Information Risk Management of the British Airways Data Breach (September 2018)

Kiran Kumar Mohanraj. Author, *MSc. Cybersecurity*

***Abstract*— With the increasing cyber incidents, the need for risk assessment to understand, control, and mitigate all forms of cyber risk has arisen. In June 2018, British Airways (BA), United Kingdom's national airline, experienced breach of data laws, where personal data of 430,000 passengers was compromised by poor security management such as released log in details, credit card information, payment card information, names, booking details and address information. This caused BA to pay a penalty of £20 million under new data regulations. This paper uses the ISMS and FAIR approaches to assess the risk faced by British Airways and provide measures to mitigate further data breaches.**

Keywords- Cyber Incidents, Risk Management, ISMS, Risk Assessment, ISO 27001, FAIR, Data Breach.

I. INTRODUCTION

Over the years, the threat faced by Information Technology has changed drastically. The tools and techniques used to attack systems are advanced because of which the stakes at risk become larger every year. Despite taking efforts to develop and defend the systems of the organization, there is some vulnerability in their infrastructure. Nowadays, organizations are shifting towards trying to understand when a cyber incident will happen, and what the consequences will be.

The most effective way to protect any organization against cyber-attacks is to adopt a risk-based approach to cyber security. "Risk management is process which allows the organization to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions" [1]. There are various mechanisms for risk management. This paper mainly focuses on Information Security Management Systems (ISMS) and Factor Analysis of Information Risk (FAIR) to perform a risk assessment, risk analysis and risk treatment on British Airways.

II. ABOUT BRITISH AIRWAYS

British Airways is an airline company created in 1974 after its board was established by the British government. Originally British Airways were four different airline companies and later merged into one. It is the second-largest flag carrier airline of the United Kingdom behind EasyJet [2]. British Airways began merging with holding companies in 2011 to obtain an international appearance. As the company is growing so is its technological advancements. This is great for a company that is expanding, but as they are continuing to grow and advance, they do not seem to be taking the correct precautions when it comes to their security protocols. There have been occasions where British Airways have been under cyber-attacks. Although they follow protocols for the aftermath of the attack, they need to develop something that will eliminate or diminish the attacks.

III. THE BA BREACH

In the summer of 2018, cyber-criminals accessed the personal data of 430,000 passengers of British Airways. Most of them (58 per cent) had crucial details stolen. The data comprised the passenger's name, travel plans, billing address, email address and payment card details – including the three-digit security code (CVV) from the back of the card. The remainder had their card numbers stolen, with 18 per cent of the total having their CVV hacked as well. The affected travelers had bought flights on the ba.com website, through the British Airways app or with Avios, BA's frequent-flyer scheme [3]. Along with these, the usernames and passwords of BA employee and administrator accounts as well as usernames and PINs of up to 612 BA Executive Club accounts were also potentially accessed [4].

The way the hackers accessed the information of an estimated half a million people was through a vulnerability in third-party JavaScript used on the website, exploited by a hacking group called Magecart. Initially it appeared that BA faced a fine of £183 million under the Data Protection Act, representing 1.5 per cent of BA's global turnover in 2017. At the time it was the largest proposed penalty under new data regulations. After IAG's (BA's parent company) appeal, British Airways paid a penalty of £20 million [5].

IV. MITIGATION OF BA BREACH

Addressing the poor security arrangements of British Airways would have avoided this major Data Breach. Magecart, a hacking group, are believed to have secreted 22 lines of code that diverted crucial details around payments to a separate website controlled by the criminals. The third-party piece of JavaScript, Modernizr, sent data to baways.com – a similar-sounding website to the official website, but controlled by these criminals.

The vulnerability in Modernizr is a well-known one, and BA had not updated it since 2012. Effective monitoring would have picked up this quickly – not the three months it took BA. Implementing subresource integrity, a security feature that checks whether any information transmitted by web browsers is delivered without being affected, would be relatively simple and less expensive. The main effort should have been taken in

having the right security management infrastructure – knowing at all times what the risks are, being able to find the solutions, and then getting organizational buy-in from implementing them as soon as possible, ideally before systems are rolled out [5]. BA could have performed ISMS or FAIR methodologies to identify their risks and analyse it avoid these types of cyber-attacks.

V. INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

ISMS is a set of guidelines built on three pillars: process, people and technology which helps in protecting and managing the organization's information. The main focus area of ISMS is to protect the confidentiality, integrity and availability (CIA) of the organization's information. It enables compliance with a host of laws, including the EU GDPR (General Data Protection Regulation).

The ISMS is the main product of ISO 27001 implementation. The ISO 27001 is the international standard that describes the development of ISMS and covers the compliance requirements. The ISMS provides various benefits for the organization by protecting all forms of information. The ISMS implementation helps in recovering from a cyber-attack. It provides a central framework for securely maintaining the organization's information. When an organization undergoes changes, whether the outside environment or within the organization, an ISMS helps in reducing the threats related to continually evolving risks. The risk assessment in ISMS helps in reducing the extra costs spent in increasing the layers of defense mechanism which does not have much effect upon a cyber-attack. An ISMS's holistic approach covers the whole organization, not just IT. This enables employees to readily understand risks and embrace security controls as part of their everyday working practices [6].

The ISO 27001 ISMS process are divided into four processes: Establish, Implement, Maintain and Improve.

a) Establish:

In this process, firstly, the Information security policies and the scope are defined. The approach for conducting risk assessment is defined and the risks are identified. These identified risks are then assessed. The process of how each risk should be treated are evaluated. The control measures for these risks are selected. The approval from the management to implement these measures are obtained. Finally, the Statement of Applicability is prepared.

b) Implement:

In this process, the defined risk assessment plan and the control measures are implemented. The employees of the organization are trained to create awareness about various risks and its control measures. The operations and resources of the ISMS are managed. If any cyber-incident occurs, they are detected beforehand and appropriate measures are taken to handle the situation.

c) Maintain:

Implementing an ISMS approach is not enough to avoid the risks. It has to be monitored and reviewed frequently. In this process, ISMS is monitored and reviewed, and its effectiveness is measured. An internal audit is conducted and the security plans are updated.

d) Improve:

After reviewing the ISMS, the identified improvements are implemented and corrective action is taken. These improvements and actions are communicated to the employees of the organization.

This paper will establish an ISMS approach for risk management of British Airways. Before implementing ISMS, we will look into key things which are essential for developing an ISMS.

a) Objective of the organization:

The objective of the organization is important in defining the purpose of running this organization and what are the requirements to fulfill this purpose.

British Airways has its objective divided into three areas: Global – To appeal passengers across the globe so as to create repeat customers; Premium – To provide passengers with high quality of service whenever they come in contact with the airline; Airline – To focus on aviation and to develop new product and services to complement this [7].

b) Asset of the organization:

The asset is a resource which produce economic value to the organization. Listing the assets of the organization helps in understanding the contribution towards the objective. The most valuable asset of British Airways is the people, its customers and employees. Other assets are its aircraft, data centers, software applications, food service, etc. Among these assets, the software application was attacked in BA Data breach 2018 leading to compromise of 430,000 passenger's data. The payments details of the passengers provided in BA's official website and mobile applications was redirected to an unofficial website.

c) People:

There are two types of people in the context of an organization; one is the people inside the organization (the employees) and the other is the people outside the organization (the customers). We need to understand about the roles of these employees and how much they can impact the organizations. It is also important to know our customers and their impact to the organization. The employees of BA are pilots, cabin crew, customer service agent, ground operations, etc. Even the employees of the outsourcing companies can impact the organization.

VI. ESTABLISHING AN ISMS

a) Define the scope of the ISMS

The main reason for defining the scope is to decide which information we intent to protect. It helps in understanding the organization's environment and to realize the security requirements which is to be addressed. In BA, the records of passenger and staffs should be protected. The passenger's data contains sensitive information which includes bank details. This information should be kept confidential and available. It is also important to include things which has potential to influence the information. Raritan, a brand of Legrand, manages BA's 6 data center by providing Data Center Infrastructure Management (DCIM) solution.

b) Define an ISMS policy

The information security policy is basis for implementing an ISMS. It sets out the board's policy and requirements in terms of information security. The element of ISMS policy includes the security objective, access control policy, data protection approaches and legislation. It is very important to include the reference to legislation that the company is working towards. [8] provides list of policies which can be adopted by any organization.

c) Define the risk assessment approach

The internal and external context of the organization and scope of the ISMS will be key drivers in determining what criteria will be needed for risk evaluation, impact, and risk acceptance. The risk assessment process should be reflective of the industry sector and risks related to the organization, as well as expectations of stakeholders and current threat landscape.

d) Risk Identification

The two important terms required for identifying the risks are threat and vulnerability. A threat is any type of danger, which can damage or steal data, create a disruption or cause a harm in general. A vulnerability is a weakness in hardware, software, personnel or procedures, which may be exploited by threat actors in order to achieve their goals.

Risk is a combination of the threat probability and the impact of a vulnerability. In other words, risk is the probability of a threat agent successfully exploiting a vulnerability, which can also be defined by the following formula:

Risk = Threat Probability * Vulnerability Impact.

The table 1.1 in appendix 1.0 provides the Risk Identification of British Airways.

e) Risk Assessment

An information security risk assessment is an important part of ISO 27001 and GDPR and forms part of a wider risk management process. The aim is to identify and assess the hazards and risks surrounding the organization's information assets so it can decide on a plan of action, including how it will treat the risks. Understanding the risks and putting the necessary controls in place to mitigate them will reduce the likelihood of a data breach or cyber-attack taking place.

Likelihood of Risk (probability)						
	1 Low	1	2	3	4	5
	2 Low-Med	2	4	6	8	10
	3 Medium	3	6	9	12	15
	4 Med-High	4	8	12	16	20
	5 High	5	10	15	20	25
Likelihood * Impact = Risk		1 Low	2 Low-Med	3 Medium	4 Med-High	5 High
		Impact to the business (Severity)				

Figure 1 Risk Matrix [9]

f) Risk Treatment

There are four risk treatment options which are not mutually exclusive:

- Risk Avoidance – Choose to avoid the risk by avoiding the actions that cause it.
- Risk Mitigations – Choose to reduce the risk by reducing the likelihood or impact.
- Risk Transfer – Choose to transfer some or all the risk to a third-party.
- Risk Acceptance – Choose to accept the risk without any treatment.

The table 1.2 in appendix 1.0 shows the Risk assessment and its suitable treatment.

VII. FAIR MODEL

The Factor Analysis for Information Risk (FAIR) is a methodology for quantifying and managing risk in any organization. This model helps in understanding, analyzing and quantifying the risks in financial terms. It provides standard taxonomy and ontology for information and operational risk. The Figure 2 shows the risk taxonomy of the FAIR model.

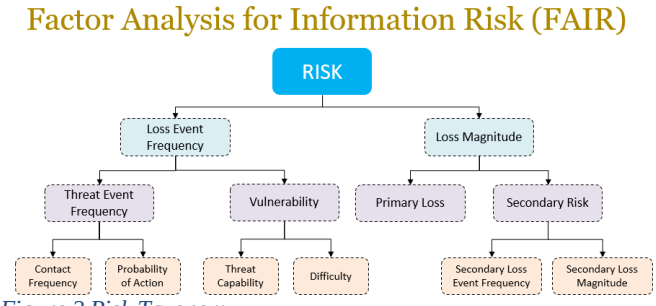

Figure 2 Risk Taxonomy

The Table 1.1 shows the Threat, Vulnerability and Effect assessment for British Airways.

VIII. ANALYSIS AND RESULTS

The analysis of data breach of British Airways has been done using FAIR-U tool. The Figures 3,4,5,6 in appendix 2.0 shows the analysis and its results.

IX. CRITICAL REFLECTION

The implementation of the ISO 27001 ISMS and FAIR methodologies helps us in identifying the risk and which risk requires immediate attention. It also quantifies the risk which helps in analyzing the loss involved if the risk is not treated. The best practice is to implement a mechanism for risk management and reviewing it periodically. In the case of BA data breach, the attack could have been avoided by a vulnerability assessment. A cyber risk management framework which reviews the risk across the business and assesses the portfolio of cyber projects. Threat Intelligence should be used to analyse the cyber risks. Working practices should be reviewed to ensure the integrity of the cyber and data security environment with additional oversight measures should be implemented. All third-party suppliers should to BA security requirements within any revised security protocols.

The ISO 27001 provides set of 14 controls which helps in reducing the risk faced by an organization. In BA data breach, Annex A.12 – Operations Security controls should have been implemented which helps in addressing a malicious behavior of web application and ensure appropriate defenses are in place. Failing to do this lead BA in realizing that a data breach has occurred, after two weeks of the initial attack. BA also failed to implement Annex A.16 – Information security incident management, which is about how to manage and report a security incident, and provides effective approach to the lifecycle of incidents and response [9].

X. CONCLUSION

With British Airways being one of the largest airlines in the United Kingdom for them to experience a data breach means that millions of their customers are at the risk of having vital information stolen. British Airways has had numerous incidences with data breaches, but they were not as big as the 2018 data breach. Even after these incidents BA fails to understand the importance of keeping their data protected.

The risk analysis based on ISMS and FAIR will help BA in avoiding future security incidents. Implementing both these methodologies provide better risk management. ISMS helps in identifying the risk and provide effective control measures. Whereas FAIR model provides quantitative assessment and assess the risk based on informed data.

XI. REFERENCES

[1] G. Stoneburner, A. Goguen, and A. Feringa, “Risk Management Guide for Information Technology Systems.” Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2002, doi: https://doi.org/10.6028/nist.sp.800-30.

[2] “British Airways - Wikipedia,” [Online]. Available: https://en.wikipedia.org/wiki/British_Airways.

[3] “BRITISH AIRWAYS CLASS ACTION SUIT ON DATA BREACH: THE KEY FACTS ON THE COMPENSATION CASE,” *Indep.*, 2021, [Online]. Available: https://www.independent.co.uk/travel/news-and-advice/british-airways-data-breach-compensation-b1786805.html.

[4] “ICO fines British Airways £20m for data breach affecting more than 400,000 customers,” 2020, [Online]. Available: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/.

[5] C. Stokel-Walker, “A simple fix could have saved British Airways from its £183m fine,” 2020, [Online]. Available: https://www.wired.co.uk/article/british-airways-data-breach-gdpr-fine.

[6] Julia Dutton, “What is an ISMS? 9 reasons why you should implement one,” 2019, [Online]. Available: https://www.itgovernance.co.uk/blog/what-is-an-isms-and-9-reasons-why-you-should-implement-one.

[7] “Our strategy and objectives - British Airways,” 2009, [Online]. Available: https://www.britishairways.com/cms/global/microsites/ba_reports0809/pdfs/Strategy.pdf.

[8] “ISO 27001 Policies,” [Online]. Available: https://hightable.io/iso-27001-policies/#h-iso-27001-policies-overview.

[9] Luke Irwin, “ISO 27001: The 14 control sets of Annex A explained,” 2020, [Online]. Available: https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained.

Appendix 1.0

Asset	Risk ID	Threat	Vulnerability	Effect
People	A	Employees providing unauthorized people access to sensitive either physically or through phishing mails.	Unauthorized access to sensitive information	The attacker can sell this information in illegal sites. Fines from GDPR
	B	Any breakdowns in the bargaining process with the unionized workforces may result in subsequent strike action.	The services provided by BA is disrupted.	Disruption of operations and adversely affect business performance
	C	Failing to attract, motivate, develop and retain employees to deliver service and brand excellence.	The performance of the organization.	Employees do not display the required leadership behaviors which causes BA's transformation plans to drive the business forward may not be achieved.
Infrastructure	D	BA is dependent on resilience within the operations of the Air Traffic Control (ATC) services. Disruption in this service will affect flight operations.	Flight operations are not delivered as scheduled	Frequent flight delays will create a negative brand reputation.
	E	BA is dependent on the timely entry of new aircraft and the engine performance of the aircraft	It affects the delivery of the sustainability programme.	Reduction in operational efficiency and resilience.
	F	Failure to prevent or respond effectively to a major safety or security incident.	-	Adversely impact the BA's brand, operations and financial performance. At worst case, it would to lead to loss of lives.
Outsourced services	G	Attack on critical third-party suppliers.	The services to customers such as airport operators, border control and caterers are affected	It causes financial stress or restructuring where these service providers exit the market for supply of services.
Information	H	If BA does not adequately protect customer and employee data. Attacks on BA's system by criminals, foreign governments or hacktivists.	Confidential and sensitive information can be accessed by the attackers.	Could face financial loss, disruption or damage to brand reputation. Could breach regulation and face penalties.
Software	I	BA's official websites and mobile application without adequate security and updates. Running an unsupported software.	Unauthorized access to sensitive information The system and infrastructure are exposed to attacks	Like in the case of BA data breach 2018, it could impact the BA's brand, operations and financial performance. Fines from GDPR
Hardware	J	Failures in network equipment, communication devices, etc.	The services provided by BA is disrupted.	Could lead to loss of valuables or affect customer satisfaction.
	K	Stopping of flight operation due to climatic changes or pandemic situation.	The services provided by BA is disrupted.	May result in lost revenue, customer disruption and additional costs.

Table 1 – Risk Identification for British Airways

Risk ID	**CIA Profile (C-Confidentiality, I-Integrity, A-Availability)**	**Risk Value (RV) (L-Likelihood, I-Impact)**	**Risk Treatment**
Employees providing unauthorized people access to sensitive either physically or through phishing mails.	C – High I – High A - Medium	L – 3 I – 4 RV – Medium	Risk Mitigation: Constant training of Staff on cybersecurity matters Behavior profiling and anomaly comparison provide the clearest picture of unusual activity
Any breakdowns in the bargaining process with the unionized workforces may result in subsequent strike action.	C – Low I – Low A - High	L – 2 I – 3 RV – Low Medium	Risk Avoidance: Collective bargaining takes place on a regular basis led by human resources specialists with a strong skillset in industrial relations.
Failing to attract, motivate, develop and retain employees to deliver service and brand excellence.	C – Low I – Low A - High	L – 2 I – 2 RV – Low Medium	Risk Avoidance: Provide leadership development and talent strategy Provide training, apprenticeship and work experience programs.
BA is dependent on resilience within the operations of the Air Traffic Control (ATC) services. Disruption in this service will affect flight operations.	C – Low I – Low A - High	L – 2 I – 4 RV – Medium	Risk Acceptance
BA is dependent on the timely entry of new aircraft and the engine performance of the aircraft	C – Low I – Low A - High	L – 2 I – 2 RV – Low Medium	Risk Mitigation: Mitigate engine and fleet performance risks, including unacceptable levels of carbon emissions to the extent possible by working closely with the engine and fleet manufacturers
Failure to prevent or respond effectively to a major safety or security incident.	C – High I – High A - High	L – 3 I – 5 RV – Medium High	Risk Mitigation Respond in a structured way in the event of a safety or security incident. Employees and key third parties take part in crisis management exercises Ensure lessons from incidents are fed into daily operations and operations are structured around the safety policies
Attack on critical third-party suppliers.	C – High I – High A - High	L – 4 I – 5 RV – Medium High	Risk Mitigation and Transfer: Work with suppliers to ensure operations are maintained and the impact to BA is understood, with mitigations implemented where necessary.
If BA does not adequately protect customer and employee data. ***Attacks on BA's system by criminals, foreign governments or hacktivists.***	C – High I – High A - Medium	L – 4 I – 4 RV – Medium High	Risk Mitigation a policy be put in place to mitigate risks of accessing external files, software, installation of unauthorized software and enable scanning of email and web pages. Implement a cyber risk management framework which reviews the risk across the business and assesses the portfolio of cyber projects.

BA's official websites and mobile application without adequate security and updates. *Running an unsupported software.*	C – High I – High A - Medium	L – 4 I – 4 RV – Medium	Risk Mitigation a policy be put in place to mitigate risks of accessing external files, software, installation of unauthorized software and enable scanning of email and web pages. Implement a cyber risk management framework which reviews the risk across the business and assesses the portfolio of cyber projects.
J	C – Low I – Low A - High	L – 3 I – 3 RV – Medium	Risk Mitigation Mitigate this risk with focus on operational and financial resilience. This includes functionality and disruption management processes in place to help customers when their journeys are disrupted
K	C – Low I – Low A - High	L – 2 I – 3 RV – Low Medium	Risk Acceptance

Table 2 – Risk Assessment and Treatment for British Airways

Appendix 2.0

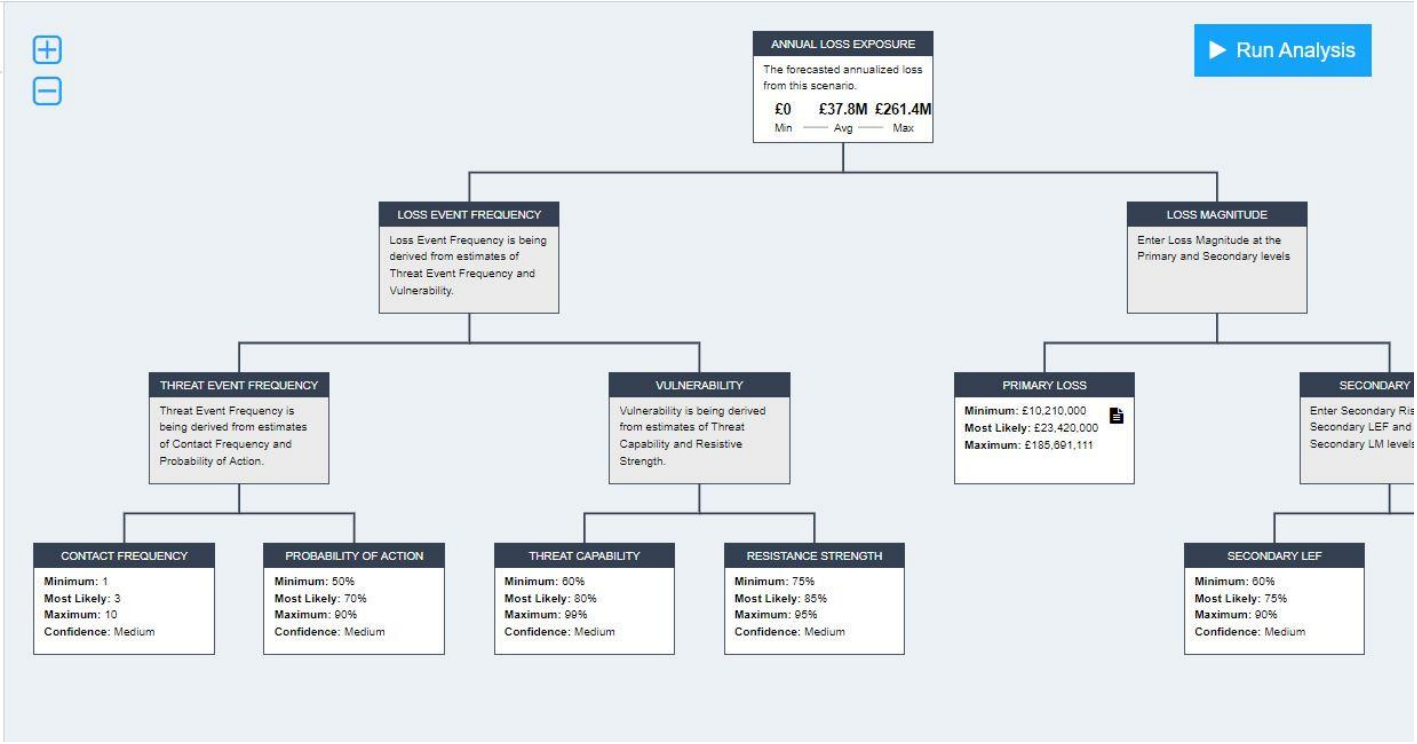

Figure 3 FAIR-U Analysis of British Airways Data Breach

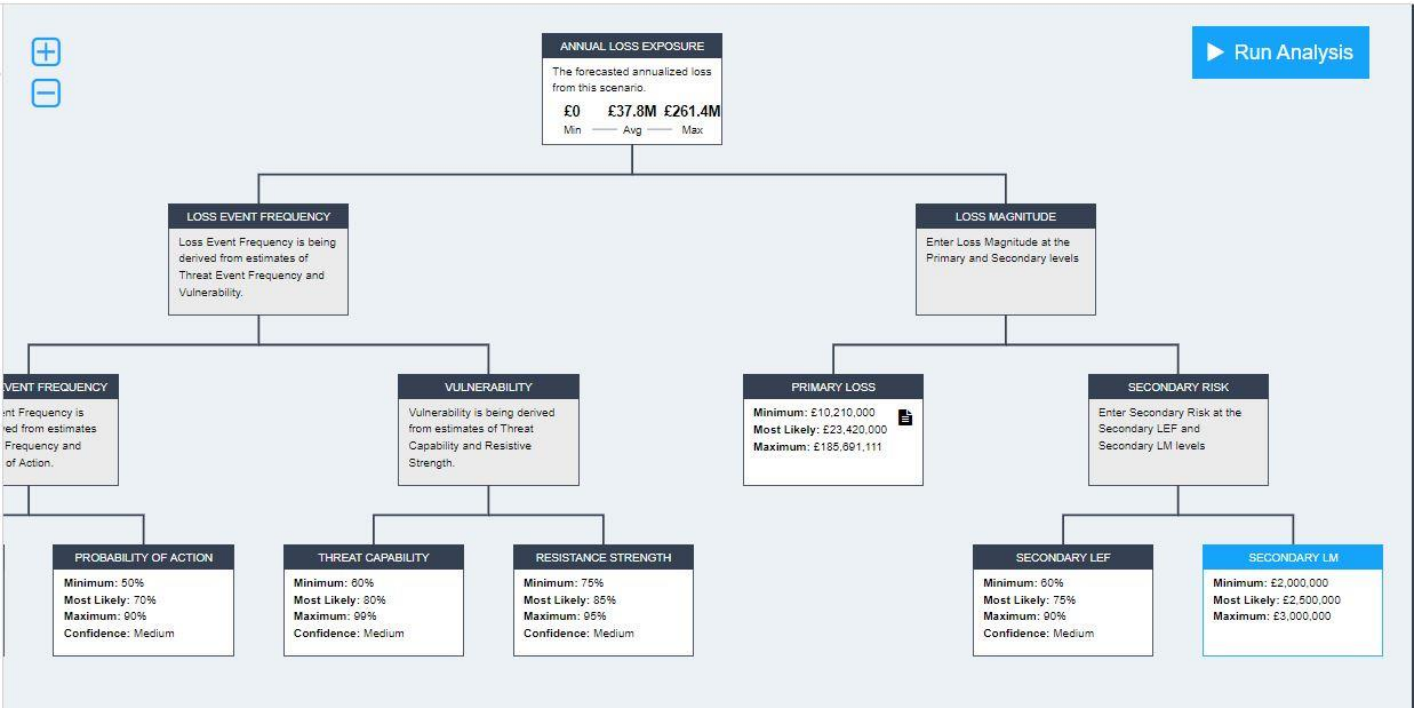

Figure 4 FAIR-U Analysis of British Airways Data Breach

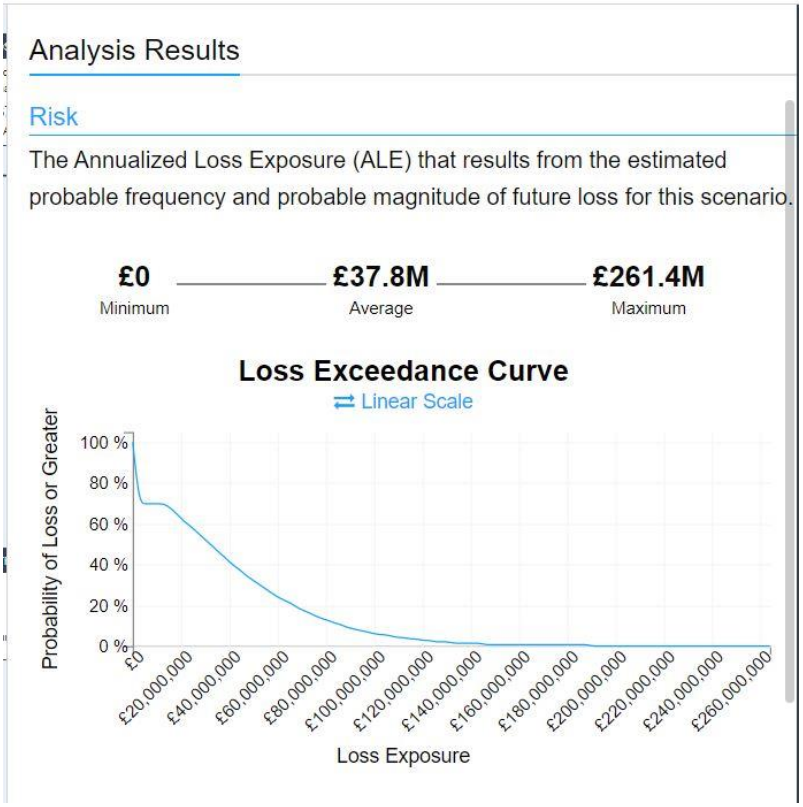

Figure 5 Loss Exceedance Curve

Figure 6 Summary of the results