deterrent signs to anyone who has the slight idea 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.

WHEN BUSINESS OPERATIONS MOVED ONLINE



Many business operations have moved online, such as e-commerce stores, financial services, education, gaming, health care, 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, catching a thief is no longer as simple as applying physical brute force.

Assailants are now coming from **ALL OVER THE WORLD**

A whole new set of strategies and tactics need to be re-defined accordingly.

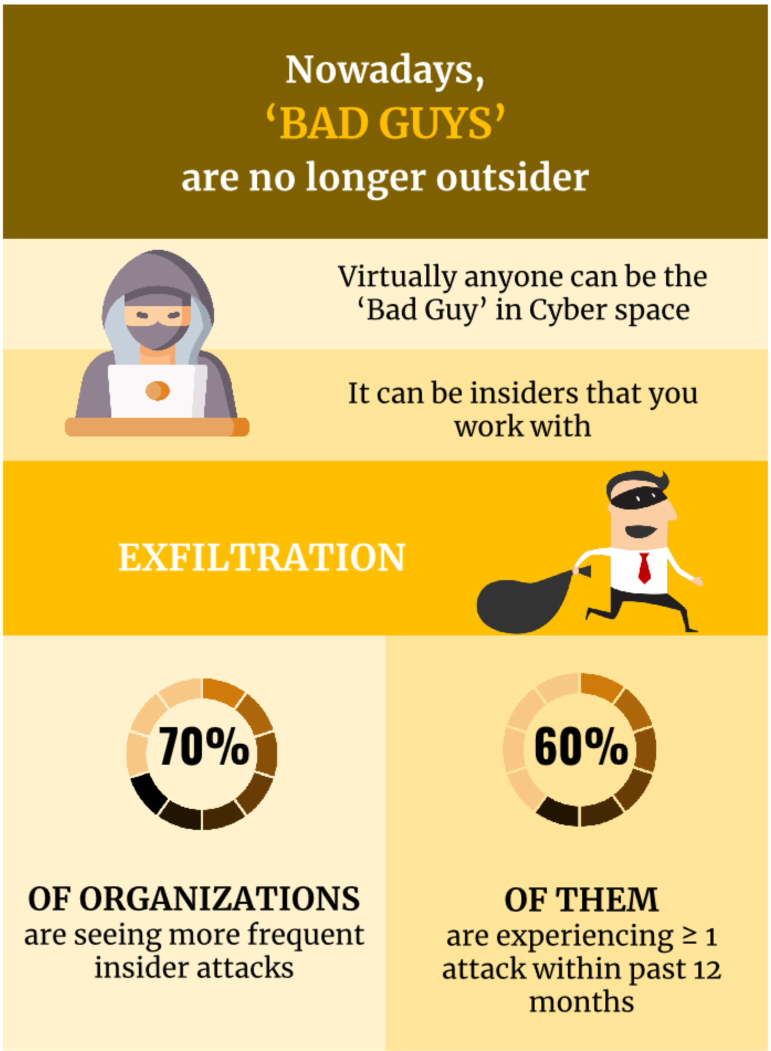
Throughout the articles of this series, I will be introducing concepts that may illuminate in high contrast against out conventional believes about Security, particularly Cyber Security.

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

Since we are in our adolescents, we have all been taught under the same doctrine that the “Bad guys” are out there. This believe is taught universally, regardless of your religion, creed, education level or culture. It is not too much to assume that we are still having this same believe firmly injected into our DNA, even passing the same believe onto our next generations.

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 just merely focusing the threat infiltration and missing out a very important part: The Exfiltration – a scenario where the bad people already came in to our house, and moving our valuable information assets out from our house.

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 are already infiltrated into our protected realm?


Nowadays,
‘BAD GUYS’
are no longer outsider

Virtually anyone can be the ‘Bad Guy’ in Cyber space

It can be insiders that you work with

EXFILTRATION

70%

OF ORGANIZATIONS are seeing more frequent insider attacks

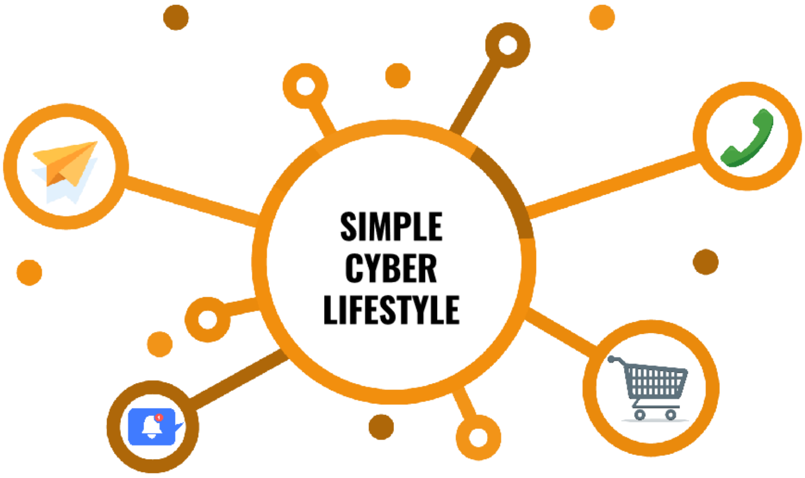
60%

OF THEM are experiencing ≥ 1 attack within past 12 months

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

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

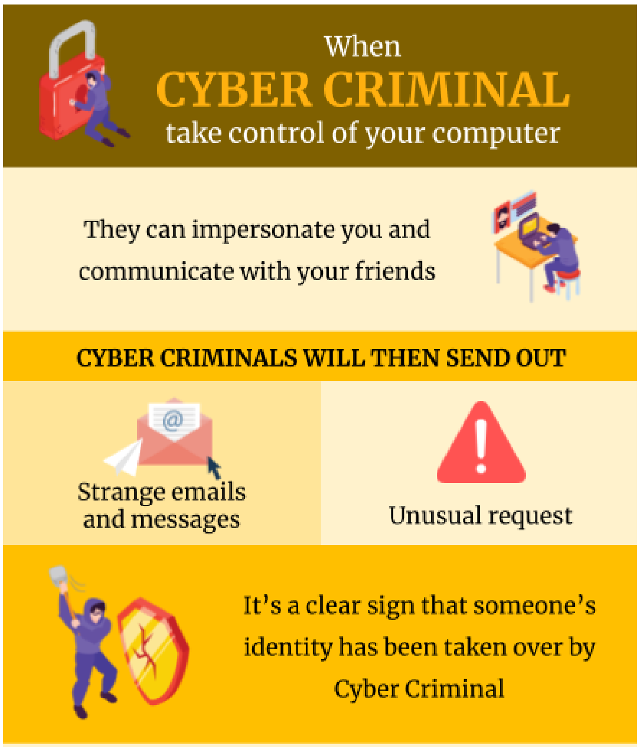
Let's be honest, not everyone of us think that we have valuable information that worth any values. Some of us just living by a simple Cyber Lifestyle: we use messenger to communicate with friends and family; we read our social media postings and shop on line occasionally; some of us do not even trust 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 subject 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' contact lists and social media accounts: their names, phone numbers, their e-mail addresses – all can be used by Cyber criminals to formulate their Cyber-attacks, especially online fraud.

In the Cyber world, our digital identities are just merely our user name and passwords. Once we lose control of these credentials, we lost our identity.



When
CYBER CRIMINAL
take control of your computer

They can impersonate you and communicate with your friends

CYBER CRIMINALS WILL THEN SEND OUT

Strange emails and messages

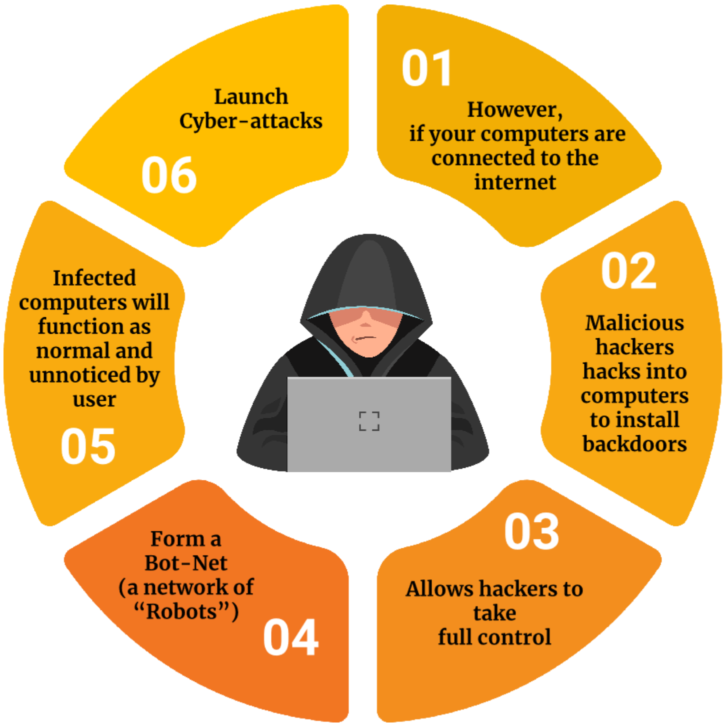
Unusual request

It's a clear sign that someone's identity has been taken over by Cyber Criminal

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 use to facilitate their attacks.
- These backdoors allow the hackers to take full control of the compromised computers, also control the computer 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 will can function as normal computers without the owner noticing any difference, but unknowingly to the owners.
- These computers will also allow hackers to go in and out as and when they like; whilst listen for command from the hackers to launch Cyber-attacks against the hackers’ target.



CONCLUSION

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

In my following articles, I will continue to elaborate about the paradigm shifts we have to adapt 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 loop of constant rat and cat chase; the loop will never end. We need to regularly assess our security postures adapt to new technologies, to ensure that we always staying ahead against the Cyber criminals.

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