# Association of South Pacific Airlines

8th September 2022

Gallagher

Insurance | Risk Management | Consulting

# Why Airlines are a Target

- Significant PII Data
- Reliance on third party vendors
- Potential for significant interruption to the business
- Use of Legacy systems

# Claims

**BRITISH AIRWAYS**
2018

Supply-chain attack which affected the personal and financial information of more than 420,000 customers – Investigations suggested that **MFA could have prevented this**.

**CATHAY PACIFIC**
2018

Threat actors accessed the airline's Active Directory, system lacked any **password protection** for backup files and the operating system was out of date. 9.4million customer records being compromised. In UK, a 500,000 GBP fine was issued by the ICO, and in Canada the airline was forced to pay C$1,550,000 in settlement funds.

**PEGASUS**
2020

The airline experienced a **data compromise** of 5.6TB of data including employee information, flight charts and navigation materials, due to the **misconfiguration of security settings** in their Amazon Web Services storage 'bucket'

**easyJet**
2020

EasyJet was the victim of a cyber-attack in which hackers obtained the credit-card information of 2,208 customers. The carrier did not notify passengers of the attack until 4 months after the incident. As a result they are now facing a **class-action suit** from 10,000 passengers, seeking around **£18 billion** in damages.

**Akasa Air**
2022

A breach occurred which resulted in the basic personal information of customers being accessed by unknown third parties.

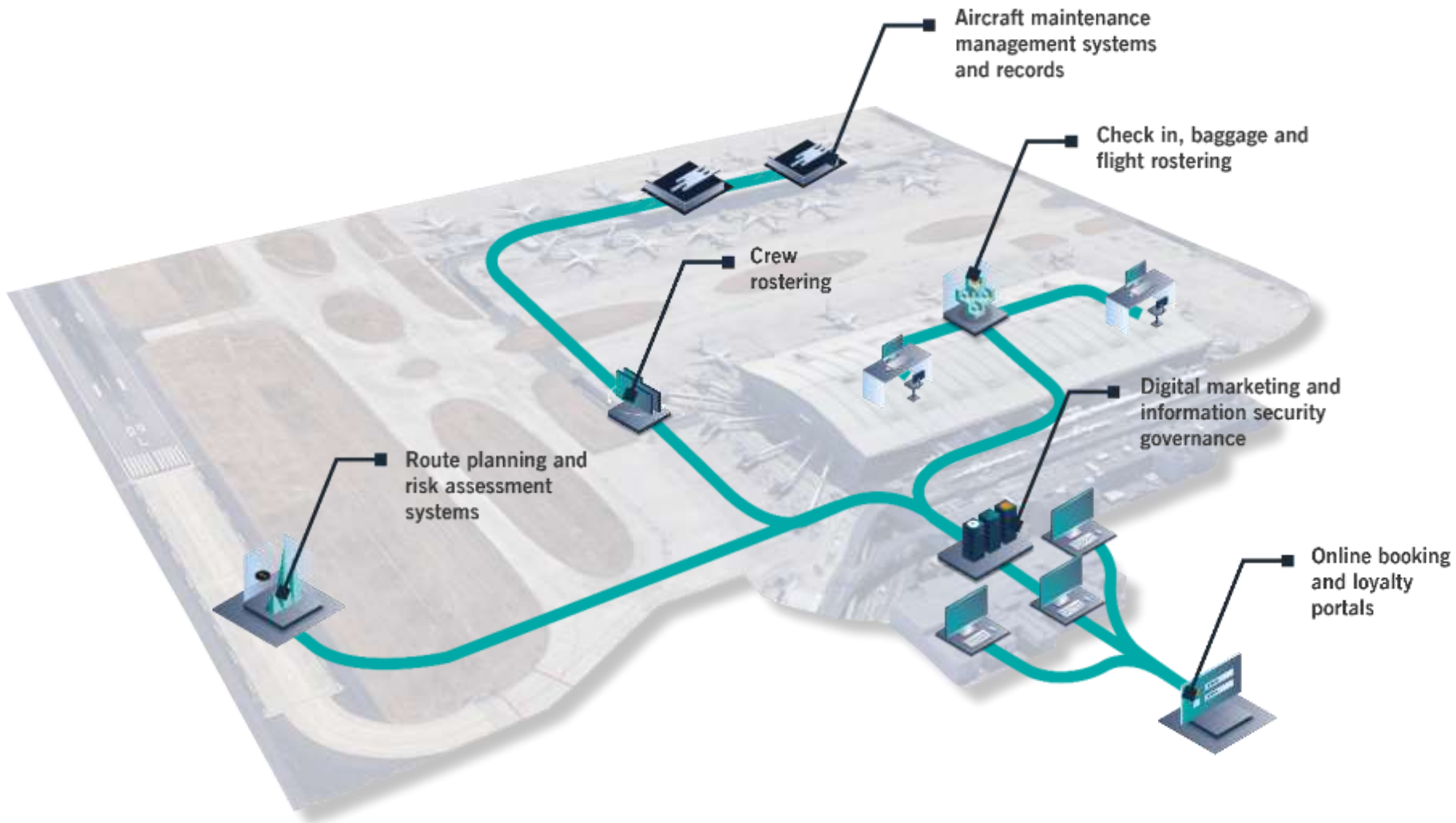
**spiceJet**
2022

Following a massive **ransomware attack**, hundreds of passengers were stranded at airports across India. The systems targeted were not revealed.

**sunwing**
2022

Canadian airline faced four days of extensive flight delays after the **third party software system** it used for check-in and boarding was breached by hackers.

# THE CYBER LANDSCAPE FOR AVIATION



# Recap of 2021

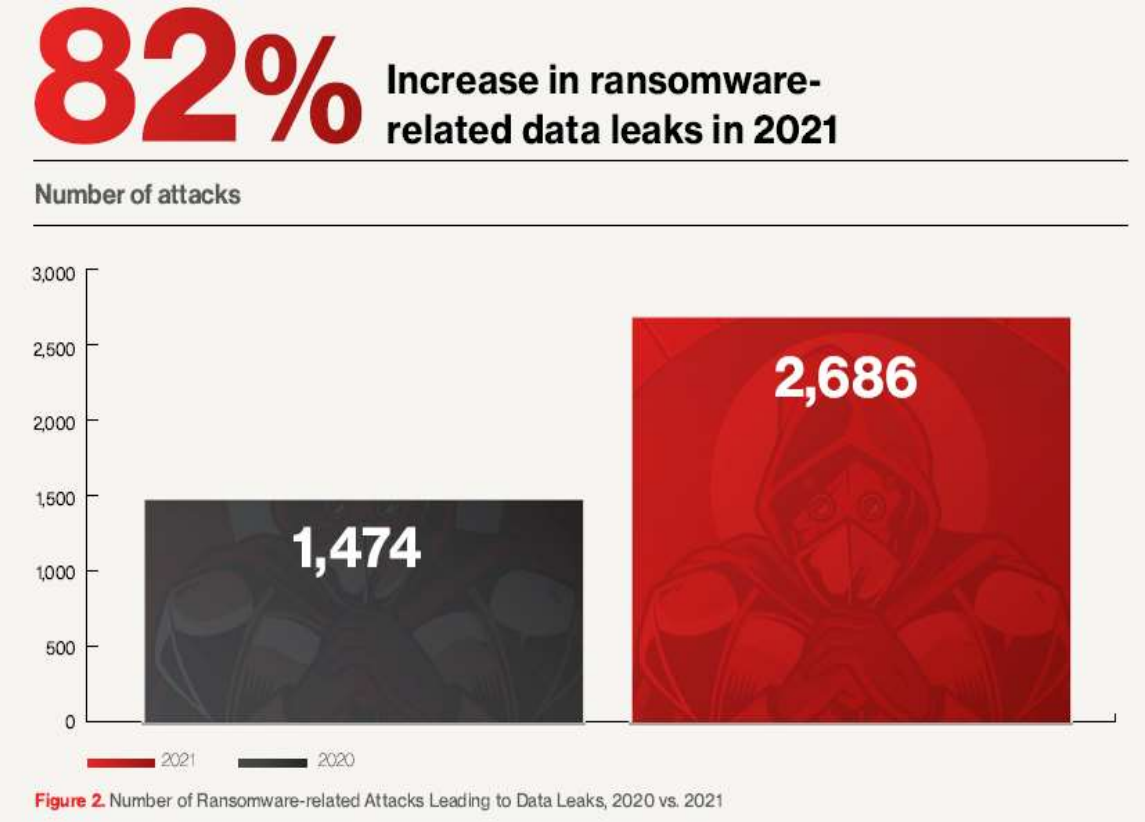


Figure 2. Number of Ransomware-related Attacks Leading to Data Leaks, 2020 vs. 2021

Source: https://www.crowdstrike.com/resources/reports/

- Privileged escalation and move laterally through the network
- Encrypt or Delete Data
- Triple Extortion to:

  A. Publicly release stolen sensitive information
  B. Disrupt the organisations access to their servers and the internet
  C. Inform the victim's partners, shareholders or suppliers about the incident

# Supply Chain Attacks - 2022

I. Nation state APT-Advanced Persistent Threat preferred method cyber espionage campaigns.

II. Kaseya VSA and Log4j events are a sign that supply chain Single Point of Failure attacks will become more frequent and also more severe.

III. “Potential for a single cyber attack to cause widespread and catastrophic damage is now undeniable”

IV. The most high-profile attack in recent times was on the Colonial Pipeline, which supplies 45% of the oil used by the U.S. East Coast. Hackers managed to shut the company down for five days in May and accrued a $4.4 million ransom demand,


Frontier software

JBS FOODS


Accellion

kiteworks

Colonial Pipeline Company

Source: https://insights.cybcube.com/global-threat-briefing-h1-2022

# TOP 10 CYBER ATTACKS

## 1 Social Engineering

Any network is hackable if an employee can be duped into sharing access.

## 2 Third-Party Exposure

Vendors, clients, and app integrations with poor security can provide access to an otherwise well-protected network.

## 3 Configuration Mistakes

Even the most cutting-edge security software only works if it's installed correctly.

## 4 Poor Cyber Hygiene

Employee training is essential to ensure those with network access maintain safe cyber practices.


## 5 Cloud Vulnerabilities

Online data storage and transfer provides increased opportunities for a potential hack.

## 6 Ransomware

Hackers can capture sensitive data or take down networks and demand payment for restored access.

## 7 Mobile Device Vulnerabilities

Devices that connect to multiple networks are exposed to more potential security threats.

## 8 Internet of Things

Smart technology users may not realize that any IoT device can be hacked to obtain network access.

## 9 Poor Data Management

When massive amounts of unnecessary data are kept, it's easier to lose and expose essential information.

## 10 Inadequate Post-Attack Procedures

Security patches must be as strong as the rest of your cybersecurity protections.

https://www.embroker.com/blog/top-10-cybersecurity-threats-2022/

# Legislation Changes

**SOCI (Security Critical Infrastructure & Amendment Nov 2020) Act 2018**

- Mandatory Reporting Obligations
- Register of Assets
- Positive obligations – Risk Management Framework – E8 Maturity Level 3

**(OAIC) Mandatory Notifiable Breach Reporting (2018)**

- Privacy Act 1988 currently under review
- Statutory tort may be introduced
- Expand the power of the regulator – penalties flagged to increase
- Redefine personal information

**Ransomware Action Plan**

**Corporations Act 2001**

- Litigation against Directors for failure to properly consider cyber risk
- Directors Duties
- Cyber Security Class Actions

# Global Privacy Laws

Gallagher
Insurance | Risk Management | Consulting

- When an organisation suffers a data breach, it may be obligated to notify regulators, affected individuals, or other stakeholders of the incident;

- An airline may fall within the scope of a data breach notification regime where it has offices, employees, contractors, or any other links to a jurisdiction.

- Airlines need to be aware of their international exposure to data protection regimes to ensure timely adherence to local laws in the event of an incident.

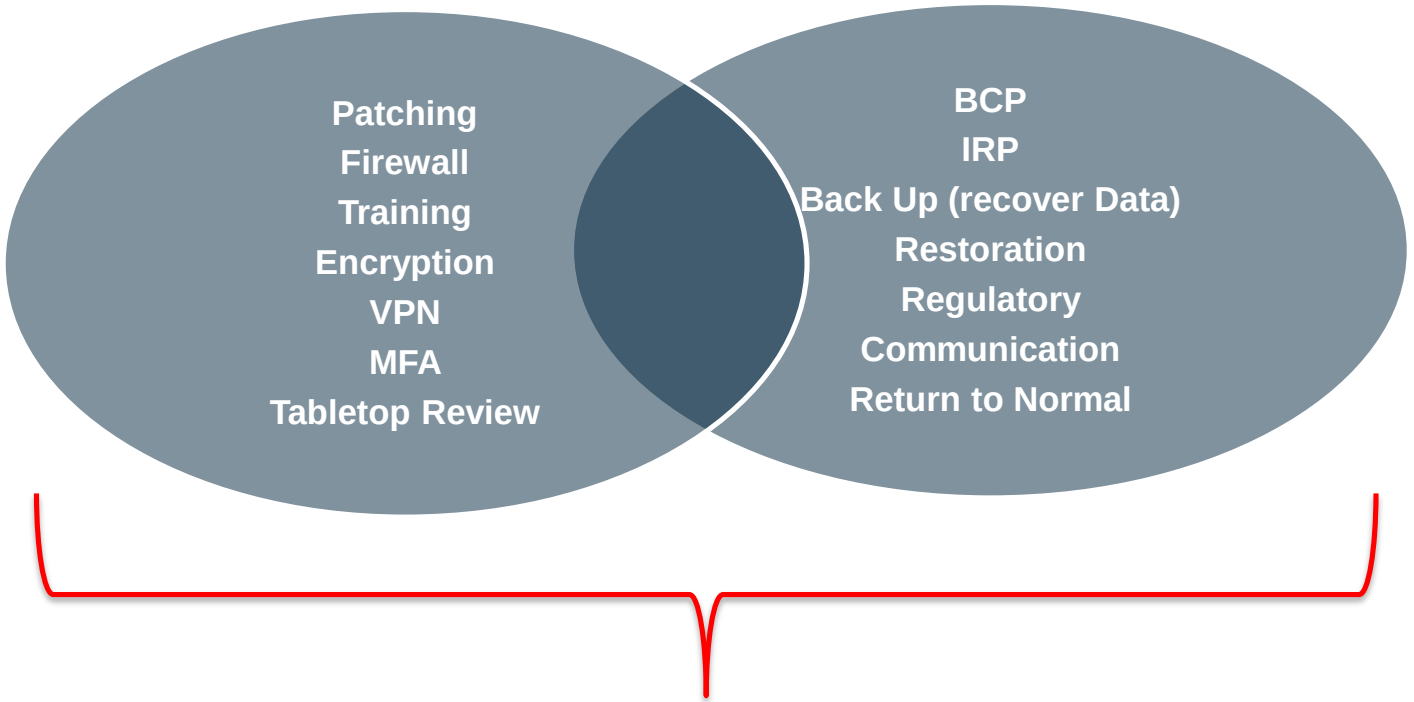
Australian Government
Office of the Australian Information Commissioner
Protecting information rights – advancing information policy

# Insurers respond to claims data

- ✓ The increase in claims is outpacing that of premiums earned
- ✓ There is a demand and supply imbalance
- ✓ Insurance is to provide for unforeseen events
- ✓ Cyber claims are often for vulnerabilities that should have been addressed with better controls

# Understanding Cyber Risk

## Cyber Security vs Cyber Resilience



# Insurers Will Require

- ✓ An organisational cyber risk culture from the board down
- ✓ A Board understanding of their knowledge of their critical assets
- ✓ A commitment to invest in best practice security controls
- ✓ An embedded culture of continuous improvement processes of employee awareness and training
- ✓ Best practice security controls being measured against known risk management frameworks – Essential 8, ISO 27001, NIST

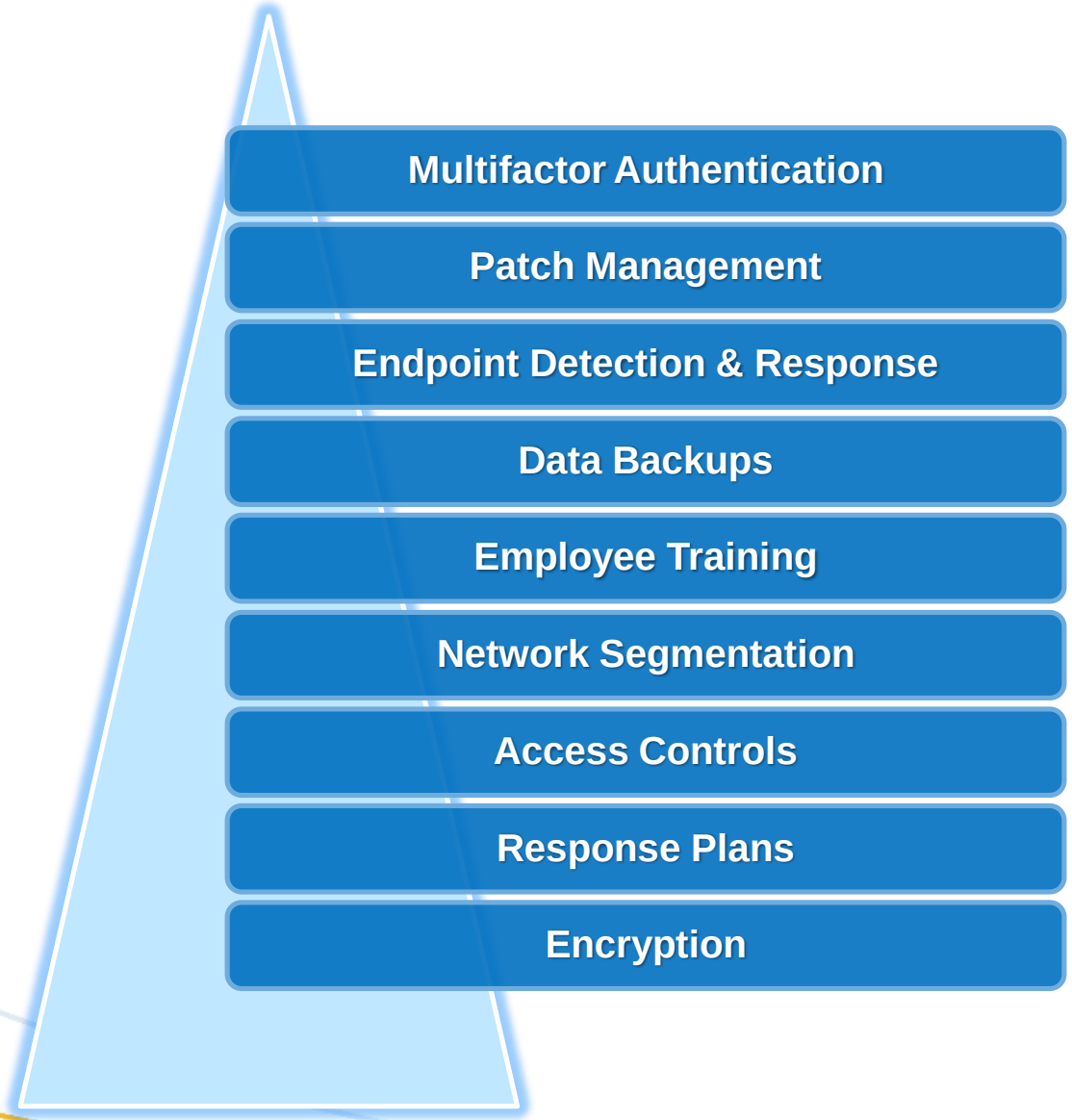
# Insurers Will Require

- ✓ Governance – Business Continuity, Incident Response, Disaster Recovery, RW plan – are all these plans in place and tested.
- ✓ Who is hosting your data?  Do you have a vendor audit process in place so you can measure the security controls of the vendors?
- ✓ Where is your back up hosted – is it off site and tested?
- ✓ Privacy policies and data destruction
- ✓ Do you understand the potential impact of a Cyber event.
- ✓ Technical Security Controls – constantly changing focus based on global claims experience
- ✓ Internal and external audits – international standards
- ✓ Vendor audits

# Insurers Will Require

- ✓ Decommissioning of Legacy infrastructure
- ✓ Known vulnerabilities have been addressed with patching protocols
- ✓ Planned and tested responses in the event of a breach – Incident Response and Business Continuity plans
- ✓ A tested Ransomware Plan

# Baseline Controls



| | |
|---|---|
| Multifactor Authentication | For all remote access, privileged access and email inbox access |
| Patch Management | Written process to monitor all vulnerabilities and updates |
| Endpoint Detection & Response | Monitor all end-points |
| Data Backups | Encrypted, tested annually and offline |
| Employee Training | Phishing, email security and awareness staff training |
| Network Segmentation | Risk-based segmentation to prevent lateral access |
| Access Controls | Role-based access control and principle of administrative privilege |
| Response Plans | Incident Response Plan, Business Continuity Plan and Disaster Recovery Plan – Annually Tested |
| Encryption | Encrypting data at rest |

# Cyber Risk Transfer – Cyber Insurance

| | |
|---|---|
| **Crisis Management Costs** | Lawyers, IT Forensics Investigators, credit monitoring firms, mailing and call centers, public relations experts. |
| **Ransom & Lost Funds** | Immediate access to Bitcoin and trained negotiators. Some, *not all*, policies reimburse lost funds due to social engineering. |
| **Business Interruption** | Lost income due to downtime. Can also cover contingent BI. |
| **Data Asset Restoration** | Restoring data that is damaged or destroyed.<br>Can include “bricking” coverage for damage to physical devices. |
| **3rd Party Liability** | Coverage for lawsuits from regulators, business partners and affected individuals. |

# Next Steps

**Step 1**

- Do you understand your risk? Have you carried out an audit and gap analysis? Is IT Security on your board agenda? Do your training and controls filter throughout your entire business?

**Step 2**

- If you have an MSP do they understand their role as your advisor – are they advising you on your cyber security- what is their scope of services?  Are you implementing their advice?

**Step 3**

- Have you met your incident response coach and are they built into your business continuity plan?

**Step 4**

- It is important to work with your broker to design a bespoke risk transfer solution tailored to your specific exposures

# What Questions Do You Have?

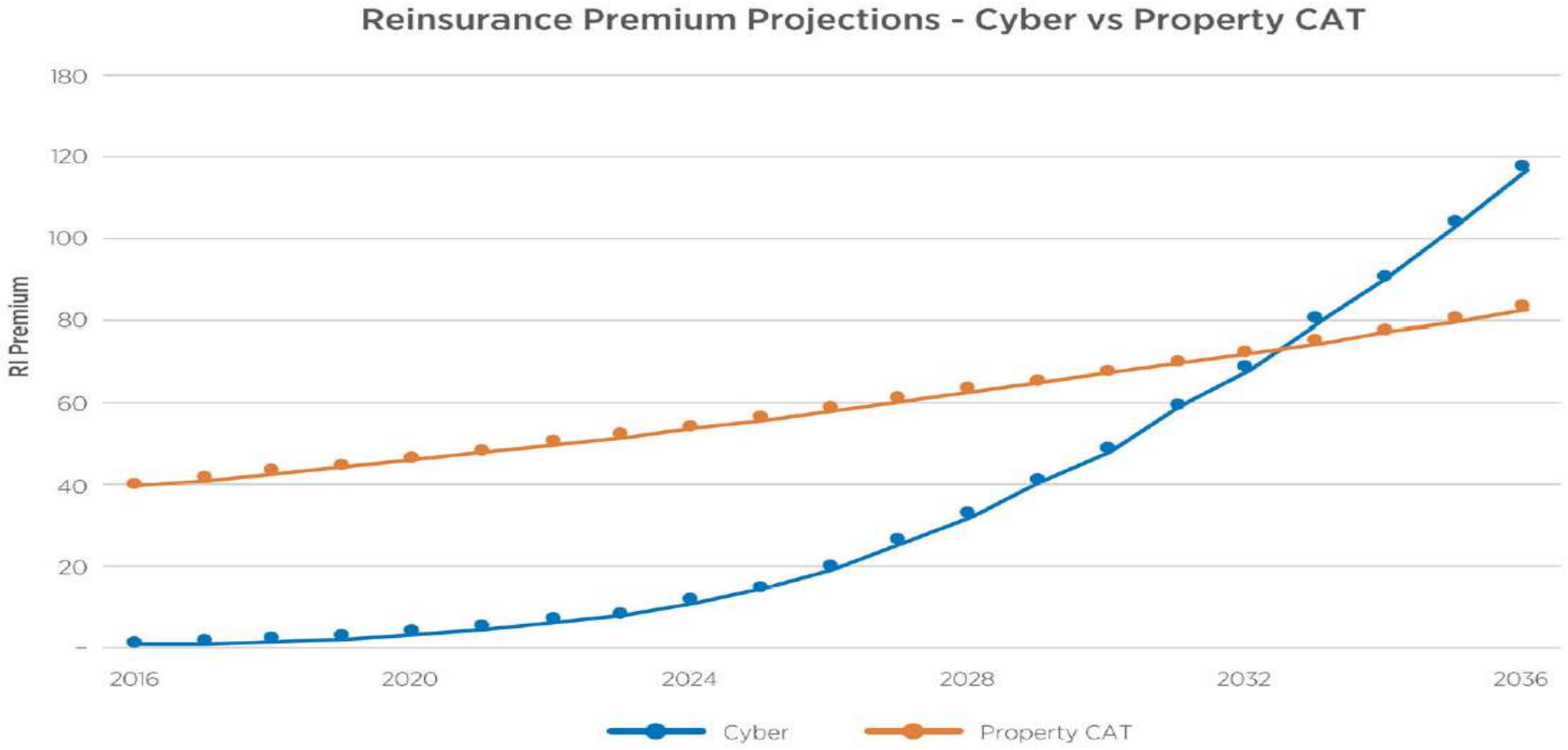
# Think about your supply chain

| Huntsman's 10 Questions | |
|---|---|
| 1 | Do you have an inventory of suppliers, subcontractors or even customers that includes those:<br>• who share data, or you allow to access your data; and/or<br>• whose contribution of goods and services is critical to your ongoing operation? |
| 2 | How reliant are you on your external providers for the security of your data? |
| 3 | Do you have digital or physical suppliers whose services to you could be disrupted by a ransomware attack affecting their systems? |
| 4 | Do you have alternate suppliers/contingency arrangements, if a cyber-attack caused a prolonged outage at a key/critical supplier or customer? |
| 5 | How do you validate a supplier's level of cyber resilience – do you have an agreed and effective mechanism to reliably assess the security of key/critical suppliers? |

# Think about your supply chain (cont.)

| Huntsman's 10 Questions | |
|---|---|
| 6 | How transparent is your IT assurance process and how reliant is it on information provided by suppliers themselves? |
| 7 | With the known limitations of a number of well-known risk assessment methodologies, how do you assess and report the level of internal security, cyber hygiene and ransomware readiness of your suppliers relative to the services/products they provide to you? |
| 8 | Do you have a tested incident management plan, points of contact and experts available to assist in the event of a key supplier's security incident? |
| 9 | Is the security posture of your suppliers part of your continuous improvement and cyber risk management process? |
| 10 | How do you prioritise the level of risk of your suppliers – in terms of data involved, criticality of services, size, complexity – and what impact does this have on how you obtain assurance on cyber security safeguards? |

# Insurance Availability




Assuming average growth of 50% growth in Cyber premium in 2021 and an average of 25% for all subsequent years.

Assuming 46% premium being ceded to cyber reinsurance market in 2021, depreciating to 25% by 2040.

Assumed a growth rate of 3.9% for property for 2016-2028, reducing it to 3.5% for 2029-40 (ignoring cycles for simplicity).

# How does a Cyber Incident occur (continued)

## Why, When and How…

Aviation like all business are vulnerable to the same cyber threats  including ransomware, Business Email Compromise (“BEC”) and Supply Chain (with our without Denial of services (“DDoS”), data exfiltration, etc).

Some aviation areas of concern include:

- ***Regulations and standards*** for developing an aviation cyber resilience culture across the entire industry
- Cyber resilience for ***business continuity*** in the new normal
- Technological innovation: updating existing and implementing new software
- Reputational Damage
- Customer data can be compromised (e.g. Privacy Breach)
- Business Email Compromise (“BEC”) / Phishing
- Human Error
- Litigation (e.g. class actions) about all of the above

Regional airlines can be more vulnerable to cyber events as they do not have the same financial infrastructure and capabilities the major carriers have … they are an easier target!

# Global Aerospace Industry

## Technology - Cyber Security, key cause of loss

Facts and figures:

530% year on year rise in reported aviation cyber incidents

Airlines are most in the line of fire, targeted by **61%** of all 2020 aviation cyber attacks in 2020 – almost twice as much as the two next largest market segments combined

Aviation faces a ransomware attack every week – the price of ransomware mitigation measures alone is expected to cost global companies **US$20billion a year**

Airlines continue to be targeted with an estimated US$1 billion a year lost from fraudulent websites alone. This is before the cost of data theft; card fraud; air miles fraud; phishing; fake invoices and more.

Ransomware to global businesses tripled between 2017 – 2020 and is set to have quadrupled by the end of 2021 to US$20billion from US$5billion in 2017

51% of IT managers across all industries revealed in a survey that their businesses had been hit at least once in 2020 by ransomware. Majority being server based and highly disruptive

Average ransom demands:
Q4 2019: US$12.8million
Q4 2020: US$42.0million
H1 2021: US$65+ million

Downtime costs are 5-10 times the ransomware payment, with average number of days an incident lasts: 21 days

Source: 01EuroControl_Aviation Think Paper July 2021
Gallagher Cyber Risk Consulting

# Looking Ahead

## Future Trending

### Complex renewal negotiations

- Renewal negotiations are likely to remain complex and will continue to take longer.
- Early engagement is essential.
- Macro themes may be of concern in the longer term (beyond 2022)

### Varied capacity levels

- Varied capacity from risk to risk
- Varied from sector to sector
- In aviation overall increased appetite / competition amongst insurers for the ‘right’ risk.
- Cyber continues to be of concern

### Focus on underwriting data

- Scrutiny of return to operation plans and safety procedures
- The supply of accurate information is critical.
- Potential increase in more technical information being required based upon macro themes

### Varied underwriter responses

- Insurer responses will remain varied by each individual risk
- Insurers will seek justification to support client requests and pricing.
- ‘Green’ thinking may influence underwriter responses in the long term

### Further moderation of technical rates

- Further moderation of technical aviation rates
- Exposures and other variables will remain a key feature in renewal negotiations and overall results.
- Continued focus on sustainability of Aviation in cyber market

**Absent no major losses/market event initial signs suggest a more positive outlook for airline insurance buyers in Aviation and a critical outlook from a Cyber perspective.**

# Looking Ahead

## Future Considerations for Insurance Buyers

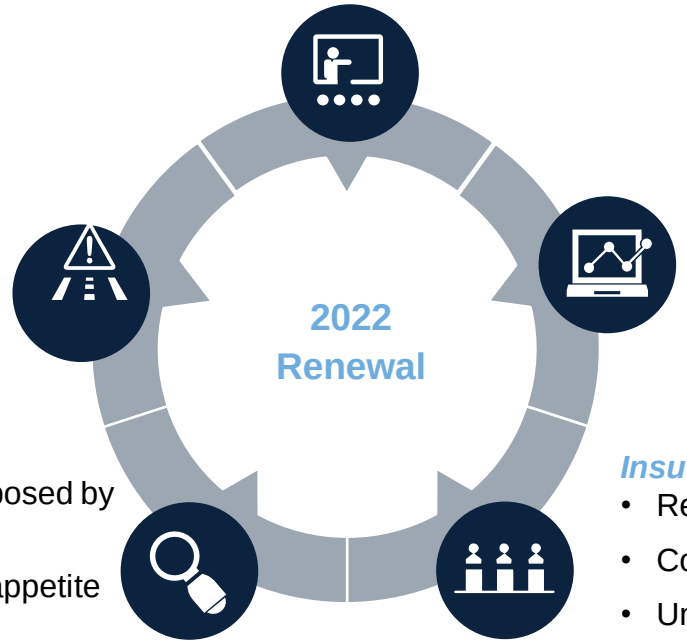
**It remains essential that clients ensure they are partnered with the right insurance broker which has the resource, bandwidth and experience to navigate the challenges posed by the current markets that the aviation industry faces and deliver results in all classes.**

***Start your renewal process earlier.***

Early preparation with your broker and early market engagement will be hugely beneficial to achieving results.

***Focus on loss control measures and safety management.***

- In the post COVID-19 environment, underwriters are looking closely at clients latest operational safety and loss control measures
- Consider new risk management initiatives to mitigate where possible




***Present the right information.***

- In the post COVID-19 environment it is critical to supply accurate information as soon as it is available and quantified
- Good information will help differentiate you from your peers
- Underwriters need justification to support pricing levels

***Explore all options.***

- Consider all strategies and options proposed by your broker.
- Review your buying requirements and appetite for risk
- Consider additional protection i.e. non-damage business interruption / pandemic risk cover.
- Consider external factors such as ESG – “green credentials” to influence Insurer views.

***Insurance carrier relationships.***

- Retain partners that have performed well
- Continuity can assist greatly in negotiations
- Underwriters will look to take advantage of any change or perceived instability

# What Insurers need to see…

Network Architecture and Critical Applications – linking to BI

- What is your Organisational Culture – does everyone understand their role in protecting your organisation
- Training, Education and Awareness
- Do you understand your critical systems, data and operations and are they mapped against key cyber security risks
- Do you have a Cyber roadmap linked to your risk register? Do you understand your overall risk, resilience and control measures.
- Governance – Business Continuity, Incident Response, Disaster Recovery, RW plan – are all these plans in place and tested.
- Who is hosting your data? Do you have a vendor audit process in place so you can measure the security controls of the vendors?
- Where is your back up hosted – is it off site and tested?
- Privacy policies and data destruction
- Do you understand the potential impact of a Cyber event.
- Technical Security Controls – constantly changing focus based on global claims experience
- Internal and external audits – international standards
- Vendor audits

# What Insurers need to see…

- Risks
- Storage of PI Data
- Malicious Insiders
- Business Interruption
- Reporting to Global Privacy Commissioners
- Restoration of the Data
- Ransomware – it can be illegal to pay a criminal in a sanctioned country, should you pay to restore data and stop the publishing of the data?
- Interconnectivity – Vendors providing services throughout a supply chain – who are they, what are your contractual relationship with them in the event they have a data breach which impacts your business or your data? Are they air gapped from your network?
- Dependent on these platforms to function well
- Cannot contract out of responsibility for your data

# What Insurers need to see…

- If this does happen you will need access to 24/7 assistance to help you through the maze that is a data breach.
- The Insurance Policy
- Can protect against reputational risk
- Threat Actors

# RISK TREATMENT PLAN

**It includes the measures we recommend, grouped into programmes, to reduce the risks identified and support frontline information security teams.**

### INFORMATION SHARING

Privileged and structured sharing of information and intelligence with industry groups, law enforcement agencies, technology user communities and staff.

### SECURITY AWARENESS

Training and awareness programmes to increase the ability for staff to recognise a threat, react appropriately, and report it promptly to the appropriate point of contact.

### RISK REPORTING

Integrating cybersecurity into the organisation's enterprise risk management process to better prioritise risk across multiple disciplines.

### SOCIAL MEDIA + COMMS

Building capacity among digital, social and communications teams to identify potential threats, and to prepare for sincere, thought-out responses in the event of a possible breach.

### CRISIS MANAGEMENT

Preparing the crisis management team to respond to a cyber emergency through training and information sharing.

### HONEYPOT DEVICES

Environments or computers which 'fake' sensitive data or services to lure in an attacker.

### CLOUD SERVICES DEFENCE

Defences configured in the cloud to protect services such as Office365 or Amazon Web Services.

### TRAFFIC SHAPING

Limiting certain types of traffic to a particular volume to thwart common attack methods inside networks.

### 'DEMILITARISED ZONES'

A gated area at the edge of the network which makes it easier to deliver services to customers safely.

### NETWORK MONITORING

Areas in which all activity and traffic is closely monitored, generating an alert for known suspicious activity.

### ANTI-MALWARE

Anti-virus deployment and other methods to prevent, detect and terminate malicious programs.

### VIRTUAL PRIVATE NETWORKS

Secure methods of connecting to the network for staff who are offsite or in other offices.

### INTRUDER DETECTION AND FIREWALL

Ways of denying connections to the boundary of the network, or detecting attempts to infiltrate.

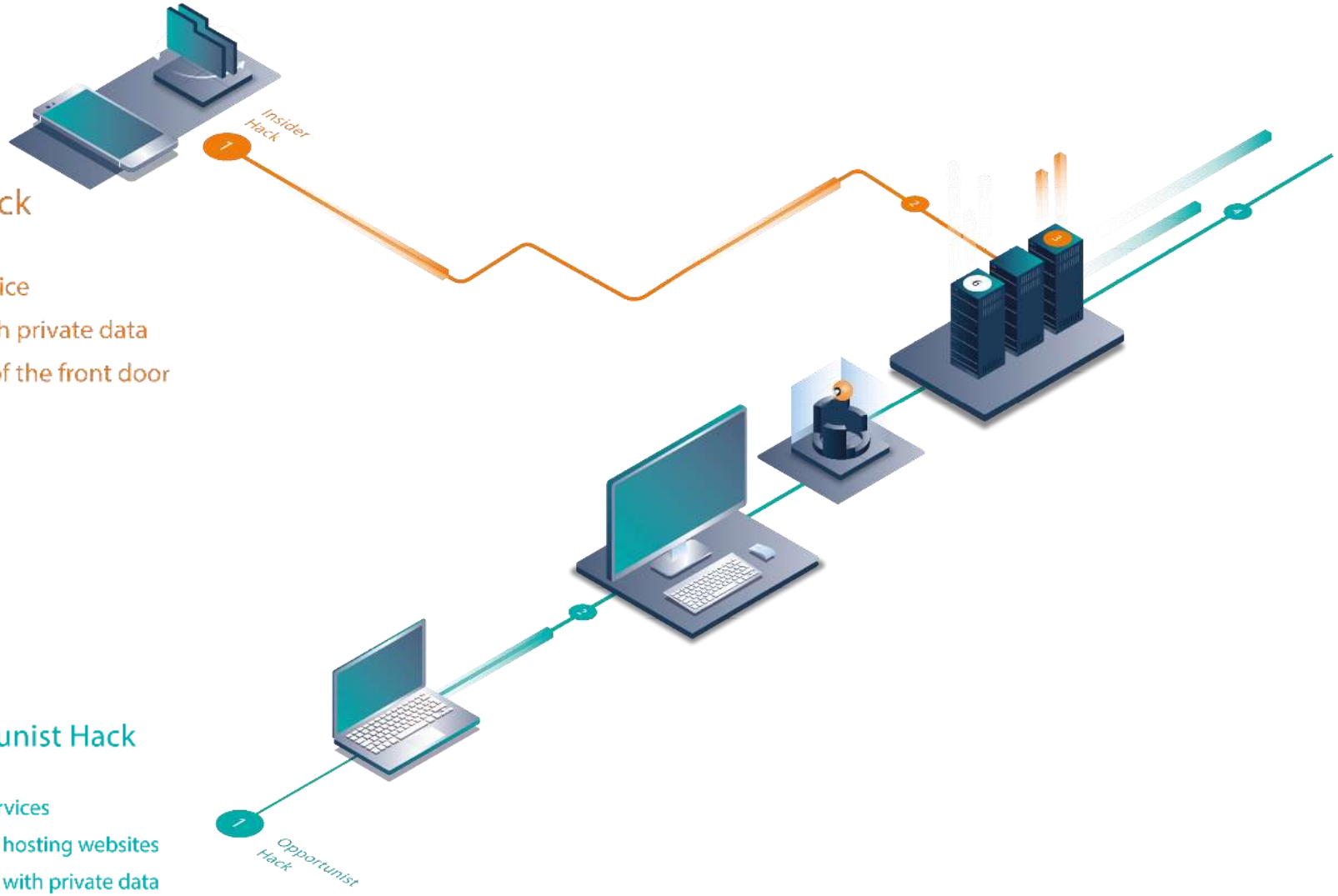
# High-level Risks Exposures for Airlines

**The processing of high volumes of third party information in combination with the ever growing dependency on technology puts Airlines and aviation providers at a significant risk of a cyber incident, for example**

- Business Interruption exposure
- Privacy Liability & Regulatory action exposure
- Crisis Management

# THREAT ATTACK

To thwart an attack, start with the attacker.




## Insider Hack

1. Mobile device
2. Servers with private data
3. Walks out of the front door

## Opportunist Hack

1. Web services
2. Servers hosting websites
3. Servers with private data
4. Data exfiltration out of the network

# Cyber Awareness

- ✓ Risks
- ✓ Storage of PI Data
- ✓ Malicious Insiders
- ✓ Business Interruption
- ✓ Reporting to Global Privacy Commissioners
- ✓ Restoration of the Data
- ✓ Ransomware – do you pay or not pay?
- ✓ Interconnectivity with vendors
- ✓ Dependency on platform functionality
- ✓ Contractual Responsibility

# Global Privacy Laws

- When an organisation suffers a data breach, it may be obligated to notify regulators, affected individuals, or other stakeholders of the incident;
- Notification obligations in numerous international jurisdictions may be triggered following a cyber incident;
- An airline may fall within the scope of a data breach notification regime where it has offices, employees, contractors, or any other links to a jurisdiction;
- as data protection remains a relatively new area of law, internationally, data breach notification regimes are at varying stages of maturity in respect of comprehensiveness and enforcement;
- there is also considerable diversity in the extraterritorial reach of laws and thresholds for notification across jurisdictions;
- the deadlines for notification across jurisdictions may also vary significantly, from “as soon as practicable” following awareness of a cyber incident, to after a 30 day period of investigation; and
- it is essential for airlines to be aware of their international exposure to data protection regimes to ensure timely adherence to local laws in the event of an incident.
- Promotes and protects the privacy of individuals and regulates how Australian Government agencies and organisations with an annual turnover of more than $3 million, and some other organisations, handle personal information
- General Data Protection Regulation 2018 – GDPR
- Purpose is to update digital security for the citizens of the EU by giving them a higher level of control on the personal information they share online
- Applies to businesses all over the world