MARSH

# Client Alert

NOVEMBER 2018

# Data Breach - Leading Airline in Asia

A recent data breach has once again highlighted the vulnerability of the aviation industry. In 2018 alone, we've seen similar attacks on other airlines across the globe.

## Vulnerabilities in the Aviation Industry

The industry has a very complex and interconnected digital ecosystem – one that is made up of several key third-party service providers, suppliers, and vendors – see Figure 1. Unfortunately, the number of touchpoints and blind spots will only continue to grow and the onus remains on the airline itself to securely handle sensitive personal data and manage the granted access of every stakeholder.

### An airline should be most concerned with the following:

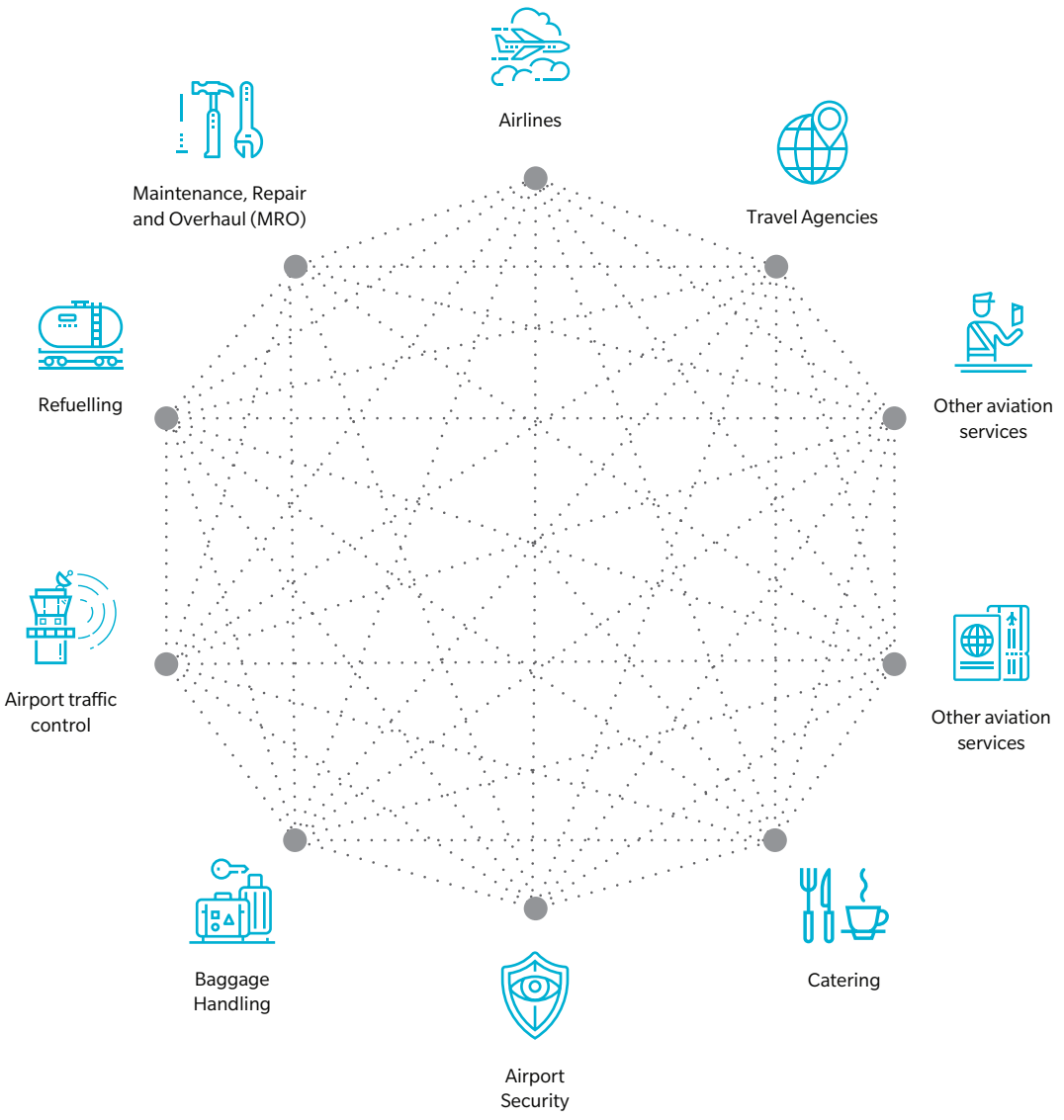
- Aircraft avionics, entertainment system
- Airport infrastructure
- Air traffic control / air navigation service provision
- Aviation liability costs for delays and cancellations
- Aviation technical records
- Corporate IT system
- Electronic flight bag
- Flight operations system
- Frequent flyer fraud
- Manufacturer's maintenance records
- Reservation system
- Supply chain

Even a superior IT security system and diligent cyber enterprise risk management can still leave a residual risk for data breaches to happen.

FIGURE 1

## Complex Digital Web of the Aviation Industry

**SOURCE:** MMC ASIA PACIFIC RISK CENTER




## Defining Cyber Risks in the Aviation Industry

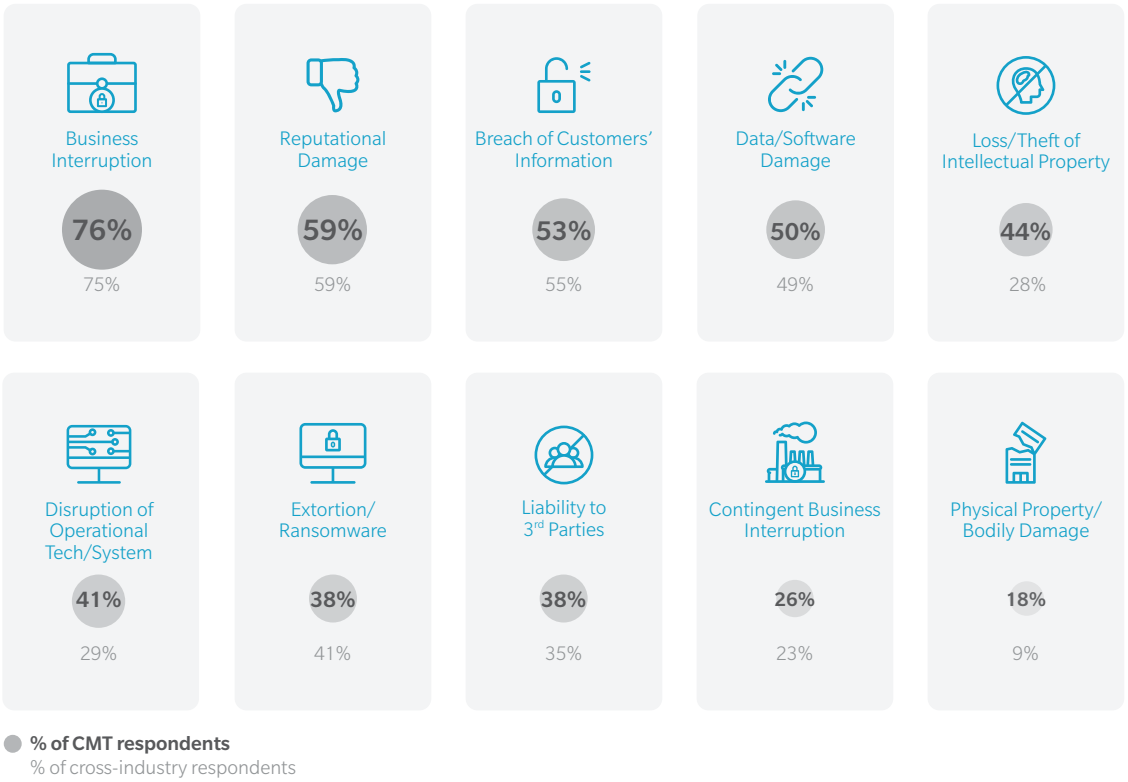
Cyber risks can materialize into a number of loss scenarios and understanding these starts with the assessment of cyber loss events, consequences and threat actors.

According to our latest Marsh Microsoft Global Cyber Risk Perception Survey, business interruption (76%) and reputational damage (59%) are the major perceived cyber loss scenarios in the aviation industry – see Figure 2. The interconnectivity and complexity of operations, as well as its intricate link to the economy as a critical national asset and infrastructure makes airlines more vulnerable to the loss/theft of intellectual property (44%) and the disruption of operational tech/system (41%), when compared to other industries.

FIGURE 2

## Top Cyber Loss Events with Largest Perceived Impact

**SOURCE:** MARSH MICROSOFT GLOBAL CYBER RISK PERCEPTION SURVEY 2017




The vast of amount of strategic IP in the Aviation industry – from commercial to those of national interests –incentivizes sophisticated threat actors to target them. A recent attack by APT33 (a hacker group identified by FireEye as being supported by the government of Iran) had sent spear-phishing emails to workers in the Aviation industry as part of a cyber espionage operation to collect information on Saudi Arabia's military aviation capabilities.

The large amount of assets at stake and the convergence of information and operational technology and systems have led to massive financial losses during cyber breaches. In May 2017, one of world's largest airlines faced an IT system failure that resulted in the cancellation of 726 flights over three days and a final bill of £100 million, all on top of the reputational damage it suffered. The financial impact of a cyber breach in the Aviation industry is one of the highest and more than 80% of the aviation and aerospace companies perceive direct losses to be more than $1 million per case, as compared to a cross-industry average of 65%.

Internal human-induced threat actors – perceived by a combined 61% of aviation and aerospace respondents compared to cross-industry average of 31% - are of the utmost concern to the Aviation industry. With the complexity and interdependency embedded within business operations, these threat actors are difficult to predict and anticipate.

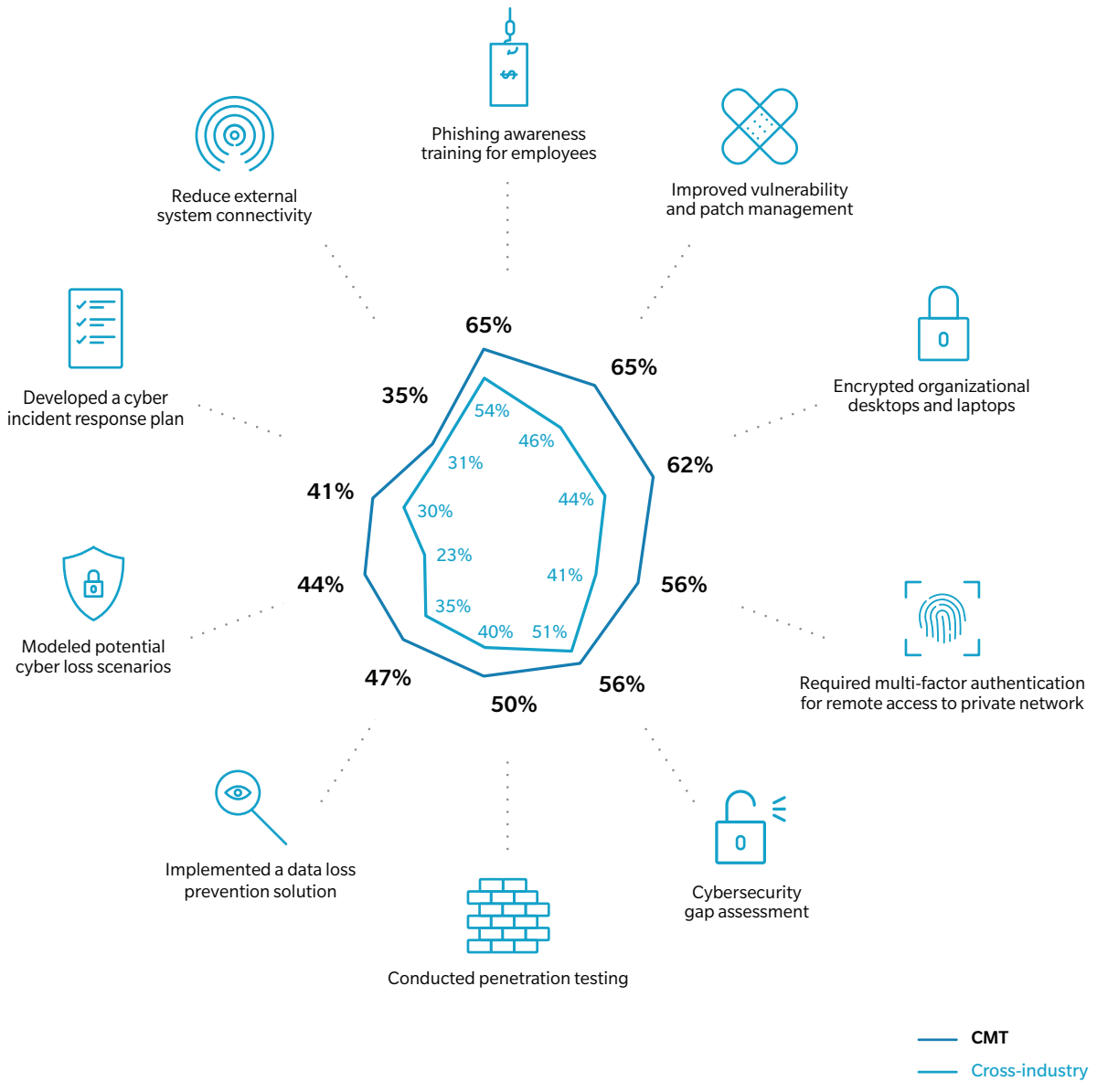
## Call to Action

Airlines need to stay attuned to the latest cyber threats and the available tools at their disposal in order to minimize occurrence and impact of cyber events. On average, the Aviation industry has taken more proactive measures than other industries, but they are still largely centered on basic preparation and prevention – see Figure 3. More can certainly be done on responses.

FIGURE 3

## Top 10 Cyber Risk-related Actions Taken by Aviation and Aerospace Companies in the past 12-24 months

SOURCE: MARSH MICROSOFT GLOBAL CYBER RISK PERCEPTION SURVEY 2017




While a superior IT security system and an all-encompassing cyber risk strategy are essential, no companies are immune to cyber breaches. Airlines must be cognizant of the heightened probability of a breach, limit their exposure in accordance to their appetite and financial conditions, and quantify the amount of investment necessary to close gaps and vulnerabilities.

The recent spate of high-profile data breaches within the Aviation industry has increased overall awareness and concerns, but there remains a glaring gap in cyber coverage. The Aviation industry is a late adopter of cyber insurance, only one-quarter of our Aviation and Aerospace respondents have cyber insurance (26%) – see Figure 4. Overconfidence in existing cybersecurity can be a major impediment to the airlines' ability to recognize that cyber insurance can serve as a backstop to a robust cybersecurity strategy and ongoing risk management.

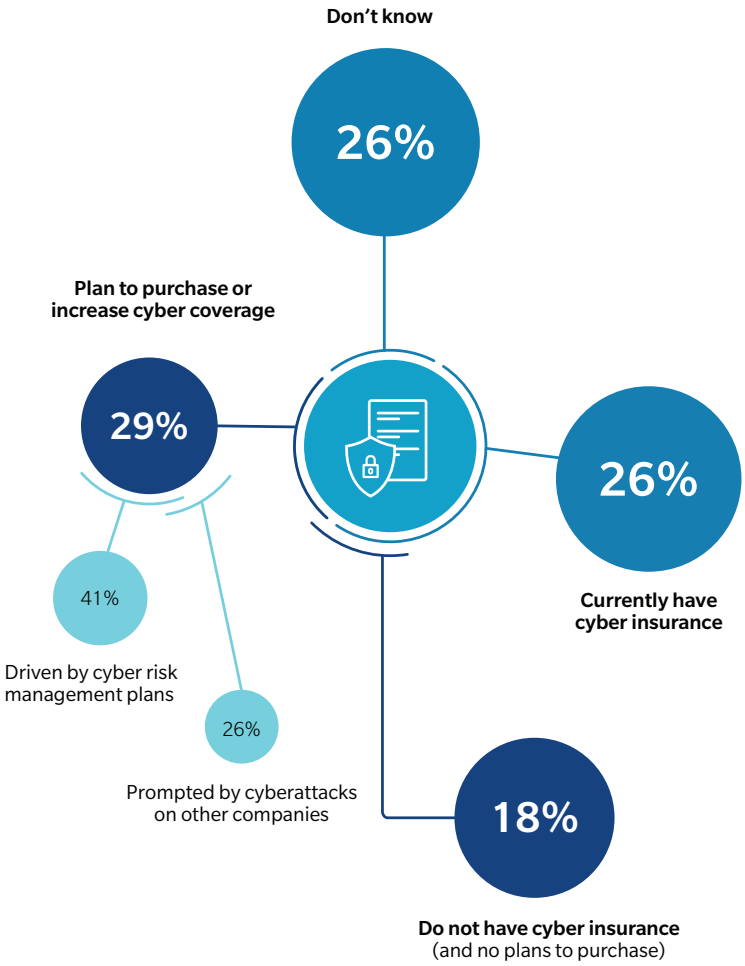
## Cyber Insurance as a Solution

Cyber insurance has become an integral part of a risk transfer strategy in any organization. In the event of a breach the potential causes of loss from a single cyber event can be insurable. Coverages available are:

- Loss of income and increased costs of working resulting from network interruption caused by security failure, system failure, or operational error, including failure of your third party outsourced partners.
- Costs of recovering, reconstructing, re-loading or replacing digital assets which have been impaired due to a security failure, system failure, or operational error, including failure of your third party outsourced partners.
- Payment card (PCI) data security standards fines and assessments.
- Payment of cyber extortion losses and expenses.
- Associated crisis response costs, including IT forensic costs, legal expenses, customer call center costs, notification expenses, identity theft remediation services, and public relations costs.
- Liability to third parties, defense costs and regulatory fines, in respect of:
  - A data breach
  - Breach of data protection legislation
  - Breach of confidentiality agreements
  - Network hi-jacking, including virus transmission
  - Content injury in connection with your publishing, broadcasting, and/or advertising activities, including your website content and/or functionality.

FIGURE 4 Status of Cyber Insurance in the Aviation and Aerospace Industry

SOURCE: MARSH MICROSOFT GLOBAL CYBER RISK PERCEPTION SURVEY 2017



Marsh's local and global specialists are available to assist clients with both pre- and post-event concerns, including insurance program management, business continuity planning, property inspections, crisis management, and claims. If you have any questions or require assistance, contact your Marsh client representative or:

NAUREEN RASUL
Cyber Practice Leader, Asia
+852 2301 7206
naureen.z.rasul@marsh.com


PH18-1184