# Risk and Strategy in Flight

Marsh Aviation Summit 2026

Cyber resilience in aviation: A real-time simulation and preparedness workshop

# Cyber risk and the aviation industry

## 2025 saw significant cyber attacks against major aviation companies

- Social engineering attacks on airlines by Scattered Spider and affiliates resulting in data breaches and airline disruption.
- Ransomware attacks on airports forcing pivots to manual operations, causing delays and disruption.
- DDOS attacks on airports and aviation infrastructure causing operational disruption.

## Threat landscape for 2026

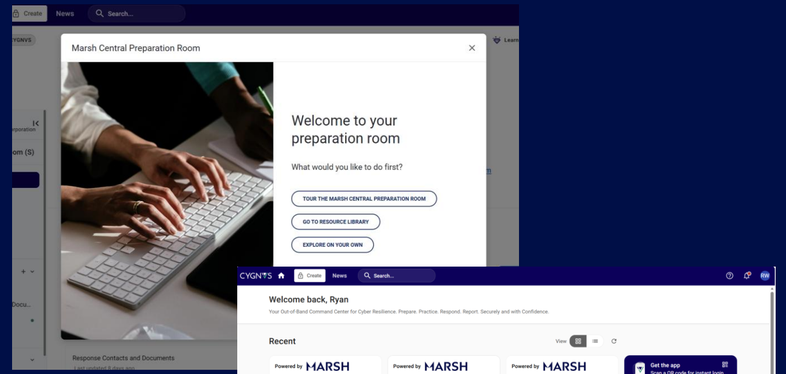
- Geopolitical unrest likely to result in more ideological hacktivist-driven attacks, including ransomware and DDOS.
- Advancements in AI will supercharge phishing and social engineering tactics, with deepfakes on the rise.
- Ever expanding supply chains expand attack surface and likelihood of downstream impact.

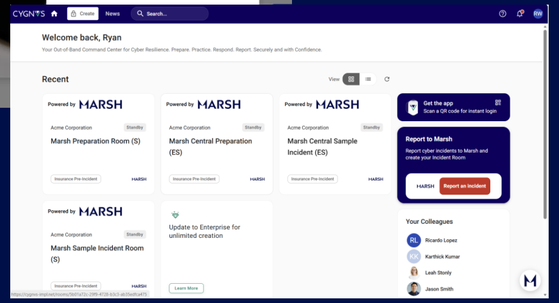
## What can you do to prepare?

- Prepare for the worst-case scenario – robust IR and business continuity plans and well-rehearsed manual processes to keep passengers moving during a crisis.

# Marsh Central: Education, preparation, and incident management platform, powered by CYGNVS

Essential resources, securely in one place, when you need them most




## Communicate and collaborate with key stakeholders

Cyber incidents occur when you least expect. How are you communicating with key stakeholders to respond?

Marsh Central provides a secure off-band communication tool available globally, through a mobile app.

## Access your incident response plan at your fingertips

Where do you store your most up to date incident response plan and is it available securely off-network?

Marsh Central allows you to store critical documents off-network, so you have access when you need it most. It's a plan in your pocket.

## Effortlessly manage and document incident and claims activity

Are you able to easily and accurately collate incident information?

Marsh Central provides a full incident audit trail, allowing everyone to understand the facts, respond quickly, and provide reports to regulators and customers.

## Review best practices on claims and incident response

Are you aware of the latest best practices and incident trends?

Marsh assists with thousands of incidents, including some of the largest global events. Access our tip sheets, videos and articles to learn best practices on cyber incident management.

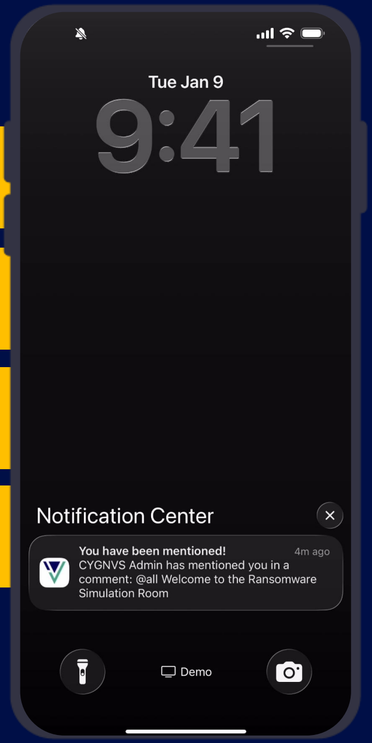
# Follow Along in the CYGNVS Mobile App

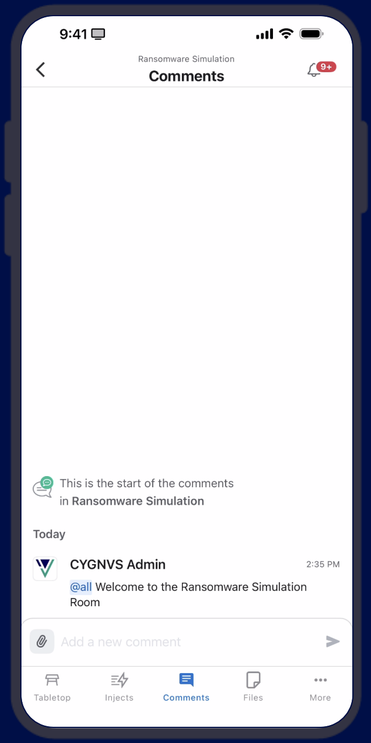
Click on the notification when the exercise starts to follow along and to participate in the discussion.

1

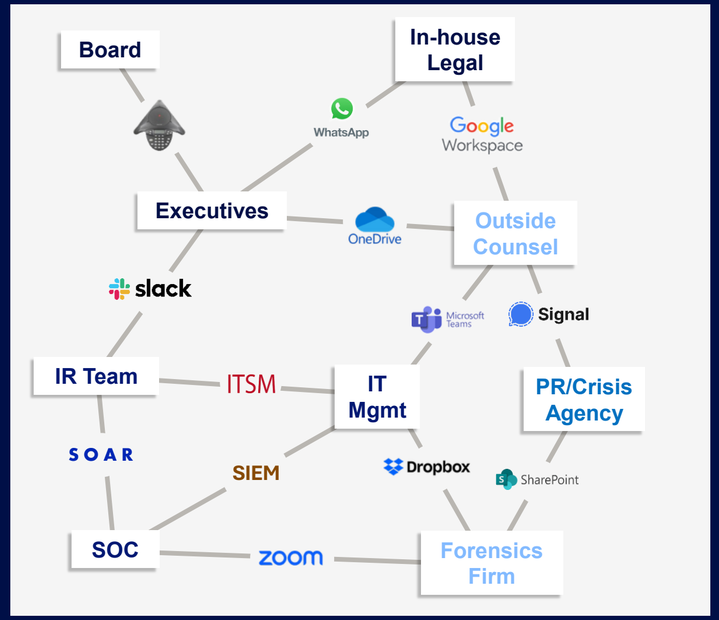
- Make a point
- Share your experience
- Ask a question
- Engage with each other and the panel

Takeaways will be in the mobile app



# CYGNVS: Cyber Resilience Command Center Trusted by 3,000 Customer Organizations




Which systems are down or *compromised*?

Mobilising the extended team rapidly?

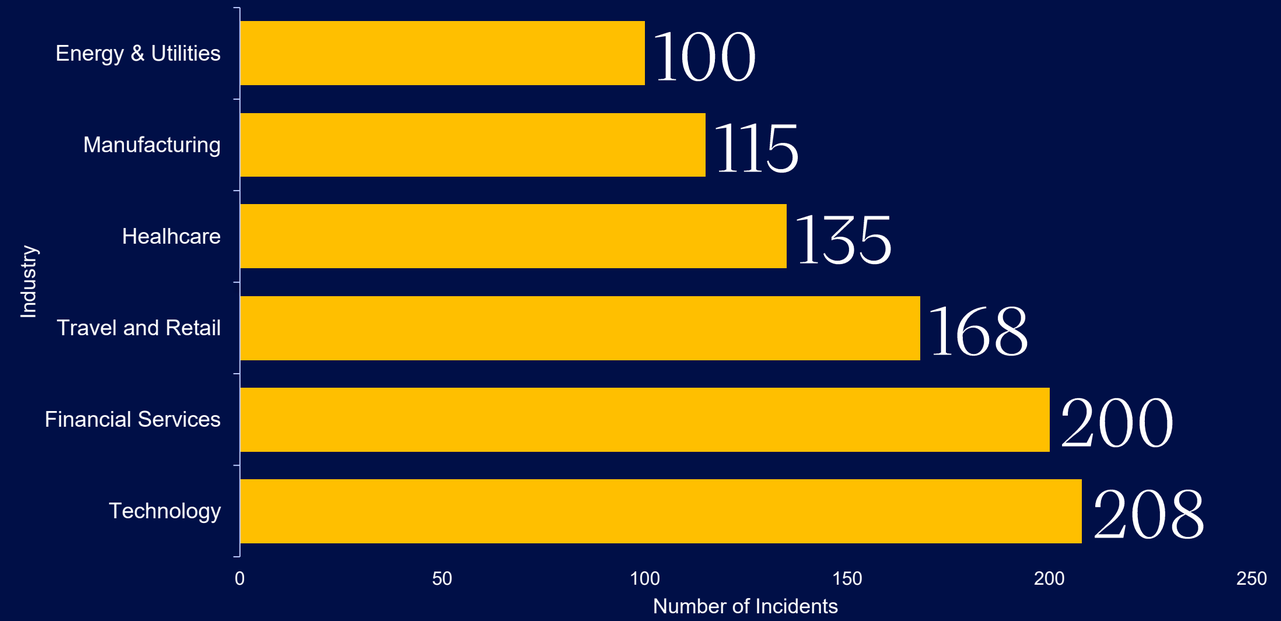
Coordinating execution and real-time visibility?

Controlling access and protect legal privilege?

Chain of custody for evidence gathering and compliance reporting?


- 66% Users from the business
- 2600 major incidents/year
- 71 countries
- 6 granted patents

# Cyber incidents are becoming commonplace... are you ready?




Source: Gartner

> We are at a point in time where nobody is being faulted for having a cyber attack, however many are being faulted for how they respond to it.
>
> -Paul Fertado, Vice President & Research Analyst

Gartner®

# Introducing our Panel

## Vikas Patel

ACME Chief Information Security Officer (CISO)

## Helen Nuttall

ACME General Counsel

# Let’s Get Started

# Scenario Introduction

## You are

on the Board at Acme plc, a publicly-traded airline with global operations

It's Friday evening at 7pm and you are just wrapping up dinner with your family at your favorite local restaurant...

# Day 1: Ransomware Detected

You get an urgent request from the Company CISO to join a conference call on *FreeConferenceCall.com*

The security team has detected ransomware on hundreds of servers. The team is investigating and attempting to contain the attack.

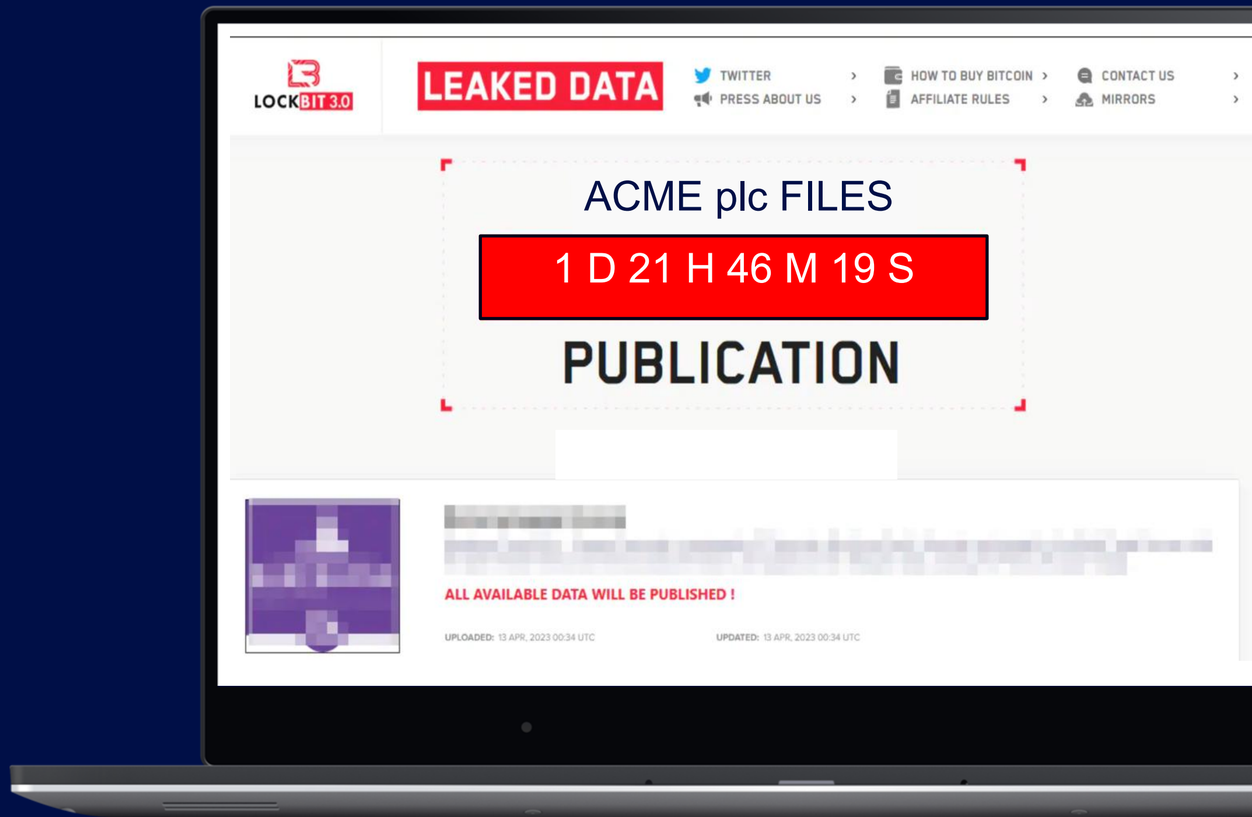
Initial reports indicate that the ransomware is linked to the LockBit ransomware group. Given the risk to the organization, the CISO has called this emergency meeting with the Executive team.

Corporate Email, Zoom, Microsoft Teams, Single-Sign-On and other core systems are either unavailable or compromised. People are starting to communicate on Whatsapp and Signal.

Flight and Airport operations seem to be unaffected.

Day 1: Discussion

# With internal communications down, what are the factors to consider for coordinating response and containment?



# Day 2: Threat Actor Engagement

The CEO receives a message from the threat actor (using an employee email account) demanding a ransom payment of £100 million within 48 hours or they will take down airport operations and publish exfiltrated data.

The CEO is given a link to contact the threat actor to open negotiations.

Initial investigation suggest that exfiltrated data includes customer data, and non-public corporate financial data.

Operations workarounds are in place for flight and airport operations but booking systems have just gone down.

Day 2: Discussion

# What are the factors that you should consider when deciding on whether and when to pay the ransom?

Polling Question

# Will you pay the ransom?

YES

NO

# Day 3: Information Spreading

Your National Cybersecurity Center has contacted the CISO asking what happened since they are seeing signals and Threat Actor chatter on the dark web about a potential breach. They are asking how they can help.

Short positions on the Company stock have increased significantly and a lot of it seems to be traced to hedge funds based in offshore jurisdictions.

The Threat Actor has informed your Aviation Regulator about the incident, and they are asking for a meeting and an explanation.

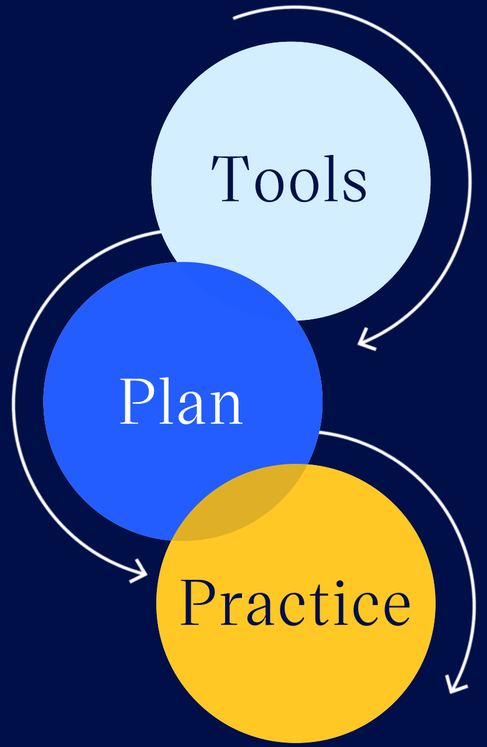
The News Network (TNN) has contacted the Company with a story they plan to run and asked for comment.

Day 3: Discussion

# What are the factors that you should consider when making decisions around notifying regulators, customers, markets and the media?

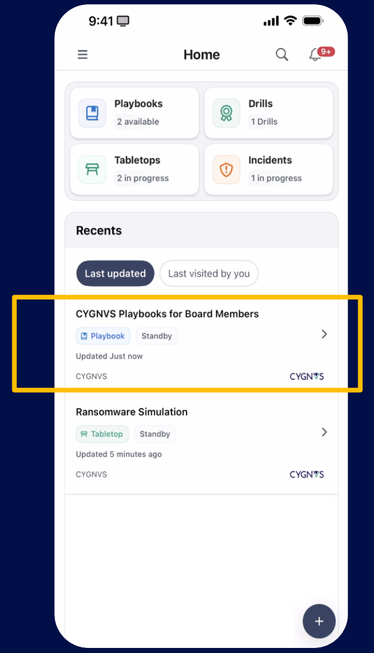
# Learnings: Out-of-Band, Playbooks, Tabletops

1. Out-of-Band platform for Board, Execs, IT/Security, Outside Counsel to collaborate.
2. Playbooks for various scenarios that periodically reviewed and updated.
3. Building muscle memory across stakeholders in realistic “tabletop exercises”.

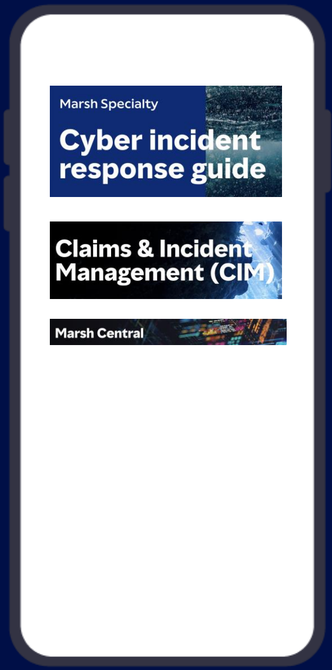


# Take Back Home

## Board Playbook in CYGNVS mobile app




## Marsh Resources inside CYGNVS mobile app




## Want to run a simulation for your organization?

Contact your Marsh broker

# Thank you