WORLDWIDE AIRPORTS LAWYERS ASSOCIATION

XIII Welcome to WALA XIII
Paris, France
June 28-30, 2023

Data Breach and Response in Aviation – Passenger & Critical Data

Stephen Baird & Tatiana Arima Cohen Zaide
SITA

29 June 2023

WALA 2023
Hosted by

GROUPE ADP

Agenda

1. Intro:
    - **About SITA** – Truly Global; Supporting Aviation's IT & Telecommunications
    - **The Context for Aviation**: Privacy, Security, Digitization & Passengers

2. Example of Successful Digital Travel – **"Happy One Pass"**

3. Data Breach Response – A suggested **"Executive Playbook"** for first 48-72 Hours

Questions & Close

WALA 2023
Hosted by

GROUPE ADP

SITA

Part 1:

About SITA -&-
The Digital Context

WALA 2023
Hosted by

GROUPE ADP

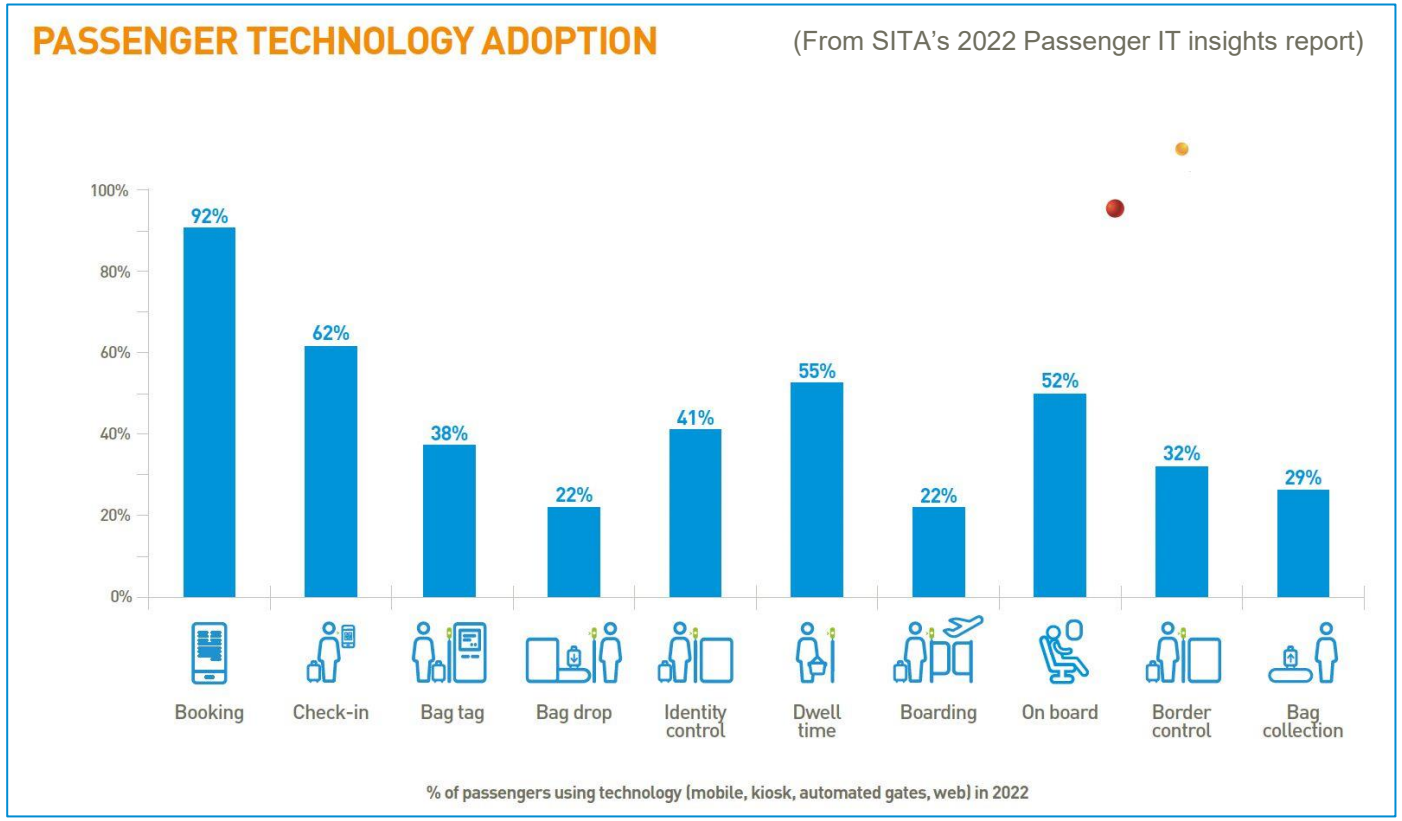
SITA

Intro: About SITA

- A truly global organization
- We represent 134 nationalities & speak 60+ languages
- Five business units:
  - Airports
  - Communications & Data Exchange
  - Borders
  - SITA for Aircraft
  - Champ Cargosystems
- A diverse portfolio covering passenger processing, airport operations, telecommunications, border management services, flight operations & cargo IT

The Context: Privacy, Security, Digitization

- Passengers enjoy using technology for travel and are using it more and more
- 100+ countries have brought in personal data privacy laws
- More countries are imposing mandatory IT security requirements on critical infrastructure operators and cloud IT operators



For airports it is necessary to: (a) enable passenger digitization for enhanced travel experience; and (b) understand the data in your IT ecosystem, and identify and manage risk accordingly

SITA

Part 2:

An example of digital technology in action:

Digital Travel
Happy One Pass

WALA 2023
Hosted by

GROUPE ADP

Welcome To The Future With Digital Travel

SITA

The Future with Digital Travel

Pre-Clearance / DTC
Biometric Verification

Multi-Modal
Processing

Low-Risk Traveler
Segmentation

Operations
Integration

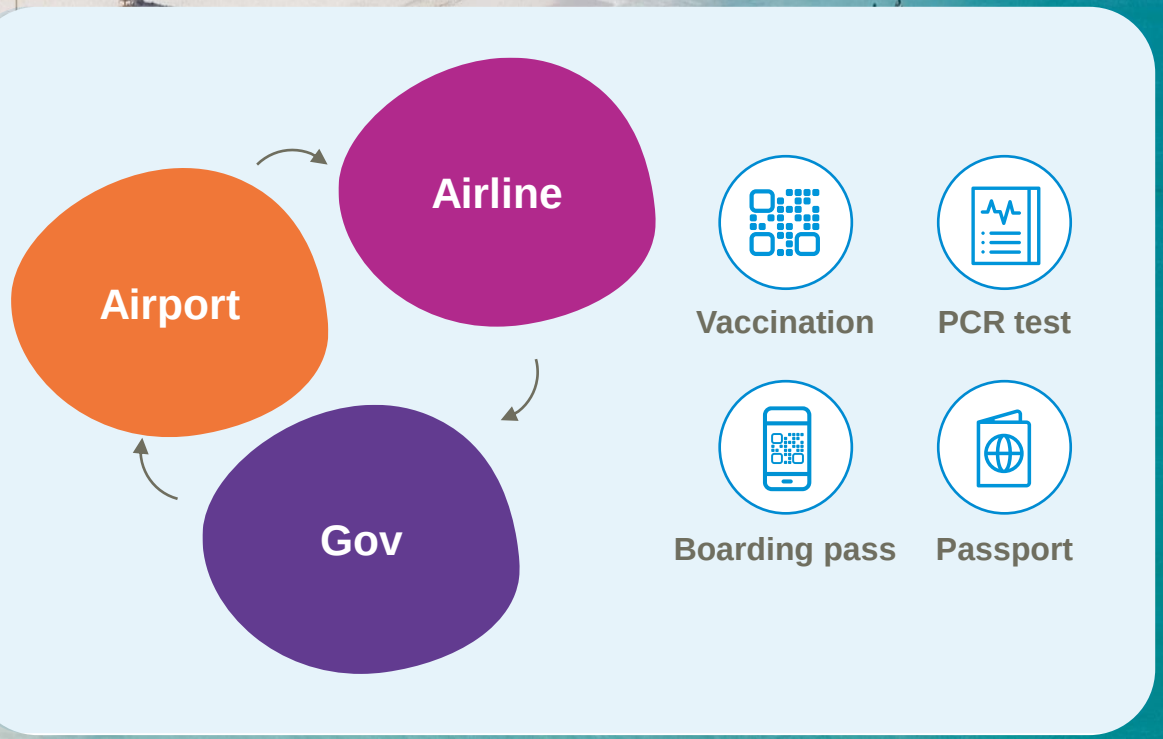
Dynamic Staffing Culture

Standards and
Interoperability

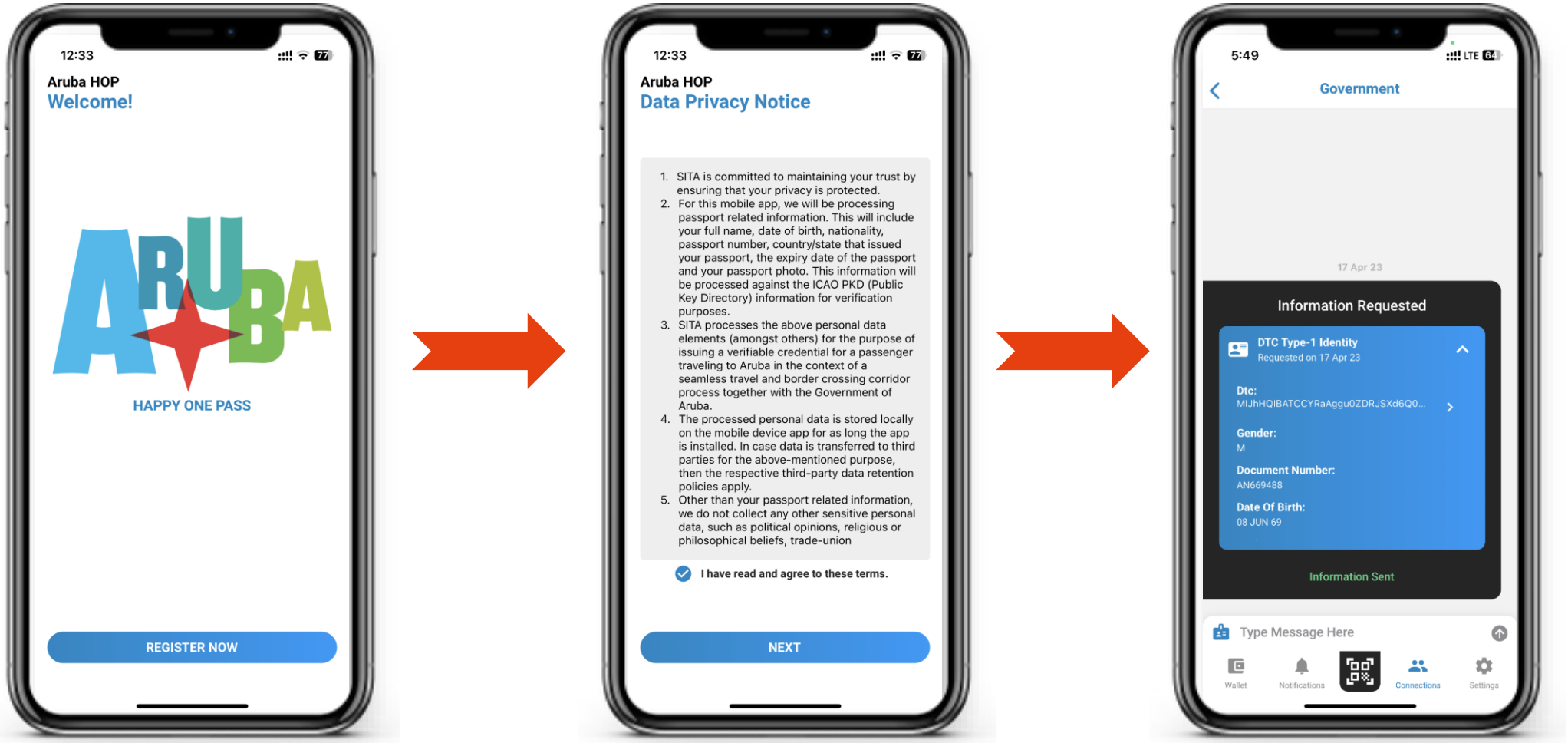
The Aruba Story – Realizing Digital Travel

Drivers for Change

1. Long immigration wait times (entry/exit). Long US departure boarding time
2. Travel process is cumbersome, clashes with the Holiday mood
3. Need safer, secure identity verification for travelers
4. Evolve passenger processing in a competitive travel and tourism market. Data Privacy, control, convenience
5. Facilitation for off airport vendors, quickest way to the beach



Aruba Happy One Pass

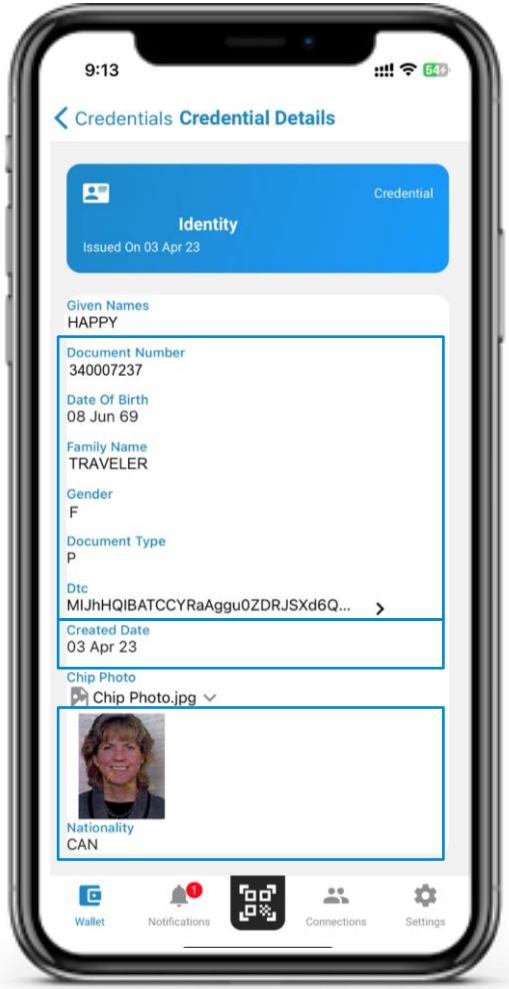


Aruba Happy One Pass

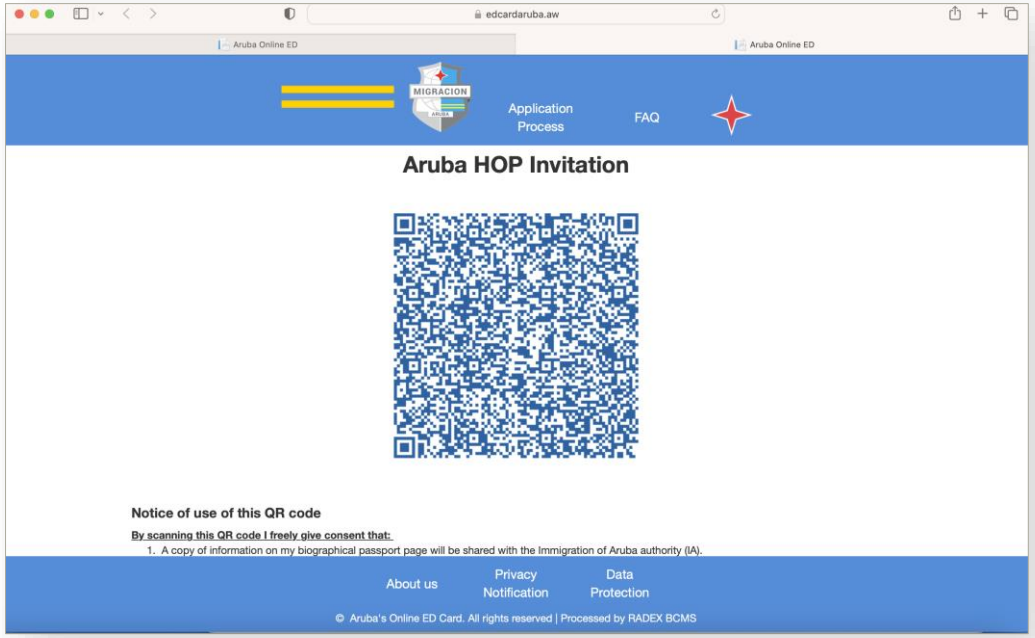
eMRTD Biographic Information (DG1)

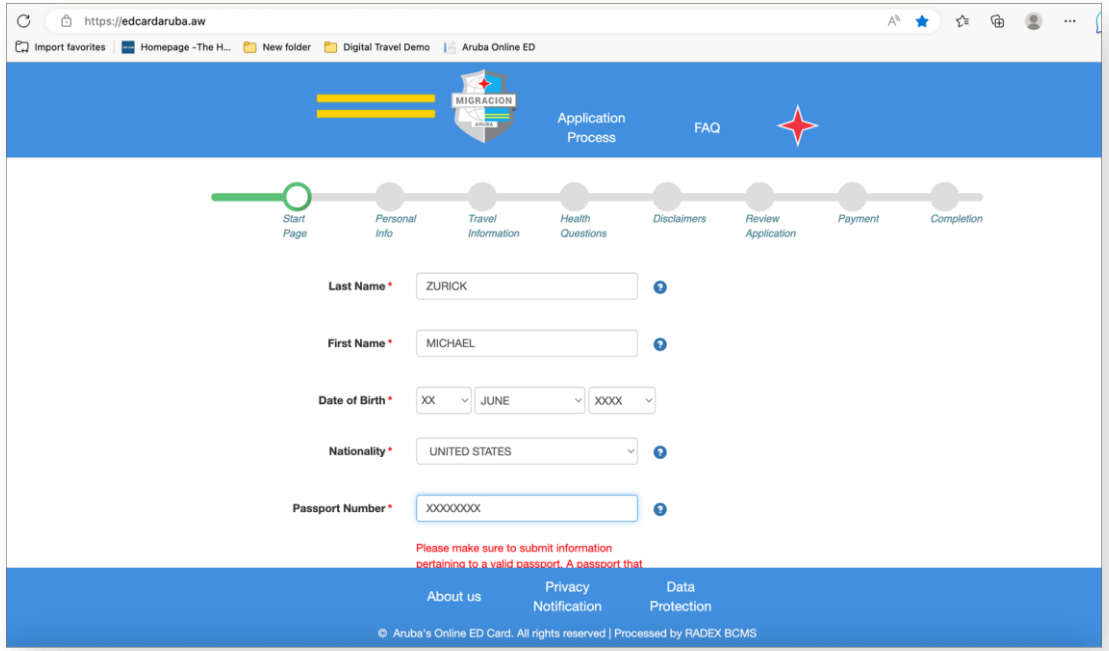
ICAO DTC

Biometric Photo (DG2)



Aruba Happy One Pass – ED Card + DTC





Travelers are able consent to share their personal information from the comfort of their home

Government is able to address historical data quality issues by travelers

SITA Trust Network

Part 3:

Data Breach Response -

Suggested “Executive Playbook” for the First 48-72 Hours

WALA 2023
Hosted by

GROUPE ADP

SITA

Data Breach!

This is written mainly from a GDPR EU/EEA and UK perspective but has global applicability

The first 48-72 hours is a vital time period after discovery of any cyber-attack on your organisation that may involve personal data or critical data.

If your organization is unfortunately targeted, the following is suggested as a practical list or “playbook” at Executive level for actions.

A Checklist – Six Vital Things

1. Minutes & Resources
2. Policies
3. Legal Privilege
4. Board Communications
5. Notifications:
    a) Govt Regulators
    b) Law Enforcement
    c) Stakeholders/Customers
    d) Banks / Credit Card issuers
6. Publicity

1. Minutes & Resources

This will become important later:

Immediately start minuting all meetings from the get-go.

You will need resources – including admin resources – for tracking all meetings and decisions made.

A clear record of managers' involvement is important.

2. Policies – Follow them

The question will come up:
Did you follow your Crisis / Incident Response Policies?

So: minute that you are following your policies or if deviating, make sure that this is also minuted with the reasons.

E.g. If the policies say that Head of IT Security is to chair meetings, make sure that occurs.

Ransomware response?

3. Legal Privileged – Use It

The inhouse legal team should engage external lawyers to ensure full privilege applies right away.

You likely will want to engage specialist security consultants – but you can have the law firm engage them to have a stronger privilege position here, if loss or harm is anticipated.

4. Board Communications

Start Board reporting – being brief, formal reports that confirm team leadership, organisation and actions.

Request Board feedback and direction.

Ensure that reports confirm the application of the company’s policies.

5. Stakeholder Notifications – Action ASAP

- Prepare to advise stakeholders. For airports: may include airlines, govts, banks, credit card issuers if relevant.

- Consider necessary regulator notifications. Even as sub-processor/contractor it can be mandatory to report.

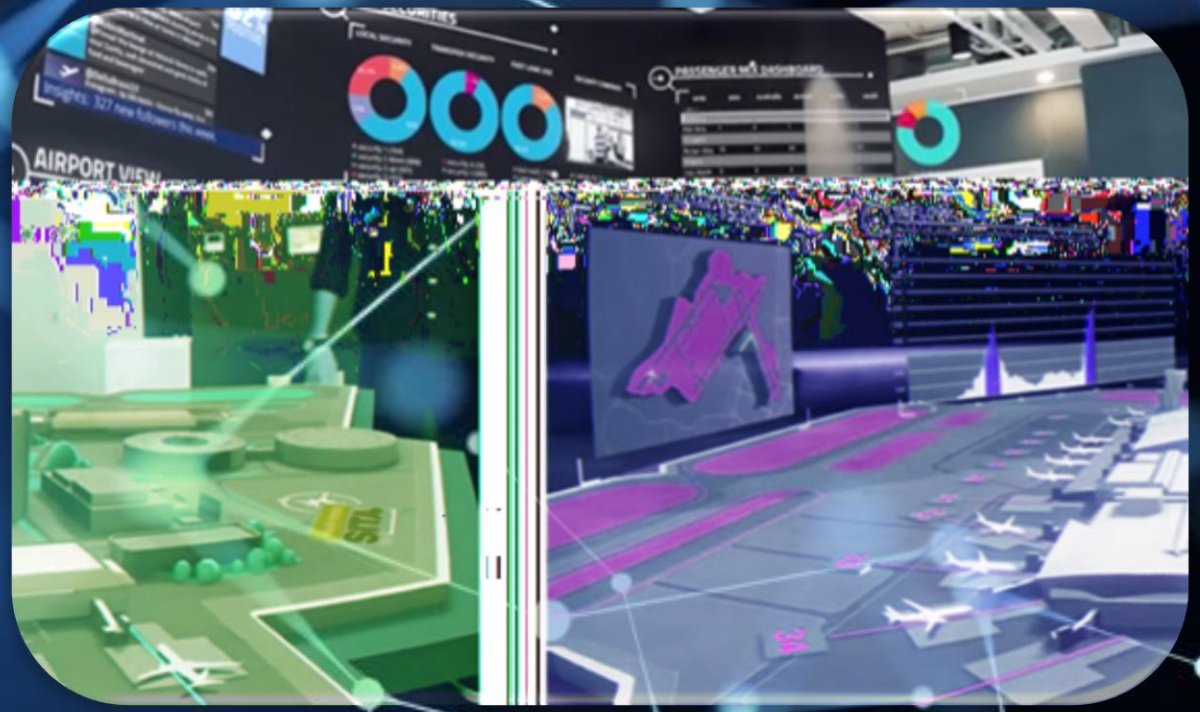
- Consider law enforcement – e.g. cyber-crime divisions.

- Laws often mandate that suppliers notify customers "without undue delay" – 72 hours may be maximum time period but regulators now expect impacted parties to notify ***as soon as there is a reasonable suspicion of a breach*** (as do controllers in contracts with suppliers).

6. Publicity – Expect it

Your Communications/Marketing team will need to prepare a responsive statement and begin to consider proactive website or other statements.

Be aware that journalists requesting comment often provide only a short window of time before going to press.



Final Thoughts and Q&A

- Data breaches are becoming more common.
- Dealing with trusted providers is key to risk reduction.
- If your organization is unfortunate to be a target, and the data incident that you are managing is serious, ensuring that the first hours are handed in the most expedient way will support future loss mitigation and damage control.

Stephen Baird
Associate General Counsel
Stephen.Baird@sita.aero

Tatiana Arima Cohen Zaide
Legal Director, Americas
Tatiana.Arima@sita.aero

Thank you!

WALA 2023
Hosted by

GROUPE ADP

SITA