IATA

Situational Analysis

Effective July 2015

2nd Edition

Table of Contents

Acknowledgement 3

1 **Introduction** 4

2 **Current Management Practices in Cyber Security** 6

2.1 IATA Member Airlines 7

2.2 System Suppliers 9

2.3 OEM (Original Equipment Manufacturers) 10

2.4 Consultants 10

2.5 Insurers 11

3 **Threats** 12

3.1 Intelligence and Threat Identification 13

3.2 Exposed System Examples and Vulnerabilities 13

4 **Responsibilities** 18

4.1 Airline Systems 20

4.2 Airline Data Management Responsibility 21

5 **Cyber Security Attack Vectors and Multivector Threats** 23

5.1 Network Intrusion 24

5.2 Malware Placement 24

5.3 Multivector Threats 25

6 **Regulation** 26

6.1 International Civil Aviation Organization (ICAO) 26

6.2 European Commission 27

6.3 United States 28

6.4 United Kingdom 28

7 **Conclusion and Recommendations** 29

7.1 Airline Security Culture 29

7.2 Industry Partnerships 30

7.3 Self-Audit and Network Documentation 30

7.4 Risk Assessment 30

7.5 Training 30

7.6 Reporting 31

7.7 Exercises 31

Glossary 32

Appendix A—Impacts and Methods 34

Appendix B—Defence Mechanisms 36

Appendix C—Current Stakeholder Groups and their Activities 37