

# LET'S TALK DIGITAL

JUNE 2020

ASIAN  
BANKING  
SCHOOL

## CONTENT



### **DIY Guide on Implementing Data Science Project**

*Koh Wyhow*



### **The Paradigm Shift of Cybersecurity in 2020**

*Fong Choong Fook*

**Let's Talk Digital is a monthly newsletter that was created to build awareness on Digital Banking and provide a platform for industry practitioners to share insight and current trends on this exciting subject matter in relation to the Banking and Finance industry.**

## **A DIY Guide to Implementing Data Science Projects**

**By Koh Wyhow**

Data science is an upcoming field which attracts a lot of interest among the public. This trend has been keenly followed by tertiary education institutions, private training agencies, and online providers which offer courses to those interested in combining their domain expertise and data analysis. This article explains that data projects are not merely about coding - they also include building a business case, a proof of concept, and testing, which tend to come only with working experience.

## **The Paradigm Shift of Cybersecurity in 2020**

**By Fong Choong Fook**

Everyone is living in a century where modern society is dominated by computers and Internet connected devices. It has since created momentum for these businesses to step into the online world. Unfortunately, this has also introduced a doorway to numerous cyber threats towards their business, paving the way to a whole new cybersecurity paradigm shift.

The article explains how the shift has affected everyone throughout the entire world in our present year, 2020.

**To find out more about the Digital Banking programmes that ABS offers, visit**

**[www.asianbankingschool.com/our-programmes/centre-for-digital-banking](http://www.asianbankingschool.com/our-programmes/centre-for-digital-banking)**



## Koh Wyhow

Koh Wyhow is the manager of the data science team at Star Media Group Berhad. He focuses on delivering advanced analytics and business intelligence solutions for the organisation like chatbots and image recognition solutions. He consulted for client in the airlines, media, property, and FMCG industries during his time as a senior consultant at EY's Data and Analytics team.

He was one of the data scientists which implemented strategies to run a national data-driven campaign for INVOKE in the 14th General Elections. As an independent learner, he picked up basic Python programming skills after office hours during his days as a Further Mathematics lecturer at a private college. Wyhow holds a BSc in Mathematics from the National University of Singapore.



## Fong Choong Fook

Fong has strong working relationships with various law enforcement agencies worldwide, as a trusted figure in the information security arena; he is also the distinguished guest speaker for The Federal Bureau of Investigation (FBI) INFRAGARD event, Polis Diraja Malaysia (PDRM) Info Security trainings and various industry associations, governments and law enforcement agencies on Cyber Security Topics.

Fong is the author of the "Certified Lead Forensic Examiner" (CLFE) courseware for Professional Evaluation and Certification Board (PECB [www.pecb.org](http://www.pecb.org), USA). The CLFE course is currently distributed worldwide by PECB in training information technology professionals in conducting computer crime investigations and digital forensic.

Fong also has had experience to be called as an Expert Witness to study, assess, evaluate and testify in the court of law.





I'll start by breaking down the first myth. Coding does look intimidating in the beginning, especially if one has no programming background. There are two skills every good coder has: the patience to read and understand code documentation, and the ability to break large problems into smaller solvable bits. Most codes available online have some sort of documentation which describe what each parameter supplied by the user does. As for decomposing large problems into several ones, a lot of us have done it before. For example, organising an event like a conference requires several steps:

1. Getting a venue
2. Booking caterers for food and beverages
3. Confirming agenda and speakers
4. Trial run of events to make sure everything runs smoothly

The second myth is about the expensive setup and infrastructure costs, which can largely be addressed via cloud computing platforms. Organisations in the airline, media, and e-commerce platforms rely on the likes of Google Cloud Platform and Amazon Web Services because these services allow users to quickly experiment and test the feasibility of deploying their code for internal or external use quickly.

As for the third myth: for people to work as data scientists, they require a few components:


1. Proficiency in mathematics, statistics, or computer science
2. Soft skills for presentations and stakeholder management
3. Domain expertise



Data science is applicable in various industries but those with in-depth domain expertise will have better understanding of what the data means and will be able to manipulate data to come up with better machine learning models. For example, a data scientist with little domain expertise will fit a regression model to find the relationship between annual GDP, and variables like consumer expenditure household, total goods and services exports, total imports goods and services etc. Someone with domain expertise would know it's better to use variables like total exports, total imports, and domestic demand per GDP without construction.

# CLOUD COMPUTING PLATFORMS

Let's assume I'd like to build an image recognition system which recommends recipes based on user-submitted images. Here are the comparative steps I'd take to deploy an image recognition system.

ONSITE SERVER	CLOUD DEPLOYMENT
<p><b>1</b> Build image recognition algorithm, and house within a server</p>	<p><b>1</b> Build image recognition algorithm, and place the code in a virtual machine</p>
<p><b>2</b> Estimate the incoming number of images to determine the hardware specifications needed</p>	<p><b>2</b> Choose the appropriate virtual machine specifications, enable scaling options, and select region where images would be stored</p>
<p><b>3</b> Estimate the software license and hardware costs, power consumption, etc.</p>	<p><b>3</b> Control access to the core code by assigning permissions to user IDs like how it's done on Google Docs</p>
<p><b>4</b> Backup plan in the event of server maintenance and upgrades</p>	
<p><b>5</b> Ensure security steps taken are adequate for data protection</p>	

There are a few advantages of cloud computing platforms.



### MAINTENANCE AND BACKUPS OUTSOURCED

Hardware maintenance and software backups are outsourced to the cloud computing service provider.



### FREE CREDIT

All cloud computing platforms also provide users with some free credit for users to experiment with, so users can rapidly test and conclude whether their deployments are feasible.



### REDUCED WASTE CAPACITY

Onsite servers tend to be underutilised outside of peak hours, so the extra capacity is wasted.

Cloud computing platforms give the option of scaling services according to usage, so wasted capacity is reduced.

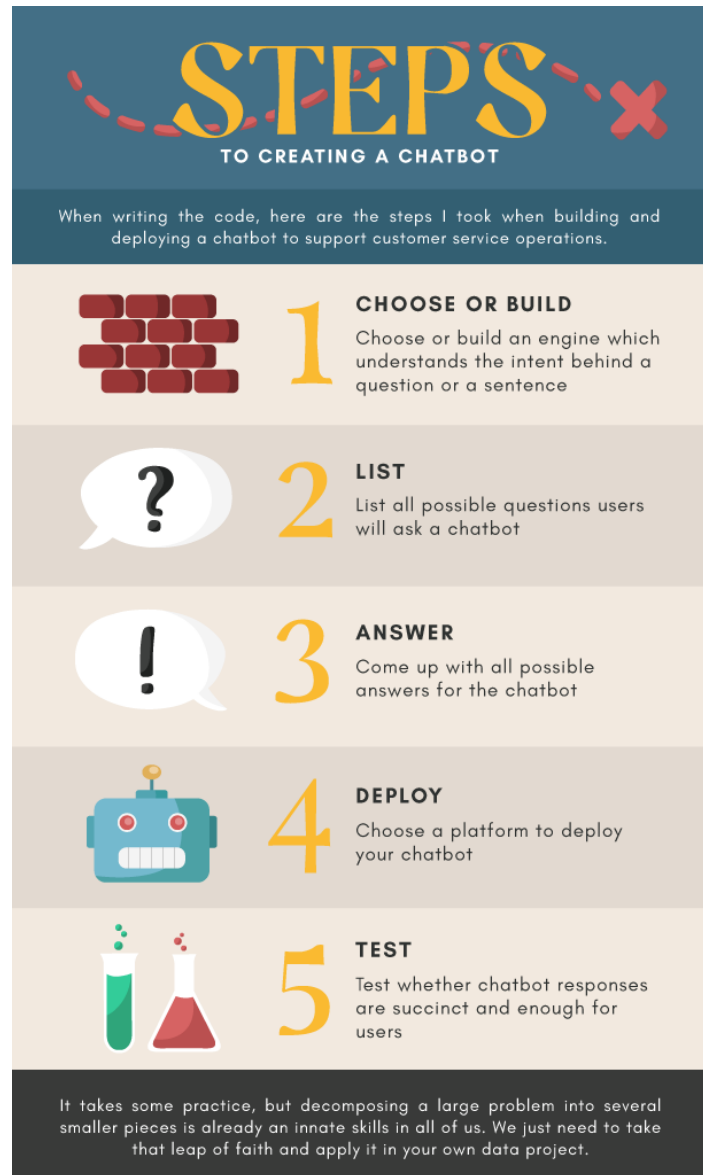


### SOFTWARE ONLY

If I were to build, test, and deploy an image recognition system, I would be able to complete the end-to-end construction within a few days, as my development work would focus only on the software side.

It's more effective for someone already familiar with the industry or domain to pick up data science skills, compared to someone already familiar with data science to pick up domain expertise over time. Here are a few more examples of roles where data science skills can be paired with and applied:

1. Financial Planning & Analysis: estimate marketing expenditure in a given city by predicting the number of new users of an app/product.
2. Sales: classify and segment their customers based on creditworthiness using historical patterns of credit term, payment frequency, amount of orders, etc.
3. Risk Management: provide early warning predictions of potential defaults, loan delinquency, and customer churn (whether these customers will change banks soon)
4. Customer Service: provide valuable input onto constructing a chatbot to address customer needs and inquiries, and advise customers through certain steps



If you are still keen to implement your own project whether to help your team manage their workload better or to increase efficiency, here are the 4 steps I usually take to implement data projects:

1. Assess talent within team/organization
2. Identify use case, perform business and technical diligence
3. Build proof-of-concept and gain confidence among stakeholders via insights
4. Scale up project, test results, and productionalize

For the initial assessment, I try to find out whether I have people I can count on for advice in the organisation. It's entirely possible that you want to effect the change, but lack the technical know-how of what to do or what services are needed.

Granted that you'll be doing most of the grunt work, it's easy to gain allies when you can demonstrate a clear advantage / value proposition. If your organisation doesn't have a data team in place, you're going to need to rely on your network of friends, or those in the IT department for advice. If your organisation already has a data team in place, your journey will be easier as you can ask them for guidance.

The next step is to identify a use case, and to perform the business and technical diligence. A few examples of solid use cases would be:

1. Build a chatbot to reduce lag time to customer inquiries to a few minutes from 3 days
2. Construct an Optical Character Recognition (OCR) system to speed up information retrieval from physical documents within a few seconds from a few days (from data entry work)
3. Automatically recommend products for cross-sell/upsell to customers periodically by inferencing from their demographics, daily transactions, web activity, etc.

Any successful experiment requires a proof-of-concept: basically, a simple version of the code which works. Going back to my image recognition system example, the proof-of-concept would be to demonstrate the code works on my computer, and the approximate accuracy based on real world input. The code should work by considering images which come in that have various resolutions, lighting conditions, background noise, etc. You should test extensively to find out the weaknesses of your code. Once you have a functioning proof-of-concept and a few thoughts on how to address the weaknesses of your code, the hard part of convincing your stakeholders to invest time and money into your project begins.

The last phase of the project would involve stakeholders like Management, Corporate Communications, and IT for purposes ranging from ensuring the correct message is reflected on your system/app, end-to-end integration with your organisation's systems, and budget approval. Most data professionals are under the impression that the technical bits are the most difficult part of their job. I can attest that it's not: it's the stakeholder engagement and management which takes up the most of my time.

The past 4 years have been an adventure for me: from exploring and using Microsoft Azure for database operations during my INVOKE days, developing and deploying image recognition and chatbot systems for enterprises, and now exploring applications of augmented reality systems for applications in the media industry. I've learnt a lot of what I know with minimal guidance from my peers, and I hope you will be able to leverage the expertise among your own social circles to implement your own data projects. One of my observations is those who excel in their careers tend to invest a lot of their time learning new skills and exploring new fields. By highlighting interesting facts from my readings, studies and observations from my career, I hope these pointers inspire you to be better in your respective careers.



# PERFORMING BUSINESS AND TECHNICAL DILIGENCE

WHEN IMPLEMENTING A DATA SCIENCE PROJECT

What do business and technical diligence mean?

## BUSINESS DILIGENCE

- 1) Researching on whether others have implemented similar systems;
- 2) Learning from their lessons; and
- 3) Estimating the effort and costs needed to achieve the business value intended.

## TECHNICAL DILIGENCE

- 1) Knowing which systems or platforms to integrate to realise your goal;
- 2) Experimenting and estimating the possible margins of error, false positives, and false negatives; as well as
- 3) How well your solution integrates with existing systems.

Assuming I'm building an image recognition system, here are the questions I would seek to answer.

## BUSINESS DILIGENCE



**1** Have others tried using image recognition to recognise ingredients?



**2** How successful are these systems, and how much value did they bring to their business?



**3** What are the costs and effort needed to develop such a system?



**4** How much value does this create for your business?

## TECHNICAL DILIGENCE



**1** What's the most efficient way to build the script? Does it require building from scratch, or can I rely on a few public APIs?



**2** Once the first code is created, how do I construct the pipelines to feed real-time data? How do I deploy this model, and where will the code output be used?



**3** Using your proposed solution, what are the limitations of your code? Under what conditions will it function well or poorly?



**4** Can the code be integrated with existing systems?

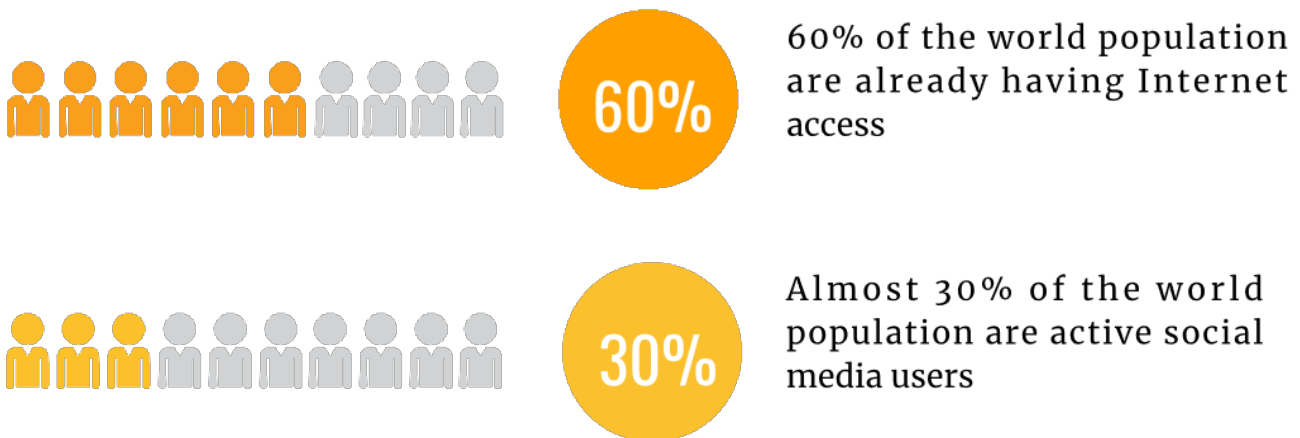
# THE NEW CYBERSECURITY PARADIGM SHIFT IN 2020

## PART 1 OF 2

By Fong Choong Fook

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.

AS OF JANUARY 2020



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.

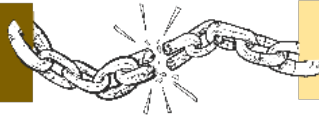
## CYBER CRIMINALS TODAY

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.

## WHEN BUSINESS OPERATIONS MOVED ONLINE

PHYSICAL SECURITY



SOLE PROTECTION

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.



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

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.

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.

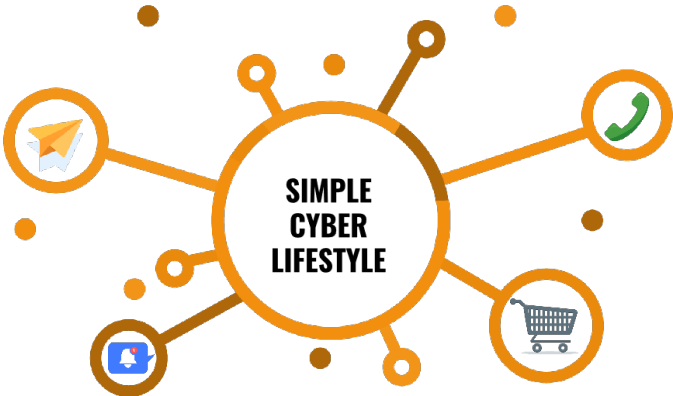
The questions that we need to ask ourselves today is no longer about infiltration, it is more about our contingency readiness – are we capable to detect and respond if the enemies have already infiltrated our protected realm?



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 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.



Assuming you are living with a simple cyber lifestyle, then you are amongst the **5.19 BILLION** Internet users subjected to **ONLINE FRAUD** and **SCAMS**

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.

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

The flowchart is set against a dark olive green background. At the top, it says "When **CYBER CRIMINAL** take control of your computer" next to an icon of a red padlock being broken. Below this, a light yellow box contains the text "They can impersonate you and communicate with your friends" next to an icon of a person at a computer. A yellow bar below that reads "CYBER CRIMINALS WILL THEN SEND OUT". This is followed by two light yellow boxes: "Strange emails and messages" with an icon of an envelope, and "Unusual request" with a red warning triangle icon. At the bottom, a yellow box says "It's a clear sign that someone's identity has been taken over by Cyber Criminal" next to an icon of a person in a blue suit holding a shield.



**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.

**For training enquiries, please contact:**

Asian Banking School (201201039737)  
Level 12, NU Tower 2, Jalan Tun Sambanthan Kuala Lumpur Sentral  
50470 Kuala Lumpur, Malaysia

**Tel :** +603-2742 7822 **E-mail :** [digitalbanking@asianbankingschool.com](mailto:digitalbanking@asianbankingschool.com)

 Asian Banking School

 Asian Banking School (ABS)

[www.asianbankingschool.com](http://www.asianbankingschool.com)