The Current State of Cyber Security Readiness in the Aviation Industry

A matter of time and money: The impact of a cyber incident

Author: Sion Camilleri
Date: 18 September, 2014
© Durasee Services
www.durasee.com
# Table of Contents

About the Author ................................................................................................ 2
Foreword ............................................................................................................ 3
1 Executive Summary ........................................................................................ 4
2 Aviation Tomorrow ......................................................................................... 5
3 The Paradigm Shift ......................................................................................... 6
4 In Recent Events ............................................................................................. 7
5 The Known Threat .......................................................................................... 8
6 What is the Concern ....................................................................................... 9
7 Plans for the Future ...................................................................................... 10
8 Risk on the Radar ......................................................................................... 11
9 A Necessary Cost ........................................................................................... 12
10 Likelihood of Loss ....................................................................................... 13
11 Estimated Spending .................................................................................... 14
12 Conclusion .................................................................................................. 15
13 Recommendations ...................................................................................... 16
   13.1 Insurance Protection ............................................................................ 16
   13.2 Assurance Regime ................................................................................ 16
   13.3 Information Sharing .............................................................................. 16
   13.4 Notification and Reporting .................................................................... 16
   13.5 Metrics and Measurement .................................................................... 16
14 Future Work ................................................................................................. 17
References ....................................................................................................... 18
About the Author

Sion Camilleri is an independent cyber security consultant, and researcher with over 15 years’ experience, and currently based at Toulouse Business School, France.

Sion has a Batchelor of Science, double major in Applied Mathematics of Finance and Micro-economics, and Computer Science from University of Adelaide, Australia.

After completing his Master of Business Administration (MBA) in Aerospace Management, as part of his thesis with Jeppesen and Boeing Digital Aviation, he developed an economic impact analysis model to assess the various business risk of cyber threat to the aviation industry.

Sion is focused on cyber security issues for government, banking and finance, defence contractors, telecom operators, and other large multi-nationals clients. Sion specializes in technology threats and vulnerability assessments, and service model strategies for risk mitigation, cyber security prevention and remediation.

Currently Sion is developing cyber security insurance and emerging risk models for critical national infrastructure, transport, aviation, and space systems for aerospace clients.
Foreword

There is increasing technological integration of air traffic management (ATM), as satellite-based navigation and data networks become more available within the aircraft for the cockpit and passengers. New international initiatives such as SESAR and NextGen are aimed at creating the future “e-Enablement” of highly interoperable, and inter-connected aviation systems. To achieve this, new data exchange formats and System Wide Information Management (SWIM) are needed. Message and data exchange between systems will enable a vast increase in the amounts of information which can be shared. Networks will also require increased bandwidth for the traffic between ground-based SWIM compliant ATM systems and aircraft cockpit avionics.

Such leaps in technology do not come without risks, and as new standards develop, so does the technology required, and the risk of change. As part of this technology evolution there is an increase in the complexity, and a new dependence on information security for systems to ensure safety of air transport. Cyber security and risk assessment methodologies are needed to assess new possible threats to aviation. Existing risk methodologies used for aviation safety must now include cyber security, to perform industry wide identification and assessment of threats, risks, and vulnerabilities. To do this information sharing within the industry must occur, between aircraft manufactures, airlines and ANSPs (Air Navigation Service Providers). Business risks and mitigations can then be measured and prioritized in terms of economic impact to the industry.

Risk assessment can be used to calculate the costs on the basis of lost economic activity. This approach must take into account the costs to the aviation industry of implementing cyber security countermeasures, as well as the benefits, and costs of not doing so. Cyber security can then become a trade-off decision between cost-benefit and the impact of compliance versus performance. Security decisions should be risk-focused, balancing the possible economic benefit of cost savings which can also be achieved, against investment in prevention rather than corrective actions.
1 Executive Summary

Using the latest aviation industry figures, and cyber threat analysis trends, a number of revealing insights show what the true risk of cyber threat in the aviation industry.

The main results obtained and validated has been the use of the Gordon-Loeb model [1]. Although there are a number of limitations to this model in the context of the possible large losses in aviation, it has been possible to utilize means to account for these non-nominal conditions.

Other means, such as cyber security insurance are becoming more applicable to all sectors. As cyber event impacts are factored into the cost of business, the question of the cost of prevention through a mix of investment and insurance to spread risk becomes key. This strategy to spread the risk was shown to be successful, not only to reduce risk, but to save money, and generate value for the industry.

A consistent and coherent view of the risk is required to insure that the limited resources available to combat cyber threats are correctly allocated where they can produce the greatest value. The approach explored to calculate this risk and its impact has been to compare two relative measures of the cyber threat, from the perspective:

- The cost associated with cyber-attack, incidents, breaches, both internally and externally of the organisation to prevent and recover from after the fact.

- The total expected loss to the organisation from loss of business operations, costs of recovery, as well as to the direct impact to the user is required.

Only by taking the difference between these two approaches can it be possible to determine the overall impact to the economy, industry, and passengers. Using the approach of the Risk Factor Analysis (FAIR) developed by The Open Group [2, 3, 4], it has been possible to determine the relative strength of the controls in place to prevent the vulnerability on the basis of the financial impact.

The questions asked in this study, and by the aviation industry today is what the risk of a cyber-attack is, and what is the cost to prevent?

- By 2030, a cyber-attack could cost the economy a total of more than $9.5Bn
  - Cost to Airlines, Airports, ANSPs, and Manufactures could be $6.5Bn
  - Passengers loss in combined delay loss and impacts could be $3Bn
- From 2013, the gap in airline IT spending on cyber security requires a 275% increase
  - Cost of security per passenger should be $0.22 up from $0.08 at least
  - Airlines should be aiming for an cyber security budget of 6.5% of IT OPEX
  - Maximum loss spending is on average, 0.038-0.044% of airline revenue
- Total spending for all threats should be $900M yearly or 0.12% airline revenue
  - Between 2013-2030, $275-325M per year is needed to cover maximum loss
  - In 2013-2014 at least $630-$670M per year is required for all loss events
  - Of this $500M yearly or 0.07% of airline revenue is in operational spending

The approach of using the maximum single event loss for the industry shows that relative to the nominal conditions, so called High Impact- Low Probability (HILP) events do occur, and their impact can only be accounted for in terms of average likelihood of occurrence.

For the industry there remains the issue of aviation risk and how to spread maximum loss event which can impact the whole industry. As globally inter-connected organizations rely increasing on each other, to survive threats there must be the mechanism to spread risk on a local, regional, and international level.
2 Aviation Tomorrow

The aviation industry is now in an era of technological progress spearheaded by the modernization initiatives in Europe called SESAR [5], and NextGen [6] in the US. The aim is to improve efficiency through global connectivity of all air transport systems. Key to the success of these programs is to harness the maturity of information technology.

The success of SESAR and NextGen relies heavily on new information technology infrastructure projects, as well as the ability of chosen service provider’s to deliver value for money [7]. The value proposition rests on the argument increased data communication and inter-connectivity of air traffic management systems, will lead to sharing of larger amounts of information [8]. Greater access to information will in turn lead to faster and better decision making by airlines and air traffic controllers. Faster decisions can save time, that drives cost savings for the industry and passengers [9].

The belief of these tax-payer funded modernization programs is technology driven decision-making will create greater automation, optimization, and efficiencies. These measures are all aimed at reducing time consuming, and manual operations. Time savings will invariably translate into cost savings for airlines, airports, and air navigation service providers (ANSPs). The quicker the investment yields savings, the faster trickle-down effect which will eventually lead to lower fares for passengers [7].

First investment is needed to upgrade existing systems with increased computational power, faster networks, and larger data bandwidth to meet the future demand. To this end, technology companies, as well as the traditional aerospace and defence players are competing to be the new partners and service providers of aviation. On offer is the opportunity to develop solutions and operate services over the next 10 years [10].

However, return on investment in SESAR (€2.1Bn in R&D, €30Bn for deployment 2015-2023) [11, 12, 13] and NextGen ($40Bn over 20 years) [14, 15] is still a challenge to measure and justify [16, 17, 18, 19]. Even with Public-Private Partnership and risk sharing with government, the benefits to the wider industry and public are still being assessed [20, 21, 8]. To support the investment arguments, real gains in operational efficiency are needed to offset congestion [22, 23]. Targets have been set for SESAR to reduce flights costs by 50% [24] and for NextGen to cut delays by 41% in 2020 [25].

To achieve such ambitions targets there must be a huge leap forward in information sharing to realize the necessary gains in efficiency. It will take a unified effort across the aviation industry to move toward global system wide information management (SWIM) [26]. Proposed as far back as 1997, SWIM was adopted by ICAO in 2005 [27].

Since 2005, SWIM interoperability facilitates data exchange between systems using the aeronautical information exchange model (AXIM) [28]. SWIM is already enabling the exchange of new types of enriched data and message formats, using a range of open standard protocols [26, 29]. Creating SWIM compliant systems will mean the complete “e-Enablement” of aviation [30]. As e-Enablement extends the SWIM perimeter to aircraft and actors in the system, information becomes a risk factor [31].

Aircraft, airports, and air traffic control will now rely on SWIM for vast amounts of data needed for situational awareness. Systems will need to be highly reliable to ensure the level of quality and continuity of information. Information security (Confidentiality, Integrity, and Availability) [32] will now guarantee the safety of SWIM and air transport.
3 The Paradigm Shift

Information centric management of the airspace has long been the aspiration within aviation. As part of the future vision of the industry, and regulators, the by-word has always been safety first [33]. Safety only considers accidental failure, but not deliberate acts. In this information age of aviation, the over-arching requirements for cyber security are to protect both the systems and information, as well as safety [34, 35].

Targets have been set by SESAR and NextGen for factor of 10 increase in safety [36, 37]. In such a risk averse industry as aviation, the introduction of any new technology and innovation has always been met with skepticism and resistance, until safety was proven [38, 39]. Aviation has seen various innovations such as fly-by-wire [40], and use of composite materials, all encountered the same rigorous safety evaluations.

Aviation like other critical industries, such as nuclear, have developed a culture of safety methodologies [41]. These assurance mechanisms have been refined and improved steadily to reduce accidents and fatalities over the years [42, 43, 44].

No event damaged more the image of air safety than the terrorist attack of the 11th of September, 2001. In the wake of 9/11, the shift of aviation from safety-focus to a security-focus began [45]. The immediate recommendation was the increased level of physical security and airport screening procedures. In the last decade, there has been incredible advancement in security technologies deployed [46], such as x-ray, biometrics, machine intelligence and data analytics processing (so called Big Data). Many of these technologies were designed as anti-terrorism counter-measures and specifically developed for aviation and border protection applications [47].

The effectiveness of such physical security measures has not only strengthen the ability of aviation to prevent, and withstand such similar terrorist attacks from occurring in the future [48]. However, given nature of this asymmetric threat, it has only seen the threat against physical targets move towards easier, so called “soft” targets [49]. The threat is no longer just against the physical security of aviation, but now also aimed at weakening the underlying systems and means of providing physical security and safety. These more exposed and vulnerable systems are now the new risks to safety.

The very technologies which will herald this new era of modernization and passenger safety, provide benefits as well as new risks [50]. Traditionally safety risk has been addressed and mitigated through step-wise human procedural avoidance and preventative measures [51]. These safety measures were learnt over 50 years, through trial, error, measurement, and ultimately post-accident investigation [44, 52].

Today the rapidly increasing complexity and globalization of aviation systems, coupled with the introduction of new technologies requires cyber reliance [53]. Threats to aviation safety remain the same, now the new attack vector is also through cyber, as well as physical means. The risk is not only from physical faults and failing of parts, but from the computerized information processing and validation procedures [54].

New models for cyber security and information assurance and needed to identify unknown risk and impacts. These are the so called unknownunknowns [55]. As terrorism has shown, attempting to mitigate security risks in the same way as safety risk, can only counter the anticipated and expected threats, not the unexpected ones. What the “human-in-the-loop” approach neglects to consider, is threats which cannot be anticipated, also cannot be mitigated. Today, cyber security and the risk of taking the “human-out-of-the-loop” is the unknown-unknown.
4 In Recent Events

To date the number of cyber security incidents in aviation vary in cause, frequency, nature, severity, but most have little or no explanation. Some incidents are accidental, the result of human negligence. Whilst those which are truly deliberate can rarely be attributed to directly to nation states, terrorists, organized crime, or hacktavists [56].

Although such attackers exists, few examples exist. The earliest indications that aviation systems were vulnerable to cyber-attack occurred at least 15 years ago.

On March 10, 1997, a hacker broke into a Bell Atlantic telephone company, causing a crash that disabled the phone system at Worcester Airport for six hours [57]. This incident perhaps became the first cyber security incident in aviation.

According to US Department of Justice statements, the crash knocked out phone service at the control tower, airport security, the airport fire department, the weather service, and carrier systems that use the airport. Also, the tower’s main radio transmitter and another transmitter that activates runway lights were shut down, as well as a printer that controllers use to monitor flight progress.

The hacker, a Massachusetts teenager, was successfully prosecuted. In doing so, the teenager become the first juvenile charged in federal court with computer hacking.

“We dodged a bullet that day,” said Joseph Hogan, Area Manager for the Worcester airport’s air traffic control center.

Since this initial incident, reports of accidental, as well as deliberate cyber-attacks on airports and aviation systems have only started to increase.

Attacks against airports currently include Delhi, India in 2011 [58], Seoul, Korea in 2012 [59], Istanbul, Turkey in 2013 [60]. All these attacks caused airport systems outages on passport, baggage, check-in systems, forcing aircraft to be grounded.

Attacks aimed at the airports, are not only effecting ANSP’s, and airlines, but also passengers are being caught in the cross-fire. There are various reports of attacks against people using the airport wireless internet access points [61]. Previous studies investigating airport wireless systems have found vulnerabilities which not only expose passengers attack, but also allow airport systems to be directly accessed over unsecured wireless access points [62].

Most recently, The Center for Internet Security (CIS) in their 2013 annual report released on June 19, 2014 [63] cites cyber-attacks on a total of 75 airports in the U.S. Of the airports attacked, two airports had their systems successfully compromised.

The threat from deliberate and unexplained acts is now already enough to concern travellers, as questions start being asked. As the FAA experience their own share of incidents related to faulty systems and NextGen testing [64, 65, 66]. Airlines also are experiencing various unexplained incidents, such the American Airlines unexplained grounding 2,000 flights in April, 2013 [67].

To address the most pressing concerns of officials regard the public reports of cyber-attacks against aviation, the FAA has now made two notifications to Boeing. The first issued in November, 2013 [68], and another notification was made in the wake of the Malaysian Airlines MH370 disappearance, in June 2014 [69].
5 The Known Threat

Media reports of the FAA notifications to Boeing have spurred the belief the In-Flight Entertainment (IFE) system could be used to access cockpit systems [70]. This type of speculation focused on possible use of mobile, Wi-Fi, and other USB devices to provide access to the cockpit systems via the same shared on-board network used for the IFE. As conspiracy theories abound, they reflect a sense of public curiosity that prompted researchers and hackers alike to start investigating.

Since 2009, Dr Ben Mahmoud, and French researchers at ENAC are investigating the security of the proposed SESAR communications protocols [71, 72]. By 2011, issues had been raised publicly by the defence community to the FAA regarding known vulnerabilities and the ability to track aircraft and intercept communications [73, 74].

However, exploring the vulnerabilities that could exist in aviation systems from an outsider perspective is a challenge for non-industry insiders. It did not take many hackers and independent researchers in the security world long to make the wider aviation industry understand, and realize what was truly possible.

Then in 2012, Andrei Costin, a French researcher presented at the Black Hat Conference [75]. Not long after, similar cyber-attack scenarios were presented. The same year, by Canadian Brad Haines at DEFCON 20 [76]. More recently Hugo Teso, a Spanish researcher presented a mobile application which claims can be used to remotely control the aircraft [77, 78]. Since 2013, Dr. Lenders and his team from the Swiss Army and ETH Zürich have demonstrated a number of experimental attacks on NextGen communications protocols, interoperable with SESAR [79, 80].

Many of the ground-based attacks focus on intercepting, recording, replaying, manipulating, and injecting messages, as well as jamming and meaconing the signals. The vulnerable protocols targeted are typically TCAS, ACARS, ADS-B, and NOTAM. Attacks on GPS, GBAS, SBAS, and VSAT signals are also possible [84, 85, 86, 87].

Attacks generally rely on two aspects. Firstly, the fact radio communications between ground and aircraft are unencrypted, and can be incepted and re-broadcasted with similar equipment that airline and airports themselves use. Since there is no authentication, trust or signal protection established though cryptographic means, the content of messages can be manipulated, based on the compliant format. Standards for message formats are usually public, to promote open use, and made available from various government and industry groups such ARINC, ICAO, EUROCAE, and RTCA.

Secondly, use of unencrypted signals are less robust, so usually require beam-forming antenna and multi-path cancellation to reduce noise, and susceptibility to interference and jamming. This requires the use of multi-lateralization and multi-angulation, used to verify the location of the trusted signal or locate untrusted interference sources.

Inside the airport also, various other ground-based approaches also assess and perform attacks on actual air and ground-based systems themselves, some using the very same equipment or variants. Infrastructure attacks center on unprotected airport wireless links and insecure protocols, vulnerable embedded device firmware, as well as antiqued unsupported versions Microsoft Windows and other operating systems. Wireless links especially have been shown to provide access to back office networks and aircraft data loaders [62, 84]. The access via these networks has shown vulnerabilities in the TSA approved Threat Image Projection based x-ray and full body scanners [85, 86]. Penetration testing of reservation and booking systems have also recently shown to be vulnerable to expose passenger manifests [87].
6 What is the Concern

The goals of security researchers have been to assess what is possible in the future, and if there is an impact from cyber security on the safety of aviation. By trying to raise awareness of the issues in various conferences, they have also prompted both positive and negative reactions from within government, and industry insiders.

Skip Nelson, President of ADS-B Technologies: “We are quite familiar with the theory that ADS-B could be ‘spoofed,’ or barrage jammed by false targets. There’s little new here. In fact, just about any radio frequency device can be interfered with somewhat. I obviously can’t comment on countermeasures, but you should know that this issue has been thoroughly investigated and international aviation does have a plan.”

Most are already familiar with many of the issues of unencrypted radio communications [88]. As most aerospace and defence contractors also originally developed the same civilian equipment for military aviation systems, they are also aware of the solution to these problems – simply to encrypt all communications traffic in air between aircraft, as well as on ground [89, 90, 91]. But the FAA and airline industry argue otherwise.

For the moment, the FAA publicly states there will be no encryption [92]. In doing so, the FAA disagrees with using encryption, and all concerns from US Department of Defence [93], and the wider security community [94].

The main obstacle for the FAA and other authorities mandating the use of such sophisticated military equipment for civil use has been the cost [93]. Already the cost of airlines and aircraft upgrades for NextGen and SESAR compatibility is a financial burden many airlines can’t afford, after only just returning to profitability [95].

Although the level of technical vulnerabilities and inherent security of the system is still being debated [96, 94], FAA responses have gotten increasing dismissive. In August 2011 the FAA announced: “No cyber security event significantly degrades or disables a mission-critical FAA system.” [36].

One year later in August 2012 the FAA said “The ADS-B system is secure and fake ADS-B targets will be filtered from controllers’ displays. An FAA ADS-B security action plan identified and mitigated risks and monitors the progress of corrective action. These risks are security sensitive and are not publicly available. The FAA plans to maintain about half of the current network of secondary radars as a backup to ADS-B in the unlikely event it is needed,” [94, 88].

ITT Exelis the FAA contractor for ADS-B explained, “The system has received the FAA information security certification and accreditation. The accreditation recognizes that the system has substantial information security features built in, including features to protect against…spoofing attacks. [This] is provided through multiple means of independent validation that a target is where it is reported to be.”

As new technology enters the cockpit, such as EFBs [97, 98] this presents new security challenges. Device such as iPads used for EFB platforms can also be vulnerable to malware which may corrupt weight and balance calculations. Connectivity of the EFB through Bluetooth, WiMAX and other protocols provides access to the FMS which may create the risk of introducing malware directly into avionics systems.

Besides these air-borne and ground-based threats at the infrastructure level, the possibility of new application level attacks on SWIM itself could also now exist. These attacks could be aimed at flaws in the very message format, conformity, integrity, and content checking [99, 100, 28].
7 Plans for the Future

As program funding and progress announcements for SESAR and NextGen continue, so too have public and government concerns over cyber security [31]. By April 2013 in response to reports of Hugo Teso’s claims, the FAA stated [101]:

“The FAA is aware that a German information technology consultant has alleged he has detected a security issue with the Honeywell NZ-2000 Flight Management System (FMS) using only a desktop computer. The FAA has determined that the hacking technique described during a recent computer security conference does not pose a flight safety concern because it does not work on certified flight hardware. The described technique cannot engage or control the aircraft’s autopilot system using the FMS or prevent a pilot from overriding the autopilot. Therefore, a hacker cannot obtain “full control of an aircraft” as the technology consultant has claimed.”

Scott Sayres from Honeywell stated: “We take this seriously and we're going to work to assess this. But as Teso readily admits, the version he used of our flight management system is a publicly available PC simulation, and that doesn't have the same protections against overwriting or corrupting as our certified flight software.”

Rockwell Collins also commented: “Today’s certified avionics systems are designed and built with high levels of redundancy and security. The research by Hugo Teso involves testing with virtual aircraft in a lab environment, which is not analogous to certified aircraft and systems operating in regulated airspace.”

In an attempt to demonstrate action, new objectives now state cyber security will be addressed by improvements funded as part of SESAR and NextGen:

Most recently, in May 2014, SESAR announces the start of “the cyber-security study, the results of which will be available in the first quarter of 2015, is expected to provide SESAR with an assessment of threats and vulnerabilities within the ATM system, a SESAR-targeted cyber-security framework, a maturity assessment and finally a cyber-security strategy. [37]

This level official recognition and awareness confirms cyber security as a real issue, and demanded a response from within the industry. Airlines began receiving assurances from aircraft manufactures of product safety and cyber security [102].

Speaking at the NATO Review in December 2013, Jeff Kohler, Vice President of International Business Development for Boeing, said when asked what will be the biggest threats in the next 10 years: “I don’t think we still understand critical infrastructure protection and how cyber can affect that. From our commercial aircraft side we’re very concerned about it. As commercial aeroplanes become more and more digital and electronic, we have actually started to put cyber protection into the software of our aeroplanes. If they enter an airport environment, they are starting to exchange information and so we have to be able to protect the aircraft’s software itself, so there’s a lot of issues coming down the road just on cyber alone.” [103].

At the same time, the definition of what is cyber security in the context of aviation is still being defined. There remains a need for the aviation industry to state what cyber security is, and is not, within the context of the roles each player has in the industry.

Cyber security is transcending traditional information security, and the organizational boundaries. The threat is no longer directed against individuals. As organizations and industries face the same imminent threat, they must share information in ways which coordinate action and response at national, regional, and international levels.
8 Risk on the Radar

Since 2013, industry bodies began to coordinate and make their message to law makers heard. From the AIAA the message was clearly cyber security must be defined in terms of a risk-based approach. There must be an understanding the threat, qualification risk, and then prioritization of the limited resource and actions [104].

On 8th of July, 2014, IATA held the first joint ICAO Cyber Security Workshop to raise awareness with member airlines on actions to take [105]. Using the occasion CANSO and IATA proposed threat and risk assessment guidelines [106], as well as a Cyber Security Toolkit [107]. From the perspective of IATA and the aircraft manufactures, the belief is industry wide information sharing is needed to ensure pro-active prevention and protection [108]. As the industry unites to defend itself, the question is who will pay if a cyber-attack occurs. From the value chain perspective airlines are looking towards manufactures [109]. Leading the efforts in this direction is Fred Schwien, Director of Homeland Security Programs & Strategy at Boeing:

“The aviation sector is also modeling an information sharing initiative after the FS-ISAC. The aviation ISAC will be collocated with the Air Domain Intelligence Integration Center in the Transportation Security Administration’s secure flight facility in Annapolis Junction, just outside Fort Meade, the location of the National Security Agency. We get classified briefings from the intelligence agencies including the FBI and TSA. We use that information to protect the networks across industry and that’s very effective. The groups will bring an unprecedented level of information sharing between government and industry.” [110, 111].

Whilst some industry leaders call for risk-awareness through information sharing, this is only one strategy. Other leader’s claim what the industry needs now is immediate risk protection and limitation from the potentially bankrupting costs of cyber incidents.

Risk protection will provide time and ensure the financial resources are available to implement the necessary information sharing prevention strategies. With this aim, there have been new calls on the Obama administration to pass legislation to limit the liability from cyber incidents [112]. Learning from the lessons of post-September 11, the crippling costs of terrorism insurance required government intervention in the market to provide protection to airlines to limit their losses [113, 114].

In the same way the Terrorism Risk Insurance Act (TRIA) [115, 116], cyber insurance can be used to quantify the risks and costs of impact on aviation. Although there as varying estimates of the probability of cyber-attack in the transport, aerospace, and defence industry [117, 118].

Limiting loss is by far the most important action to be taken, for an industry which is only just starting to recover from a series of events including deregulation, consolidation, 9/11, SARS, a Volcano, and a financial crisis [119].

Cyber insurance provides a means of financial mechanism to spread and transfer the risk to limit the losses incurred. Within the insurance industry, understanding of the risk for technology dependence industries is growing. According to Lloyds, cyber risk has moved from position 12 (malicious) and 19 (non-malicious) in 2011 to the ranking of 3rd highest risk overall [120]. Other insurers have also changed their rankings [121].

This approach to risk management and limitation is gaining appeal within a number of industries. Already a number of organization in aviation, especially airlines are taking cyber coverage [122], but take-up in transport sector is slow, if not the slowest [123].
A Necessary Cost

In a 2011 FAA sponsored report, most of the 12 airports surveyed indicated that their airports do not insure cyber-related risks at all [124].

In a scenario proposed by Ponemon Institute in a 2014 study, the impact of a cyber-attack being launched against the GPS systems of a major US airline was assessed [125]. It was speculated the problem is detected, and grounds all flights and airports for an indefinite period of time until the systems are repaired. The time distribution is estimated with probabilities of occurrence over 24 month period. Based on this distribution, the study extrapolated an average probability of occurrence over the 24 months to be 2.18%. The maximum exposure was then calculated by taking the maximum loss, which yields an average value of loss to be $127M. Using Expected Values (EV) equal to Likelihood of Occurrence multiplied by Maximum Exposure, this scenario implied cyber security could cost $1.35M per year.

In the same study by Ponemon an industry wide study, containing at least 18 transport sector respondents. In the survey 64% of respondents said they do not have cyber-security insurance policy (or set of policies). Of this group, 41% said they were not planning to buy cyber-insurance in the next 24 months. Most chose not to have cyber insurance because the premiums were too high, coverage is inadequate based on exposure, too many exclusions, restrictions and uninsurable risks [125].

Marsh & McLennan Companies estimated in 2014 the U.S cyber insurance market at $2 billion in premiums. The European market is currently a fraction of that, at around $150 million, but is growing by 50 to 100 % annually [126]. In testimony before the United States Senate Committee on Commerce, Science & Transportation, Peter Beshar, Executive Vice President and General Counsel for Marsh stated [123], specifically mentioning the transport sector:

- Cyber risk is assessed using a proprietary Information Security and Privacy Self-Assessment, based on the information security standard ISO 27001
- The cost of cyber insurance varies depending industry, but on average $1 million in protection ranges from about $20,000 to $25,000
- The average price per million dollars of coverage for a cyber-policy actually dropped in 2013 in a number of sectors, including financial institutions, utilities
- Premiums are low but increasing for communications and transportation
- Take-up rates in transport are the lowest of all industries at just 1%-5%
- Coverage rates are 11-12% between 2011 to 2013, for premiums of $10,000

Higher premiums for the transport industry reflects the complex nature of policy assessment and higher risk of cyber-attack. Insurers have had difficulty pricing cyber risk, and there can be large differences (as much as 25%) between the premiums charged by two different carriers to insure the same risk [126].

From 2014, Gartner claims cyber-insurance remains a relatively nascent industry, with only 50 or so insurers now offering policies, mostly in the United States [127]. Beginning in 2014, German insurance giant Allianz has partnered with Thales to perform the assessment.

Allianz says its premiums for 10-50 million euros in protection run about 50,000-90,000 euros in annual premiums. For protection of over 50 million euros, companies can get coverage up to 300 million euros through co-insurance policies involving multiple underwriters [126, 128].
10 Likelihood of Loss

Robert Parisi, head of cyber products at Marsh says “It is a difficult risk to price by traditional insurance methods as there currently is not statistically significant actuarial data available,” [126]. The limits of cyber liability being purchased vary widely depending on the industry type, firm size, as well as IT and security budgets required.

According to Gartner the global IT Spending Forecast was $3.7Tn in 2013, putting the overall security technology and services market at $US67.2Bn. Spending on cyber security as part of the overall technology budget is then by deduction at 1.8%.

Visiogain has assessed that the value of the global cyber security market in 2014 will reach $76.68Bn [132]. ABI Research estimated that cyber security spending for critical infrastructure alone to be $US46Bn in 2013 [133]. Other estimates from M&M put the future cyber security market at $95.60Bn in 2014 to be $155.74 billion by 2019, with CAGR of 10.3% from 2014 to 2019 [134]. If correct, this could mean cyber security spending could 2.6% of technology spending by 2015.

Gartner already states Retailers spend 4% of their technology budgets on security, compared with 5.5% for banks and 5.6% for healthcare companies. [135, 136, 137].

According to Lufthansa Airline IT was worth $10Bn in 2013 [138], based on global airline revenues of $638Bn [139] that’s only 1.7% spent on airline IT. In 2014, SITA estimates of airline information technology spending to be at 2.2% of overall revenue (breaking down at 1.4% OPEX, 0.8% CAPEX) [140], in line with Gartner [137]. In 2014 IATA expect $746 billion in revenue [141], this puts IT spending at $16.4Bn

Similarly, in 2013 the SITA estimates for airports technology spending from the ACI (Airport Council International) are 5.43% of revenue. On revenues of $110.9Bn, this equates to $6Bn for airports globally, with CAGR of 2.8% since 2010 [135].

Visiogain have also assessed that the value of the global aviation cyber security market covering Airports, Airlines & Air Traffic Management (ATM) will reach $1.73Bn in 2014 with a CAGR of 5.4% [136]. In this analysis the sub-markets for ATM is 8.0% ($138.4M), Airlines are 42% ($726.6M), and Airports are 50% ($865M). This puts the aviation cyber security market segment at 2.25% of the global cyber security market, or $1.5Bn based on Gartner figures, or $2.2Bn from M&M figures.

In April, 2014, Jamie Dimon, CEO of JPMorgan, the largest U.S. bank said by the end of 2014 annual cyber-security budget will rise to $250 million from $200 million in 2012 and 2013 [137]. JPMorgan will have about 1,000 people focused on cyber security, compared with 600 people two years ago. Applying Gartner measures, JPMorgan with revenue of $96.60Bn in 2013 may spend 6.3% ($6Bn) on technology.

According to Howard Rubin [145], US banks spend from $7 to $10Bn, which implies JPMorgan is spending close to 10% of revenue on technology. A more likely scenario is JPMorgan doubled security spending to take first mover advantage, ramping up now reducing the cost of net present value of investment [146]. For this claim by JPMorgan to be consistent, the budget for cyber security would be estimated at 2-3% of their current technology spending, or 2% of global revenue.

Since aviation only spend 2.2% of global revenue on IT, this reveals the gap in aviation cyber security spending. On Visiogain estimates this requires a security budget of 5.3% from airlines IT and 12% from airports IT. Using models such as Gordon-Loeb for calculating the cost investment in security at 37% of total loss [139, 140, 1, 141] this level of spending in aviation implies mitigation of total loss close to $5bn.
11 Estimated Spending

For 2013, taking the Gartner estimate of 4% cyber security spending from technology budgets [131, 132, 133], an evaluation of the impact of doubling the security budget over 24 months to end of 2014 can be made. This change in budget will assess if current spending was sufficient now or will be in the future. Only operational expense (OPEX) will be considered to remove capital (CAPEX) variations.

Combining the SITA 2013 and 2014 estimates of airline information technology spending at 2.2% of overall revenue (1.4% OPEX, 0.8% CAPEX) [134], in line with Gartner [133] the following figures are attained. Note there is also an industry trend to move towards operational rather than capital investment models as cloud computing and outsourcing shift the spending on technology and security resources.

Based on the 2013 figures, the estimated industry average for airline IT and security budgets required today to bring the future budget gap to 0% for the best case:

![Cyber Security Budget Estimates to mitigate Total Loss](image)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Air France KLM</td>
<td>3,000,000.00</td>
<td>3,000,000.00</td>
<td>0%</td>
<td>3,000,000.00</td>
<td>3,000,000.00</td>
<td>0%</td>
</tr>
<tr>
<td>Emirates Airlines</td>
<td>5,000,000.00</td>
<td>5,000,000.00</td>
<td>0%</td>
<td>5,000,000.00</td>
<td>5,000,000.00</td>
<td>0%</td>
</tr>
<tr>
<td>Lufthansa Airlines</td>
<td>7,000,000.00</td>
<td>7,000,000.00</td>
<td>0%</td>
<td>7,000,000.00</td>
<td>7,000,000.00</td>
<td>0%</td>
</tr>
<tr>
<td>American Airlines Group</td>
<td>9,000,000.00</td>
<td>9,000,000.00</td>
<td>0%</td>
<td>9,000,000.00</td>
<td>9,000,000.00</td>
<td>0%</td>
</tr>
<tr>
<td>Qatar Airways</td>
<td>11,000,000.00</td>
<td>11,000,000.00</td>
<td>0%</td>
<td>11,000,000.00</td>
<td>11,000,000.00</td>
<td>0%</td>
</tr>
<tr>
<td>Air Canada</td>
<td>13,000,000.00</td>
<td>13,000,000.00</td>
<td>0%</td>
<td>13,000,000.00</td>
<td>13,000,000.00</td>
<td>0%</td>
</tr>
<tr>
<td>Japan Airlines</td>
<td>15,000,000.00</td>
<td>15,000,000.00</td>
<td>0%</td>
<td>15,000,000.00</td>
<td>15,000,000.00</td>
<td>0%</td>
</tr>
<tr>
<td>Air New Zealand</td>
<td>17,000,000.00</td>
<td>17,000,000.00</td>
<td>0%</td>
<td>17,000,000.00</td>
<td>17,000,000.00</td>
<td>0%</td>
</tr>
<tr>
<td>Delta Airlines</td>
<td>19,000,000.00</td>
<td>19,000,000.00</td>
<td>0%</td>
<td>19,000,000.00</td>
<td>19,000,000.00</td>
<td>0%</td>
</tr>
<tr>
<td>American Airlines</td>
<td>21,000,000.00</td>
<td>21,000,000.00</td>
<td>0%</td>
<td>21,000,000.00</td>
<td>21,000,000.00</td>
<td>0%</td>
</tr>
<tr>
<td>China Southern Airlines</td>
<td>23,000,000.00</td>
<td>23,000,000.00</td>
<td>0%</td>
<td>23,000,000.00</td>
<td>23,000,000.00</td>
<td>0%</td>
</tr>
<tr>
<td>Delta Airlines</td>
<td>25,000,000.00</td>
<td>25,000,000.00</td>
<td>0%</td>
<td>25,000,000.00</td>
<td>25,000,000.00</td>
<td>0%</td>
</tr>
<tr>
<td>Air Berlin Group</td>
<td>27,000,000.00</td>
<td>27,000,000.00</td>
<td>0%</td>
<td>27,000,000.00</td>
<td>27,000,000.00</td>
<td>0%</td>
</tr>
<tr>
<td>China Eastern Airlines</td>
<td>29,000,000.00</td>
<td>29,000,000.00</td>
<td>0%</td>
<td>29,000,000.00</td>
<td>29,000,000.00</td>
<td>0%</td>
</tr>
<tr>
<td>Southwest Airlines</td>
<td>31,000,000.00</td>
<td>31,000,000.00</td>
<td>0%</td>
<td>31,000,000.00</td>
<td>31,000,000.00</td>
<td>0%</td>
</tr>
<tr>
<td>British Airways</td>
<td>33,000,000.00</td>
<td>33,000,000.00</td>
<td>0%</td>
<td>33,000,000.00</td>
<td>33,000,000.00</td>
<td>0%</td>
</tr>
<tr>
<td>Air China</td>
<td>35,000,000.00</td>
<td>35,000,000.00</td>
<td>0%</td>
<td>35,000,000.00</td>
<td>35,000,000.00</td>
<td>0%</td>
</tr>
<tr>
<td>Ryanair</td>
<td>37,000,000.00</td>
<td>37,000,000.00</td>
<td>0%</td>
<td>37,000,000.00</td>
<td>37,000,000.00</td>
<td>0%</td>
</tr>
<tr>
<td>Jetblue Airways</td>
<td>39,000,000.00</td>
<td>39,000,000.00</td>
<td>0%</td>
<td>39,000,000.00</td>
<td>39,000,000.00</td>
<td>0%</td>
</tr>
<tr>
<td>Alaska Airlines</td>
<td>41,000,000.00</td>
<td>41,000,000.00</td>
<td>0%</td>
<td>41,000,000.00</td>
<td>41,000,000.00</td>
<td>0%</td>
</tr>
<tr>
<td>Air Asia</td>
<td>43,000,000.00</td>
<td>43,000,000.00</td>
<td>0%</td>
<td>43,000,000.00</td>
<td>43,000,000.00</td>
<td>0%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Region</th>
<th>Security as % of IT</th>
<th>Security CAPEX</th>
<th>Security OPEX</th>
<th>IT as % of Revenue</th>
<th>IT CAPEX</th>
<th>IT OPEX</th>
<th>Security per PAX – low to high ($)</th>
<th>Underspending– low to high ($)</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>3.25%</td>
<td>71.43%</td>
<td>28.6%</td>
<td>2.1%</td>
<td>1.50%</td>
<td>0.6%</td>
<td>0.01-0.08</td>
<td>60%-95%</td>
</tr>
<tr>
<td>Europe</td>
<td>6.5%</td>
<td>63.6%</td>
<td>36.4%</td>
<td>2.2%</td>
<td>1.40%</td>
<td>0.8%</td>
<td>0.22 (required)</td>
<td>0%-85%</td>
</tr>
<tr>
<td>Asia</td>
<td>100%</td>
<td>-7.83%</td>
<td>7.83%</td>
<td>0.1%</td>
<td>-0.1%</td>
<td>-0.2%</td>
<td>22-2.75x</td>
<td>60-10%</td>
</tr>
</tbody>
</table>

Table 1 – Security Spending
12 Conclusion

Visiongain have assessed that the value of the global aviation cyber security market covering Airports, Airlines & Air Traffic Management (ATM) will reach $1.73Bn in 2014 with a CAGR of 5.4% [136]. These estimates put the aviation cyber security market segment at 2.25% of the global cyber security market according to Visiongain.

In this analysis the sub-markets for ATM is 8.0% ($138.4M), Airports are 42% ($726.6M), and Airlines are 50% ($865M). Recalling the SITA estimates for aviation IT spending [134, 135], using Visiongain estimates this implies a security budget of 5.3% from airlines IT and 12% from airports IT budgets respectively.

In 2014, SITA estimates of airline IT spending to be at 2.2% of the $746Bn in overall revenue (breaking down at 1.4% OPEX, 0.8% CAPEX) [134], in line with Gartner [133]. That is OPEX is 63% of the total IT budget, and assumed to be the same for security.

This implies Visiongain estimate cyber security budget in airlines at 5.3% of the 2.2% (OPEX plus CAPEX) taken for IT from 2014 revenue. In other words, 0.12% of airline global revenue should be spent on cyber security. Focusing on the OPEX costs for cyber security, this can be estimated at 0.07% of airline global revenue in 2014, or approximately $522M.

Based on the results attained by analyzing the airline spending to mitigate loss, a comparison can be made of the calculation by Visiongain. This result reveals $660M should be spent on operational security budgets. This result shows a best case 26% increase on the VisionGain estimate and the approach used to calculate aviation cyber security market.

This also demonstrates that calculating the cyber security market value by the cost of investment in security required to mitigate loss is also valid. This shows the cost of mitigation or market size can be based on the Gordon-Loeb model use of 37% of total expect loss.

Conversely, applying models such as Gordon-Loeb for calculating the cost investment in security at 37% of total loss [139, 140, 1, 141] can be used to determine what the total loss is expected. By reversing the calculation, the estimate of the market size or cost of mitigation can be used to estimate total loss.

Based on the Visiongain estimates, this reveals a total loss expected for all aviation of $4.68Bn in 2014. Taking the sub-markets this estimate reveals a yearly total loss of $2.3Bn for airlines, $1.96 for airports, and $374M for ATM.

Taking the airline loss for the year, and the likelihood of a single attack, according to the average cost of the combined nominal and non-nominal loss for attack between 2015 and 2020, this is consistent at $2.22Bn, but could be as much as 26% higher at $2.8Bn.

There is an optimum range of investment required between 0.038-0.044% of airline global revenues per year, or on average $270-320Mn per year from 2014 to 2030. The cumulative yearly rate of investment required by airlines in cyber security. This investment is the amount of required security spending by airlines can offset the nominal maximum single event loss, mitigating the primary loss due to business impact.

Similar to calculating the insurance premium, the break-even point for the investment in cyber-security is when the expected loss will occur. Following this, the break-even point is in 2025, after which point positive rates of returns of 14% from the security investment can be gained.
13 Recommendations

13.1 Insurance Protection
At the present moment, the level of coverage required for maximum loss events due to cyber
remains critical. In the recent events, both accidental and deliberate, there is an absolutely
necessity for insurance in aviation. History has shown the risk of terrorism and change in
technology in aviation requires a step-change in the level of protection afford to passengers for
compensation, and likewise to the industry to survive. Only through comprehensive insurance
coverage for such cyber incidents can aviation develop the required approach to allocate the
resources needed in prevention.

13.2 Assurance Regime
In order to provide protection to aviation though the use of insurance, a compliance and audit
regime must be put in place to create industry baseline. Not only for the benefit of the insurance
industry to have a basis on which to benchmark and measure risk and premiums, but also to
have an industry minimum in terms of capability. There must be a minimum level of capability
set in the industry to respond to the threat. What is lacking at the moment in all industries is the
level playing field and sense that there is a common approach to cyber security risk analysis and
use of countermeasures. Industry approaches exist in the form of NIST SP 800, and ISO 27001
control frameworks. However, these standards do not mandate industry guidelines or
certification. Oversight of the effectiveness of security measures once deployed in operation
environments such as aircraft, is needed over time. The threat, unlike the aircraft is not static
once built, its dynamic and ever changing in the environment.

13.3 Information Sharing
Cyber security requires an approach which is based on information sharing and transparency to
gain full situational awareness of the threat and mitigations as fast as possible. As the threat is
able to adapt once the countermeasure is applied, and learn how to overcome them, it is
essential to coordinate effort as the resources and skills required can overwhelm individual and
isolated targets. Any attempt to conceal and isolate the approach to prevention will inevitably
lead to organizations, industries, and individuals being singled out and targeted. The greatest
strength and form of defence to prevent this type of threat is through united and coordinated
sharing of information.

13.4 Notification and Reporting
Collection of cyber events using standard codes from IATA, ICAO, FAA, and Eurocontrol is also
required to provide visibility of the threat landscape, and the activity on a real-time basis. Not
only is the level of alerts and notification required, on an infrastructure level, but also on a human
level. There must be real-time information exchange protocols developed to allow systems to
communicate, but there must also be forum to raise and inform issues which require human
intervention, analysis, and decision making. Fast decision making is key to maximize the value
of acting in time.

13.5 Metrics and Measurement
Cyber risk requires a strategy which is able to take event driven data and apply metrics that can
be used to make automated and intelligent decisions on the allocation of resources. Only through
measurement of the strength or success of counter measures, and the effectiveness of
measures and resources can the threat be countered.
14 Future Work

As part of this work, and the techniques developed, there remains many still to be answered questions, and alternative approaches to be explored.

The system level analysis models developed and proposed can only help assess high level risk, and where to allocate resources to most efficient mitigate identified risk. This is required in the first instance to determine identify the risk where to allocation resources. Future work could also investigate the portfolio theory approaches to spreading cyber risk. Although at present the level of information on claims, and investment in cyber prevention, insurance, mitigation and recovery remains limited. This is the challenge to develop more robust cost and impact models for cyber-attack, which is currently being faced by the insurance industry.

However, such models cannot determine if the threat scenario is creditable, or how to best spend the allocated resources in terms of most effective countermeasures. What is still required at an operational level is the technical vulnerability models, able to apply the threat scenarios to the implementation of the systems. By taking threat scenarios and allocating the risks to the underlying systems in aviation, only then can the threat be asseses as creditable to expend resource to counter.

All the possible paths of attack must be assessed to determine if and how the threat scenario can be achieved. Only then can the cost of mitigation under each branch on the attack be determined, based on the counter measure coverage, and the mitigating controls in the environment.

To achieve this, threat scenarios will need to be combined with safety analysis techniques such fault-tree analysis (FMEA). As such safety barriers provide natural defence for security, these countermeasure provide a ready and available means to verify if security events are possible. Based on the results of this analysis, it is clear that safety will be a consequence of security events, rather the inverse.

Most importantly, in the future the security risk analysis must prove that safety barriers are also not broken in the course cyber security events. This type of unified methodology for safety and security is somewhat of a holy grail for aviation, aerospace, nuclear, and other safety critical industries.

Nevertheless, through the analysis and development of models to systematically and exhaustively assess the combinations of attack-trees, branches, and paths there could be the basis for cyber assurance in aviation. However likely that the threat is neutralized due to the complex and time consuming level of attack required, the risk will be low, be never fully mitigated.

In future, it appears only such an exhaustive multi-step attack assessment will provide aviation with the methodology capable of assuring, certifying, and accrediting systems and equipment to the levels achieved in safety today.
References


CAPA: Centre for Aviation, "NexGen, SESAR values quantified in new study but airline question remain unanswered," CAPA: Centre for Aviation, 2011.


[34] National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity, version 1.0," national Institute of Standards and Technology (NIST), 12 February 2014.


[61] Trusteer, and IBM company, "Citadel Trojan Targets Airport Employees with VPN Attack," Trusteer, and IBM company, 12 August 2012. [Online]. Available:


[75] A. Costin, "Ghost is in the Air(Traffic)," in Black Hat, Las Vagas, July 2012.


