



LEVEL 7 ASSESSMENT SPECIFICATION

Student name:	Lam Wai Yeung	Student ID number:	1913636
Programme:	MBA		
Module:	Leading and Managing Projects		
Module code:	BMMB7010	Contribution to Overall Module Assessment (%):	100%
Lecturer:	Dr. Joe Leung	Internal Verifier:	Dr Poon Che Cheong
Assignment Title:	How Cathay Pacific Airways Ltd improve its cybersecurity control after impact on 2018	Word count (or equivalent):	4,000 words (project report)
Submission deadline:	4 May 2020	Return date of provisional marks & written feedback:	25 May 2020
Submission method:	All written assessments, where practical and possible, must be submitted via Turnitin unless otherwise instructed by the Lecturer. (Please DO NOT put this assessment specification into Turnitin or it will match many similarities with other students' submissions.) Late submission of the assessment will result in a late penalty mark. Penalties for late submission: Up to one week late, maximum mark of 50%. Over one week late, 0%. Only the Extenuating Circumstances Panel may approve a change to submission dates.		
Academic honesty / referencing:	Academic honesty is required. In the main body of your submission you must give credit to authors on whose research and ideas your work is based. Append to your submission a reference list that indicates the books, articles, etc. that you have used, cited or quoted in order to complete this assessment.		

UWTSD MBA (May/Nov 2019 intakes)

BMMB7010 Leading and Managing Projects

Assignment Title:

How Cathay Pacific Airways Ltd improve its cybersecurity control after impact on 2018

“I, Lam Wai Yeung, certify this work is the result of my own investigations, except where otherwise stated. All references have been duly cited”

Signed: *Marco Lam*

Date: 4 May 2020

Table of Contents

Executive summary	1
1. Background	2
1.1 Company Background	2
1.2 Incident background	2
1.3 Proposal background	3
2. Impacts and findings	4
2.1 Financial impact	4
2.2 Potential impacts	5
2.3 Technical findings	5
3. Analysis	8
3.1 Before the incident	8
3.2 After the first event	9
3.3 Follow-up	10
4. Recommendation	11
4.1 Company structure and policy	11
4.2 System development and monitoring	13
4.3 Training	15
4.4 Implementation	16
5. Conclusion	19

Executive summary

Cathay Pacific Airways Ltd. is one of the largest airlines in the world. The data breach in 2018 lead to a series of management issues of different departments in Cathay Pacific. This consultancy report highlighted facts and findings and provide an overall recommendation in company structure, process control, and methodologies to prevent future risk of violating different regulations with a specific timeline.

This reports will focus on discussing the weakness and avoidable risks in Hong Kong office. The other follow up on technical risk and comments made by government officials will be covered in further study.

1. Background

1.1 Company Background

Cathay Pacific Airways Ltd. is one of the largest airlines in the world who provides cargo and traveller flight services with HK Stock code 0293. On March 2019, they acquired another Hong Kong airline company - HK Express, which made them became the largest airline company in Hong Kong.

On 26 April 2020 Cathay Pacific Airways Ltd worths over 35 billion Hong Kong Dollars. It operates under brand of Cathay Pacific and Cathay Dragon, HK Express, Air Hong Kong, and Airline Services segments. As of 31 December 2019, it operated 236 aircraft directly connecting Hong Kong airport to 119 different destinations in 35 countries worldwide (Cathay Pacific Airways Ltd, 2019).

They are also one of the leading global airlines. Its passenger service ranked 5th among all the airlines in the world in 2020 (Forbes, 2019), and its cargo service rank 5th in the world in 2018 (International Air Transport Association, 2019). Cathay Pacific had started a 3-year restructuring plan in 2017, cutting over 30% off of their supporting staff (South China Morning Post, 2017).

1.2 Incident background

Cathay Pacific had a cybersecurity incident that leads to a data breach in 2018 March of which over 9.4 million customers compromised. Many media and news stated that it is the worst crises in the history of aviation (South China Morning Post, 2018). After over 2 years of investigation, experts point out that there are different management issues need to be solved.

An independent data investigation had been conducted between October 2018 to June 2019 by Privacy Commissioner of Personal Data, Hong Kong. The enforcement action of the incident had proposed to establish a risk management committee, which will oversee the design, implementation and monitoring of the risk management and internal control systems of the company.

1.3 Proposal background

After 2 years of the incident, court judgment has been final also with other related claims. It is a good time for management to look into the event and seek for feasible proposals to the board of directors to restructure their information system department's operation and a long term policy to prevent or manage the next cyberattack.

The event just happened before the implantation date of the General Data Protection Regulation, a regulation that protects personal data of EU citizens (*General Data Protection Regulation 2018a*). Estimated the total fine for the case might come up to 4 billion HKD (*General Data Protection Regulation 2018c*). The event raises the awareness of company management, and they are taking action to improve their system and related policy.

2. Impacts and findings

2.1 Financial impact

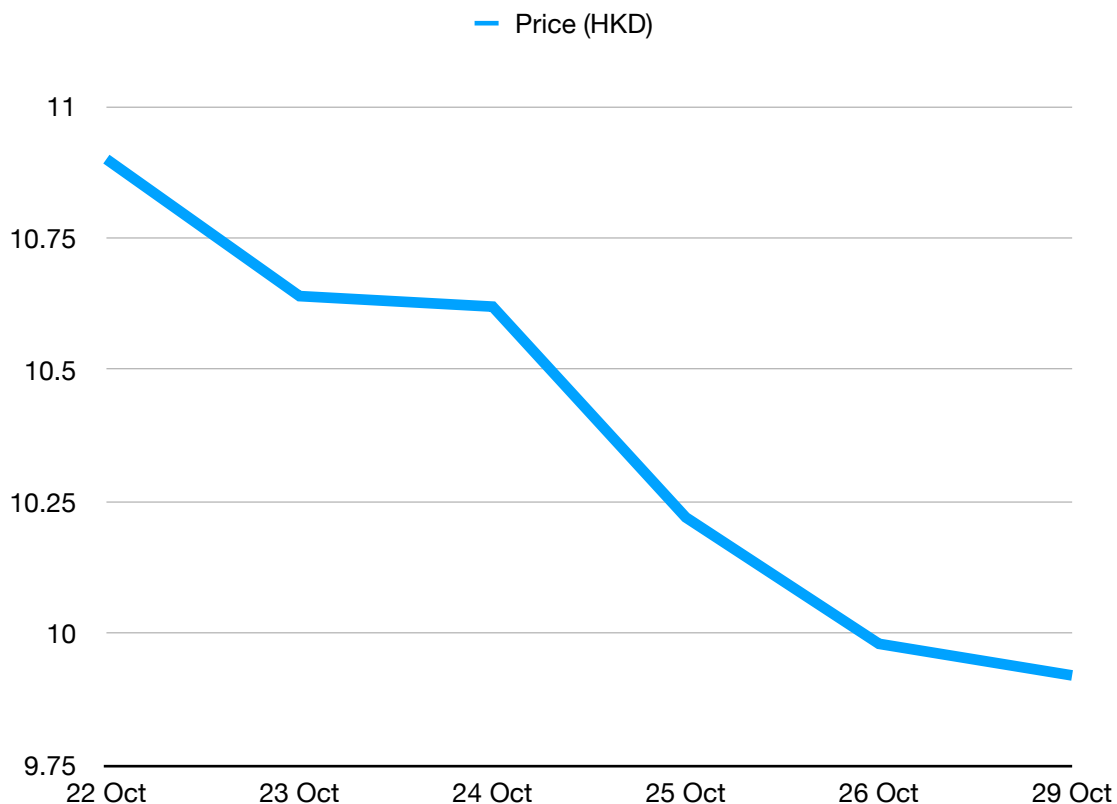


Chart 1: Closing stock price of Cathay Pacific on 23 October to 30 October 2018

Source: <https://finance.yahoo.com/quote/0293.HK/history> period1=1539993600&period2=1540857600&interval=1d&filter=history&frequency=1d

Cathay Pacific is a Hong Kong Main Board listed company since May 1986. The above chart has shown that, 3 days after the incident public, the stock price drop around 7% from HKD 10.62 to HKD 9.92, which worth around 0.35 million HKD. Other than direct Financial impact, it also impacted their goodwill as well as the image of the company. After one year, there are more than 40% of customers are still remembered the incident.

After 2 years, many countries had finished their legal procedure and imposed a different amount of fine while one of the most recent cases in the United Kingdom. It has imposed £500,000 fine accordingly.

2.2 Potential impacts

The incident was found out by cybersecurity department on March 2018, after an in-depth investigation, an internal review was announced on 23 October 2018. Many media and lawyers think it was lucky timing for Cathay Pacific management as the data protection law published by EU was enforced on 28 May 2018, which is 2 months after the incident.

The data protection law names General Data Protection Regulation, which have a penalty up to 4% worldwide revenue. With over 111 billion revenue which is around 4.4 billion HKD accordingly. (Cathay Pacific Airways Ltd., 2019)

2.3 Technical findings

There are two attack groups targeted Cathay Pacific's system at the same period, and one of them has hacked the network since 2014 while another one was since 2017 (Privacy Commissioner for Personal Data, 2019).

Date	Group A	Group B
15 October 2014	Key-logger Activity start	
13 March 2018		Brute force attack
22 March 2018	Attack activity ended	
5 May 2019		Remotely access Cathay's system
8 May 2019		Accessed the administrator console
28 August 2018		Attack attempted, blocked before any data was accessed

Table 1: The timeline of two different attack

Sources: Cathay Pacific Airways Limited Report and Hong Kong Dragon Airlines Limited Unauthorised access to personal data of passengers

Shown in the table 1 above, The group A of hackers attacked the system by using a tool called vital logger, which is a tracking device in one of the Cathay Pacific servers. It was being installed and logged all the traffics, usernames and

passwords in their servers. This style of attack is popular yet effective among large enterprises and networks like Cathay Pacific. The key logger can steal system administrator credentials. With the stolen credentials, hackers can use it to log in different servers, access systems and create different levels of damages or acquire confidential data. This hacking behaviour has not been noticed the public since 2014 till this event happened. Attackers using the harvested credentials to dumplings up specific account access rights, including different networks, systems and extract domain's credentials.

The group B of attack is the main reason that has drawn cybersecurity department's attention. A brute force attack happened on 13 March 2018. A brute force attack is an attacking method that use multiple locations and different computers to send the request to target services, and in this case, they tried to login staff accounts. This kind of attack usually apply with DDOS, using high traffic to cover up attacker login attempts as a result, around 500 staff accounts was lockout by the hacker.

After 5 months of the brute force attack, their internal investigation team has found out 7 more successful attacks targeting member loyalty system, web database, customer information reporting system and Asia miles redeem database.

There are approximately 9.4 million passengers from over 260 counties were affected, as shown in Chart 1. Apart from the general data such as name, flight number and email address, there are 9% of the user's passport number, and 6% of user's ID card number has involved in the incident. Typically, sensitive information will be encrypted and placed into a separate database instead of putting into together with general data.

After that huge amount of data were comprised, Cathay Pacific had proactively search for any trace of leakage in different ways, including dark web and hacker forum. No proof of any data had been selling in mentioned platforms.

To inform all the affected customers, Cathay Pacific had sent email separately to notice customers what personal data involved in this incident. Emails were starting to send out on 25 October 2018, 7-month after the first attack was spotted. The investigating report questioned about reasons for the long handling time, Cathay Pacific explained they need 7 months to fully understand the scope and specific details to inform affected customers accurately.

3. Analysis

3.1 Before the incident

Cathay Pacific claimed that they had invested over 1 billion HKD in managing cybersecurity threats. However, the 1 billion HKD compared to Cathay Pacific's extensive IT infrastructure, which contained 1.3 billion backup files, 470 databases, 4,500 different servers and over 600 application systems. That is not signed to handle threats or attacks in a challenging environment compared to the average cost of a penetration test which is USD 15,000-30,000 (Glover, 2018).

Cathay Pacific has operating thought different brand name, which they also provide information management service to its subsidiary, Cathay Dragon. The information management service including hardware infrastructure, IT consulting, network and telecommunication services yet not include any cybersecurity service. (Privacy Commissioner for Personal Data, 2019).

One of the primary system involved in this incident is an internet-facing server that let a hacker gain administrative access. Cathay Pacific stated that it had engaged a third-party vendor to perform a vulnerability scan in 2017 before the system launched. The test was unable to detect the widely published vulnerability. A vulnerability scan is a process that the development team engage a third-party consultant to help to look for a known vulnerability. However, as the scan accuracy is heavily related to the profile and vulnerability database provided by the consultants, the enterprise usually engages more than single submit to perform the scan. Moreover, any system contains sensitives customers data should go though severely testes by a professional penetration tester. A penetration test is a cybersecurity process that tester will use different tools and known exploit to simulate the real-life scenario of attack.

As a company providing IT consulting service to its subsidiary, Cathay Pacific management didn't put effort to upgrade its internet-facing server into the latest version. Cathay Pacific explained the latest versions were incompatible with an airbus fleet manual application, which means their management did consider to upgrade. Still, due to different reasons, they put the upgrade timeline off the book.

The management seem didn't understand the system development process of cybersecurity and try to put the responsibility to the third party.

3.2 After the first event

After the suspicious activity, they discover on 13 March 2018. Their management discussion is to commence an internal investigation and take over 7 months to notify all the affected clients and government officials. At that time, as the GDPR is going to implement, the Data protection officers of Cathay Pacific should be working on fulfilling the requirement of this critical data protection law.

In GDPR, DPO should ensure all incident involve EU citizens personal data should be reported to the local government within 72 hours of first noticing (*General Data Protection Regulation, 2018b*). Cathay Pacific stated that they need to have a full understanding of the events before reporting, that is not acceptable under the international standard. With the short period from the GDPR enforcement, management of Cathay Pacific is trying to cover up the event with a different excuse.

Some of the leakage data are dated back to 2005, which show Cathay Pacific didn't set a limited time for personal data storage. With the guideline provided by GDPR, the company should establish a limited period of storing personal electrical data.

After the event, on 25 May 2018, Cathay updated its privacy policy in the main website, with GDPR wordings and legal point of view. This action clear state that the management of Cathay aware of the new GDPR and on purposely avoid incident being public.

3.3 Follow-up

Cathay is a Hong Kong-registered company. Hong Kong doesn't have a comprehensive data privacy law like GDPR. Company against data protection law are not going to have any legal punishment.

However, Cathay pacific setup operating office in 76 countries, many of these countries have a comprehensive data protection system. After the incident, a different file lawsuit against Cathay Pacific, for example, Turkish Data Protection Board impose a 600,000 Hong Kong Dollars fine for not taking necessary technical and administrative measures to ensure the data security. There are 15 countries file a lawsuit on this event (South China Morning Post, 2018).

4. Recommendation

There are many different approaches that Cathay Pacific can do to prevent the impact on the company and the massive awareness of the society when such an incident happen. We will explore the different improvement department can be made. At the moment, Cathay Pacific outsource its IT department and system maintenance jobs to a third party, there is no management team member take in-charge (Cathay Pacific Airways Ltd., 2020)

4.1 Company structure and policy

4.1.1 IT and cybersecurity department

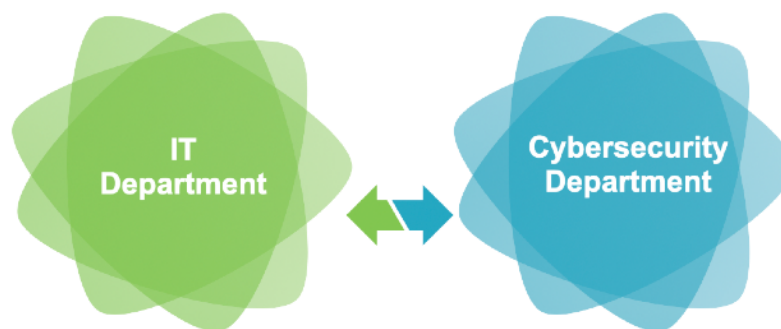


Figure 1: The timeline check and balance of two department

IT and cybersecurity are recommended to be operating in two different departments, which can check and balance each other. Senior management will have better internal control on the system and company network states. There are common that company's CTO or IT department head will report the difficulty and latest development of the company. Since CTO is the only expert among the BOD, the BOD cannot draw an overall opinion. There might miss the importance of different issue. With the help of Cybersecurity department head, BOD can gain more insight from him.

4.1.2 Incident response policy



Figure 2: The concept of incident response

Cathay pacific are recommended to prepare different incident response plan for different department. Incident response is a standing process for enterprises to handle another type of cyber attack as shown in Figure 2.

After discovering a new cyberattack incident, an ad hoc committee should be formed. The committee chairman should be the data protection officer with a committee member from cybersecurity department, public relationship department, law department and human resource department. Cybersecurity department needs to generate all system log with the maximum time period and save it to an independent location from the Security Incident and Event Management (SIEM) system. SIEM provides important primary evidence for any further investigation. Within the next 24-48 hours, the security team need to have the first draft of the report that includes what kind of information is being involved in the event. The committee will start to draft the report of the incident, and within the first 72 hours, the organization must inform the local government about the details of the event. A formal notice to the customers are required, the notice needs to include the information involved in the incident.

4.2 System development and monitoring

4.2.1 DevSecOps Approach

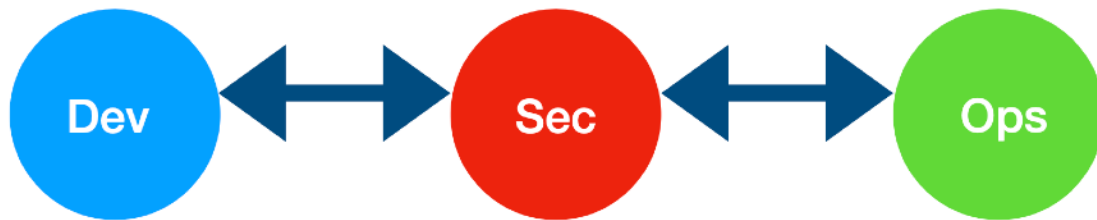


Figure 3: The process of DevSecOps

DevSecOps approach is a development cycle for better security control on system development. In traditional program development, the project manager would draft a function plan and assign to the different programmer. The programmer will only need to provide a function that aligns with the plan, due to the tight timeline, the manager usually will not provide a guideline on how the programmer writes the code. DevSecOps approach helps enterprises address security threats more effectively, in real-time. It is essential to view security teams as a valuable asset that help prevent slowdowns rather than a hindrance to agility. For example, early detection of a poorly designed application that cannot scale in the cloud saves valuable time, resources, and computing costs. In a recent survey, the system using DevSecOps approach are 700% more likely to fully integrated security practices (Walters, 2019).

In the planning stage, it is suggested to provide a full picture of the system and other team member process (Petricek, 2019). Management needs to provide development staff full details of the usage and data involved. In this case, one of the affected databases preserved a remarks space that allows users to input custom wordings. Cybersecurity department

is also reasonable for taking a role as a reviewer, to review important details of any new system. In the latest guideline, the company are required to encrypt all database with customer information, providing full information to development staff also increases their awareness of using a more secure way to handle data transition.

It is recommended to hire a third-party penetration tester to perform the security check for all system. As there are many industry-specific frameworks, as this framework is commonly used in the world, known public vulnerability may not easily found on the internet. A penetration test should perform by qualify tester, e.g. OSCP for server system and OSWE for the web application. However, a penetration test will not be enough for a complex system like a ticket system and miles redeem system. For such a system, a white-box penetration test is recommended. A white box review is allowing the tester to see the source code of the system in the process. A white box penetration test can provide a full picture for the tester to understand the weak point of the system, and focusing weak point to test.

4.2.2 Threat intelligence

Cathay Pacific is recommended to subscribed multi-threat intelligence source. Threat intelligence is a research-based service, the service provider will collect Common Vulnerabilities, and Exposures combine threat news from experts forum, black market and software officials update. With these services, cybersecurity can draft the patch of vulnerabilities more timely. The IT department can spend less time on research, but using more time on software update and patch.

4.3 Training

Training is one of the most important areas to build an effective cybersecurity environment. In nowadays operation, almost all staff will have a company email and login credential for different working space. The only count of the cybersecurity department to protect company data is not realistic.

Cybersecurity Culture (Schlienger and Teufel, 2002) is one of the latest trends in cybersecurity (Gcaza and others, 2017). As the hacker develop a new way to attack every possible weak point of a company, the employee needs to be aware of attack anytime. For example, the billing department needs to do two factors checking for every new vendor and bank account.

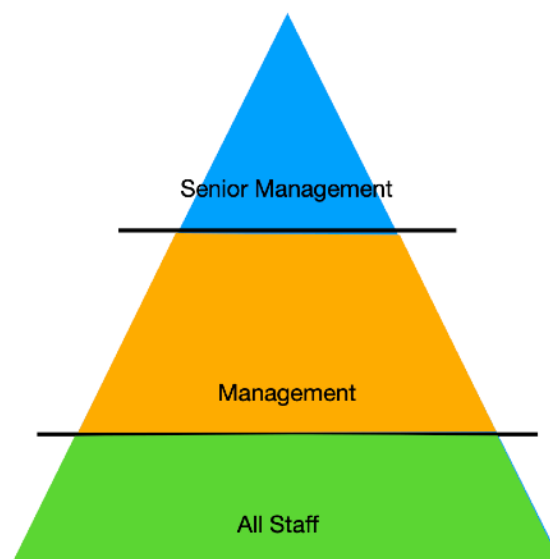


Figure 4: 3 Level of cybersecurity training

As shown in Figure 4, the culture training is suggested to divide into 3 levels, for senior management, management and all staff. We can see in this case, Cathay Pacific senior management didn't have a proper mindset in cybersecurity.

Senior management training should major in company policy, law and regulation and incident response. When senior management makes a discussion on the new company service, buying new software or drafting next year budget, they need to

put cybersecurity in consideration. These considerations should be a higher priority than others.

Management training should focus on handling customers information. Management level staff's credentials are able to access a large amount of sensitive information. They need to have a good habit of handling these access right and their credentials. These training should include how to work in a different location, how to protect their credentials and understand the data access right policy in their department.

Some awareness can't be trained (Wilson and Hash, 2003). All staff should be getting company cybersecurity policy training in their orientation training. Topic includes how to handle customers and different partner email, how they should log in their email and how is the report methods when they notice cybersecurity threat happening in their working area. With a proper orientation training and monthly worldwide cybersecurity news update, all staff will have a better sensitivity of new attack. This can help cybersecurity department to build the first line of defence against an attacker.

4.4 Implementation

4.4.1 Timeline

Facing the challenge of COVID-19 (Reuters, 2020) and different competitor, there are not easy to put all resources into building a more safe environment. It is suggested that to develop a 3-year plan to take all the recommendation above.

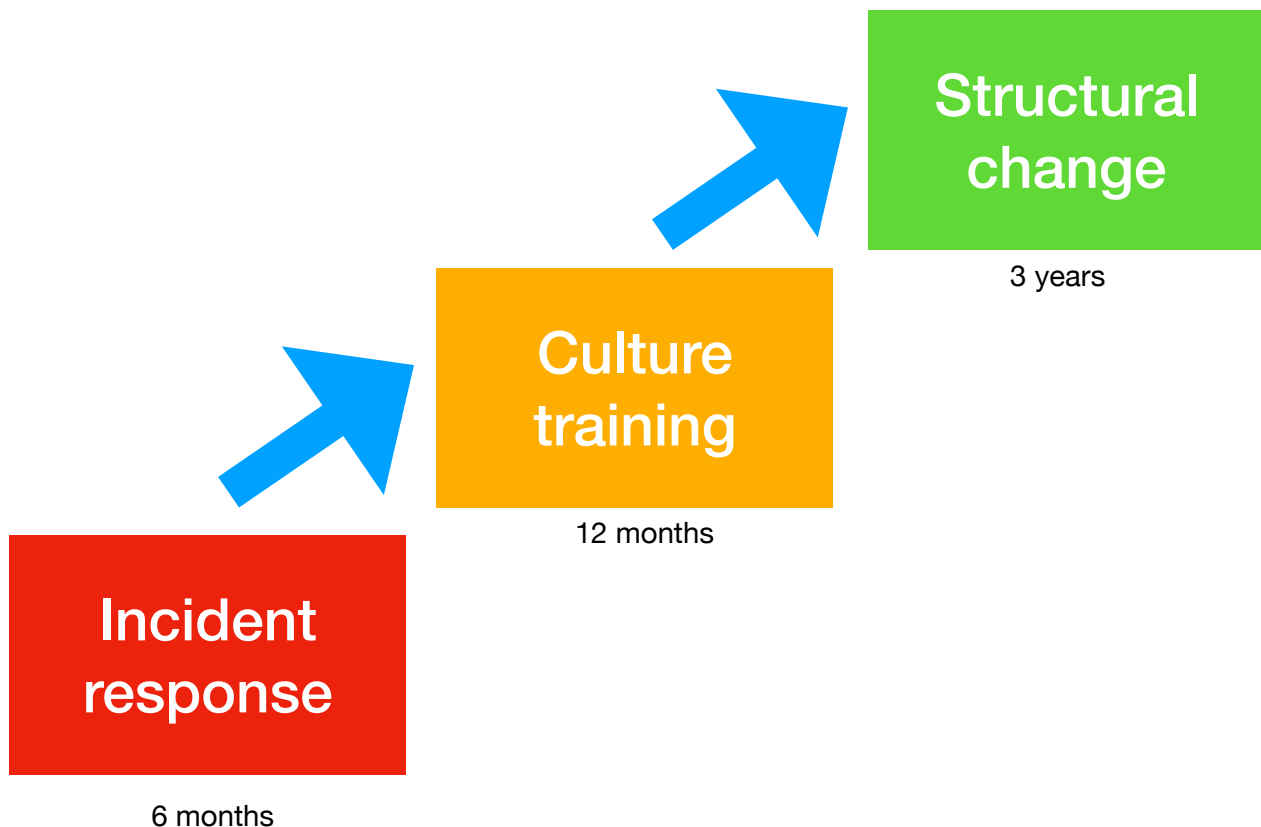


Figure 5: 3-year plan for Cathay Pacific to enhance company cybersecurity

As shown in Figure 5, the first 6 months, Cathay Pacific should make good use of the experience getting in this massive data breach to draft a more comprehensive incident response plan. Every year, they should perform a cyber-attack drill, or do a risk base penetration test to ensure all related positions well understand the plan how would it be run in a real-life situation.

Cathay is suggested to implement all layers of training in the next 12 months, and the training can be online for staff outside of Hong Kong. Tests and interview should be conducted.

In their next 3-year plan, Cathay Pacific should form a new cybersecurity department. As staff training is an essential factor for the department to success, the department should be more in-house staff and

Cathay should provide in-depth training on perpetration testing, threat hunting and SOC operating. With the massive scale of Cathay, it is suggested to build a team of around 20 staff and form at least 5 groups, Internal testing team, SOC operating team, threat intelligence and training team.

With the recommendation above, Cathay would be able to migrate the risk if being fine by GDPR, as the above advice aligns with the requirement of GDPR. With a new department and continues training, Cathay will set a new standard in the best practice to protect clients personal data.

4.4.2 Potential risk

A certain amount of investment needs to be made in executing the recommendation. The board of director may face the challenge of shareholders. If no action is taken, there will be a more significant impact on the company in the next attack. There are also some risks that the third-party review may not show some hidden information for this proposal. Without all the data, the solution might overlook some potential dangers.

The higher management must be able to show the determination to all employee. The motivation of the management is curial to successfully implement this 5-year plan (Bada, Sassa and Nurse, 2019).

5. Conclusion

Cathay Pacific data breach happened in 2018 is not caused by a single weak point of the system and management. With the huge and complexity of the system they have, it is not wise to outsource their company cybersecurity department. After 2 years of the incident, the position of CTO is still empty, show that there are still lots of follow up work need to be done, and the weak point needs to be fixed.

The board of director need to take the first big step starting to promote cybersecurity culture in Cathay Pacific. Due to COVID-19, the business environment of the airline industry will have many unforeseeable challenges. However, the cyberattack will keep happening no matter how the world changes. A reliable support of IT and cybersecurity department can help the company to prevent risk from another wave of cyberattack, which might cost a lot more than investing in enhance the cybersecurity recommended in this report.

For a full review of the company's cybersecurity policy and weak point, management can focus on the policy among different operation locations, vendor policies and the system maintains workflow which didn't cover in this report.

Reference

A. Buğra Aydın and Nurhak Özer (2019) *Turkey: Recent Fines Imposed By The Turkish Data Protection Board On Data Controllers*. Available at: <https://www.mondaq.com/turkey/data-protection/823922/recent-fines-imposed-by-the-turk305sh-data-protect305on-board-on-data-controllers> (Accessed: 19 April 2020).

Cathay Pacific Airways Ltd. (2018) *Annual report 2018*. Available at: https://www.cathaypacific.com/content/dam/cx/about-us/investor-relations/interim-annual-reports/en/2018_annual_report_en.pdf (Accessed: 20 April 2020).

Cathay Pacific Airways Ltd. (2019) *Annual report 2019*. Available at: https://www.cathaypacific.com/content/dam/cx/about-us/investor-relations/interim-annual-reports/en/annual_report_2019_eng.pdf (Accessed: 20 April 2020).

Cathay Pacific Airways Ltd. (2020) *Management team*. Available at: https://www.cathaypacific.com/cx/en_HK/about-us/about-our-airline/management-team.html (Accessed: 30 April 2020).

Elissa Walters (2019) *5,558 IT Professionals Reveal Patterns of Elite DevSecOps Practices: 2019 DevSecOps Community Survey shows mature programs are 700% more likely to automate security, as adversaries accelerate pace*.

Forbes (2019) 'The 2020 List Of The World's Best Airlines Is Out Now' Forbes 27th November 2019. Available at: <https://www.forbes.com/sites/ericrosen/2018/11/16/the-2019-list-of-the-worlds-best-airlines-is-out-now/#636851c6470f> (Accessed: 28 April 2020).

Gary Glover (2018) *How Much Does A Pentest Cost?* Available at: <https://www.securitymetrics.com/blog/how-much-does-pentest-cost> (Accessed: 20 April 2020).

Gcaza, Noluxolo, Solms, Rossouw, Grobler, Marthie and Jansen van Vuuren, J.C.. (2017). A general morphological analysis: Delineating a cyber-security culture. Information and Computer Security. 25. 10.1108/ICS-12-2015-0046.

South China Morning Post (2017) 'Job cuts expected as Cathay Pacific targets 30 per cent savings in head office management costs'. *South China Morning Post* 17th March 2017. Available at: <https://www.scmp.com/news/hong-kong/economy/article/2079777/jobs-cuts-expected-cathay-pacific-targets-30pc-savings-head> (Accessed: 25 April 2020).

South China Morning Post (2018) 'Cathay Pacific under fire from 15 countries on data breach, bosses reveal as they address 'one of Hong Kong airline's worst crises' '. *South China Morning Post* 14th November 2018. Available at: <https://www.scmp.com/news/hong-kong/politics/article/2173214/cathay-pacific-under-fire-15-countries-data-breach-bosses> (Accessed: 25 April 2020).

General Data Protection Regulation 2018a, Art. 2.2c European Union. Available at: <https://gdpr.eu/article-2-processing-personal-data-by-automated-means-or-by-filling-system/> (Accessed: 25 April 2020).

General Data Protection Regulation 2018b, Art. 33.1.European Union. Available at: <https://gdpr.eu/article-33-notification-of-a-personal-data-breach/> (Accessed: 25 April 2020).

General Data Protection Regulation 2018c, Art. 83.5 European Union. Available at: <https://gdpr.eu/article-83-conditions-for-imposing-administrative-fines/> (Accessed: 25 April 2020).

International Air Transport Association (2019), *IATA's Annual Review 2019. Available at: <https://www.iata.org/contentassets/c81222d96c9a4e0bb4ff6ced0126f0bb/iata-annual-review-2019.pdf> (Accessed: 25 April 2020).*

Maria Bada , Angela M. Sasse and Jason R.C. Nurse (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour <https://arxiv.org/pdf/1901.02672.pdf>.

Reuters (2020) 'Cathay to let crew wear masks on all flights due to new coronavirus'. Available at: <https://www.reuters.com/article/us-china-health-cathay-pacific/cathay-to-let-crew-wear-masks-on-all-flights-due-to-new-coronavirus-idUSKBN1ZL019> (Accessed: 22 April 2020).

Privacy Commissioner for Personal Data (2019). *Cathay Pacific Airways Limited Report and Hong Kong Dragon Airlines Limited Unauthorised access to personal data of passengers*. Available at: https://www.pcpd.org.hk/english/media/media_statements/files/PCPD_Investigation_Report_R19_15281_E.pdf (Accessed: 1 April 2020).

Tomas Petricek (2019) *Cultures of programming*. Available at: <http://tomasp.net/academic/drafts/cultures/cultures.pdf> (Accessed: 28 April 2020).

Thomas Schlienger and Stephanie Teufel (2002) *Information Security Culture: The Socio-Cultural Dimension in Information Security Management* 191-202.

Wilson and Hash (2003) Building an Information Technology Security Awareness and Training Program Available at: <https://csrc.nist.gov/publications/detail/sp/800-50/final> (Accessed: 15 April 2020).

Student Self Evaluation Form			
Student name:	Lam Wai Yeung	Student number:	1913636
Programme:	MBA	Year of programme	2020
Assignment Title:	How Cathay Pacific Airways Ltd improve its cybersecurity control after impact on 2018		

This section repeats in brief the common assessment criteria detailed on previous pages. The *extent* to which these are demonstrated by you determines your mark. Using these criteria, tick the box that best indicates the level of achievement you feel you have achieved with regard to each of them.

Common Assessment Criteria Applied	Level of Achievement						
	REFER			PASS		DISTINCTION	
	FAIL	FAIL	MARGINAL FAIL	SATISFACTORY	GOOD to VERY GOOD	EXCELLENT	EXCEPTIONAL
1. Engagement with literature	0-29%	30-39%	40-49%	50-59%	60-69%	70-84%	85-100%
	☐	☐	☐	☐	✓	☐	☐
2. Knowledge and Understanding	0-29%	30-39%	40-49%	50-59%	60-69%	70-84%	85-100%
	☐	☐	☐	☐	☐	✓	☐
3. Cognitive and intellectual skills	0-29%	30-39%	40-49%	50-59%	60-69%	70-84%	85-100%
	☐	☐	☐	☐	✓	☐	☐
4. Practical Skills	0-29%	30-39%	40-49%	50-59%	60-69%	70-84%	85-100%
	☐	☐	☐	☐	✓	☐	☐
5. Transferable Skills for Life and Professional Practice	0-29%	30-39%	40-49%	50-59%	60-69%	70-84%	85-100%
	☐	☐	☐	☐	☐	✓	☐

PLEASE COMMENT ON AREAS IN WHICH YOU FEEL THAT YOU HAVE PERFORMED WELL		PLEASE COMMENT ON AREAS YOU FEEL THAT YOU NEED TO DEVELOP	
The combination of theory and real life case.		Referencing and building up solid conclusion	
Student's Name	Lam Wai Yeung	Date	4 May 2020
Student's Signature	<i>Marco Lam</i>		