

Keynote Speaker  
Tarquin Follis OBE  
Founder & Innovation Director  
Othrys Ltd.



# Cyber Attack on Business Systems

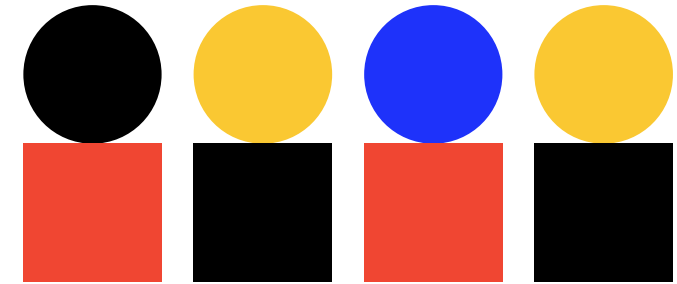
## Part 1

### Co-Chairs:

- Reid Sawyer (Marsh USA) and Rob Lawson QC (Clyde and Co.)

### Panelists:

- Pascal Buchner (IATA)
- Ria Thomas (Brunswick Group)
- Elmarie Marais (Go Crisis)
- Andrew Tsonchev (Darktrace)
- James Tuplin (AXA/XL)
- Felicity Burling (HFW)
- Helen Bourne / Tom White (Clyde and Co.)
- Mark Whitehead (Deloitte)
- Tarquin Folliss (Othrys Ltd.)



# Scenario 1

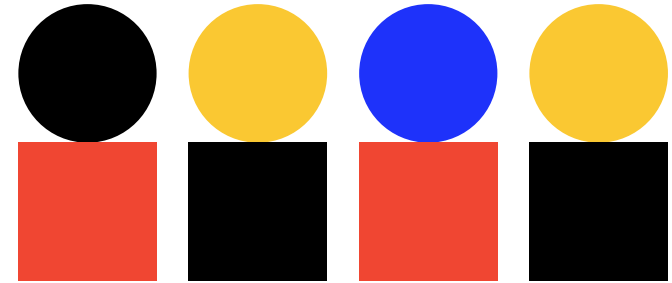
## INCIDENT TAKES PLACE

The DG receives an untraceable email from the hacker who claims credit for the compromise of the DPC at ACCA and attempts to extort money from your organization to avert public disclosure. The message says that the hacker has full control of the DPC and that he has exfiltrated 2 million of credit card information with all the Personal Identifiable Information from the credit card holder. The email includes current, dated admin screen shots of the BSP. The email states that IATA has 24 hours to pay a ransom of \$1 million or the BSP will be shut down and data will be sold on the Dark Web.

One hour after the email to the DG, while ACCA has started their security investigations, the hacker disconnects all ACCA internal logins and shuts down the iBSP production environment by installing a ransomware on the systems;

IATA is now unable to process settlement transactions, meaning funds can't be transferred to Airlines. Some travel agencies might be blocked in selling ticket in case they have reached the limit of the bank guarantees.

The ACCA Backup site has also been locked down with a ransomware and is not available.

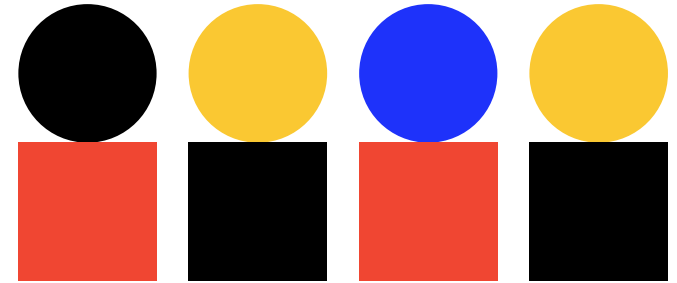


# Scenario 2

## INVESTIGATION DEVELOPS – DATA BREACH DISCOVERED

Meanwhile, cybersecurity experts have completed the assessment and found out the entire ACCA domain has been compromised and the hacker has had access to credit card details of customers, as alleged in the ransom demand.

Rebuilding the production environment is not an option. A new hosting site must be set-up from scratch. It could be at the same location, but it must be segregated from the existing infrastructure and should reuse any of the existing equipment.



# Scenario 3

## PR and Public Knowledge of Incident

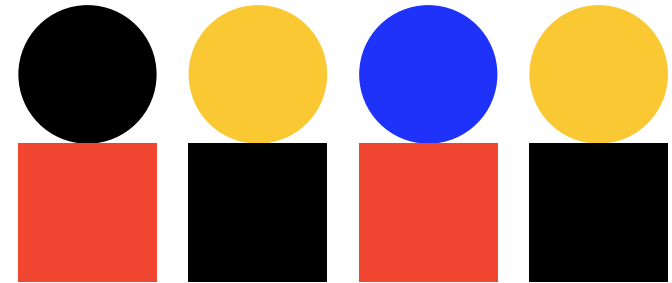
After notifying the police, IATA tries to negotiate with the hacker and delays in paying the ransom; the hacker subsequently shuts down all the IATA domain controllers preventing employees to access their systems from the office.

The media have started calling / emailing account managers / IATA generic emails asking for more information. Reuters have sent a set of questions and said they will publish an article in 30 mins with or without IATA comment.

Social media activity is starting to increase. Direct questions to IATA being asked on Twitter, FB and LinkedIn. Tweets growing as well as direct questions - @IATA has the global billing and settlement system have been hacked? Hash tags being used: #IATAHack #IATAHacked

Questions are being posted on the intranet by staff asking what's going on. Reuters publish their article – sparking major media interest. The article incorrectly alludes to the fact that customer credit card details maybe compromised.

Media enquiries continue to increase. Phones are ringing off the hook with questions from media, passengers, banks, GDS's. IATA employees from across the organization are requesting more info on the situation and asking what they should respond to their stakeholders / customers. CNN, BBC, ABC, Fox News have all requested interviews with DG.



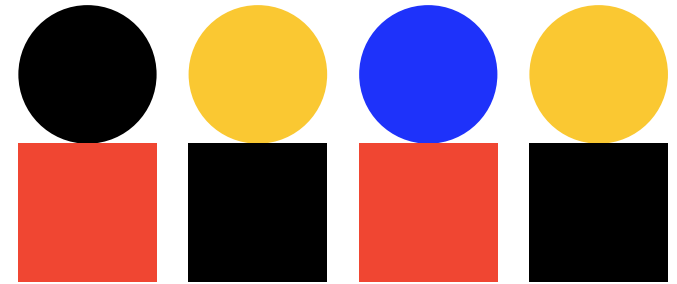
# Legal Panel - Part 1

## Co-Chairs:

- Joanna Kolatsis (Themis)

## Panelists:

- John Samiotis (Clyde and Co.)
- Giles Kavanagh (HFW)
- Mark Welbourn (Kennedys)
- Bart Banino (Condon and Forsyth NY)
- Joanna Kolatsis (Themis)
- Saleema Brohi (ASB Law LLP)





# The Triumph of Consumerism – a brief case study

John Samiotis  
Partner Clyde & Co LLP  
RIM Forum, London – 15 May 2019





# The Triumph of Consumerism

---







---


Around the world legislatures and courts are doing their utmost to ensure that consumers are fairly treated by airlines...but what is fair?




---

There are numerous examples:

- EC Regulation 261 for the payment of compensation for cancellation, delay and denied boarding in the European Union
- Consumer courts at airports in Brazil where passengers can file their claims immediately after their travel
- Malaysia – following EC 261 style regime via Malaysian Aviation Consumer Code 2016, in operation since 1/7/16
- Korea – Korean Consumer Dispute Standards
- Taiwan – Regulations on Civil Air Transport Enterprise

- 
- 
- ..... and in India we have Civil Aviation Requirements ( CAR ) Section-3, Series-M, Part-IV

- 
- 
- Facilities to be provided to passengers by airlines due to denied boarding, cancellation of flights and delays
  - Applies to all scheduled and non-scheduled carriers and to foreign carriers and/or the regulations of their country of origin

# Denied Boarding

---

- If carrier fails to organise alternative flight within one hour of scheduled departure then carrier must pay 200% or 400% of one way basic booked fare plus airline fuel surcharge up to a maximum of:
  - 10,000 INR if airline arranges flight within 24 hours of booked departure
  - 20,000 INR if airline arranges flight to depart more than 24 hours of booked departure
- If passenger does not opt for alternative flight, refund of full value of ticket and compensation equal to 400% of booked one way basic fare plus airline fuel surcharge to a maximum of 20,000 INR



# Cancellation

---



If flight is cancelled within 24 hours of scheduled departure passengers get a refund of the ticket plus:

- 5,000 INR or booked one way basic fare plus airline fuel surcharge whichever is less for flights having a block time of up to 1 hour
- 7,500 INR \_\_\_\_\_ of between 1-2 hours
- 10,000 INR \_\_\_\_\_ of more than 2 hours
- Plus facilities ( meals, refreshments, hotel accommodation where necessary )

# Delay

---



Airlines to provide facilities if the passenger has checked in on time and if the airline expects a delay beyond its original announced scheduled time of departure or a revised time of departure of:

- 2 hours or more in case of flights having a block time of up to 2.5 hours
- 3 hours or more in cases of flights having a block time of between 2.5 and 5 hours
- 4 hours or more in cases other than the above

# Defences

---



No obligation to pay compensation for cancellations and delay where these have been caused by an event of force majeure ie extraordinary circumstances beyond the control of the airline and which could not have been avoided even if all reasonable measures had been taken by the airline eg:

- Political instability
- Natural disaster
- Civil War
- Insurrection
- Riot etc

# Consumerism in the State Consumer Dispute Redressal Forums

---

- Pro consumer in outlook ( somewhat obviously!)
- Cheap to use in that there is either no fee or a negligible one to pay
- Impose strict deadlines on the Defendant party – the airline – for example a Reply must be filed within 45 days of service of the proceedings and if it isn't the case can be decided ex parte; Claimants are frequently granted adjournments

# Consumerism in the State Consumer Dispute Redressal Forums

---

- Reported cases demonstrate either an ignorance or wilful blindness to the application of basic concepts in aviation law eg the Montreal Convention
- Regularly award damages for mental agony and harassment where perception is that the airline has been deficient in the providing of services to passengers
- Some cases suggest that remedies under the Consumer Protection Act 1986 are in addition to those contained in the Montreal Convention 1999





# SANCTIONS

Update

15 May 2019

Mark Welbourn  
Partner - Kennedys Law LLP

Kennedys

# Overview

1. JCPOA Update
2. Recent Activity
3. Enforcement Action
4. OFAC Sanctions Compliance Programme (SCP) Guidelines

# JCPOA Update

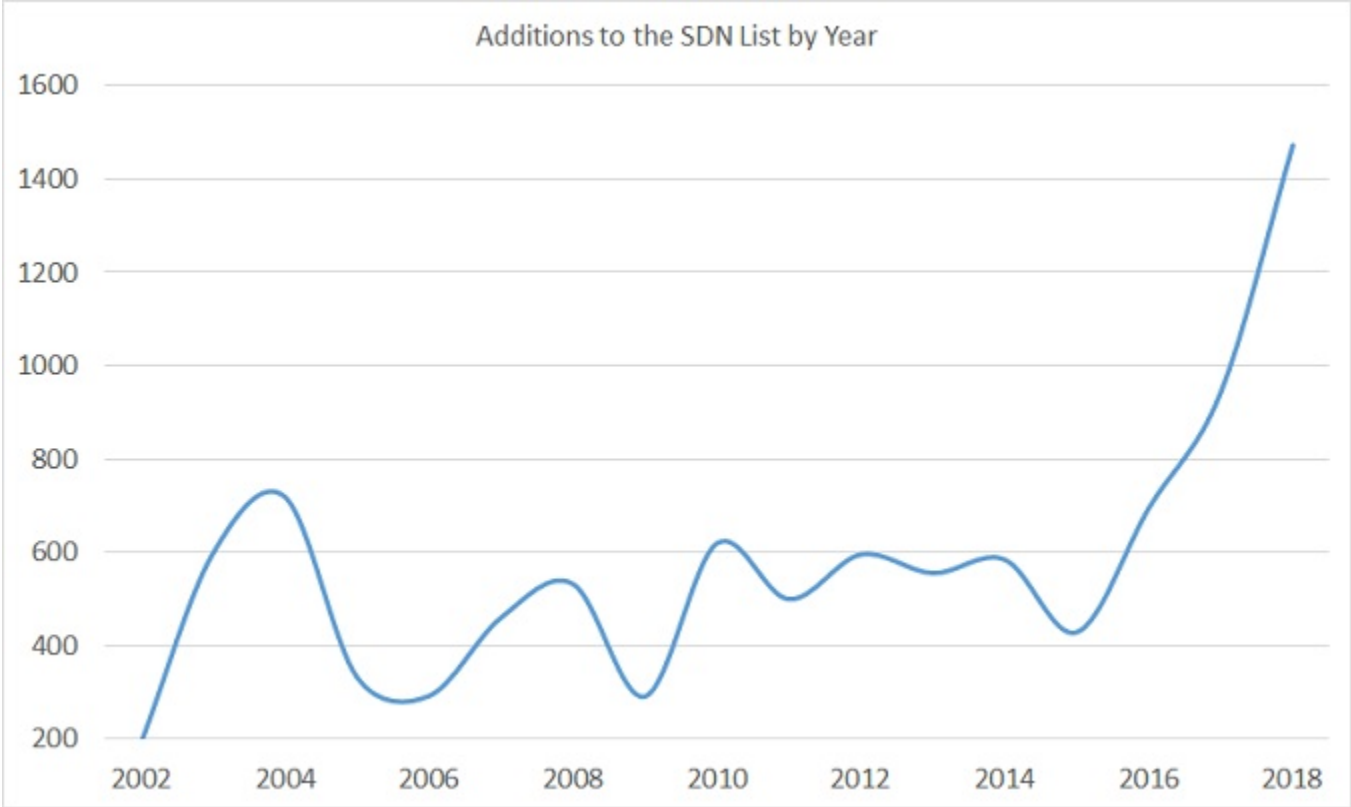
US Abandons P5+1 Nuclear Deal and re-imposes nuclear sanctions on Iran.

EU extends “Blocking” Regulation to prohibit EU entities and persons from complying with new US sanctions on Iran.

UK, France and Germany established SPV in Jan. 2019 to facilitate non US\$ trade with Iran (INSTEX - Instrument in Support of Trade Exchanges) to permit trade without relying on direct financial transactions.

# Additions to US SDN list by Year

Approx 1500 persons designated in 2018



# General Licence H





# General Licence J



DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

## OFFICE OF FOREIGN ASSETS CONTROL

### Iranian Transactions and Sanctions Regulations 31 C.F.R. Part 560

#### GENERAL LICENSE J

##### **Authorizing the Reexportation of Certain Civil Aircraft to Iran on Temporary Sojourn and Related Transactions**

(a)(1) The reexportation by a non-U.S. person of Eligible Aircraft to Iran on temporary sojourn is authorized, provided all of the criteria set forth in paragraph (b) are satisfied.

(2) For purposes of this general license, the term “Eligible Aircraft” means a U.S.-origin fixed-wing civil aircraft or non-U.S.-origin fixed-wing civil aircraft of which U.S.-controlled content constitutes 10 percent or more of the total value and that is (i) classified under Export Control Classification Number (ECCN) 9A991.b on the Commerce Control List (CCL) of the Export Administration Regulations (15 C.F.R. parts 730 – 774) (EAR), and (ii) registered in a jurisdiction other than the United States or any country in Country Group E:1 of Supplement No. 1 to Part 740 of the EAR, which includes Iran. See 31 C.F.R. §§ 560.205(b)(2) and 560.420 for information on what constitutes U.S.-controlled content.

**Note to paragraph (a):** This paragraph does not authorize the reexportation of any rotary wing aircraft or unmanned or optionally-piloted aircraft to Iran on temporary sojourn.

(b) All of the following criteria must be satisfied for a non-U.S. person to reexport an Eligible Aircraft to Iran pursuant to paragraph (a) above:

# Recent US Sanctions Developments

1. Russia - SDN designations on 40 Russian oligarchs and officials, and implementation of CAATSA. CBW sanctions - expanded export controls.
2. North Korea - 56 designations targeting shipping companies.
3. Nicaragua - subject to new sanctions targeting govt. officials.

## Recent US Sanctions Developments contd.

3. Sudan - SSR removed from CFR following revocation in 2017. Remains subject to SST and relating to Darfur. Separate programme relating to South Sudan remains in place.
4. Venezuela - PdVSA designated on 31 Jan 2019, OFAC asserted jurisdiction over Venezuela's new cyber currency.

# Magnitsky Sanctions

Gives the US President authority to sanction individual perpetrators of serious human rights abuses and corruption:

Imposed on 17 Saudi nationals associated with the death of death of Jamal Khashoggi

Over 100 individuals and entities sanctioned under the Trump E.O. issued in Dec 2017, including 2 Turkish government ministers over the imprisonment of an American pastor.

# Enforcement Actions

In 2018 OFAC netted US\$71,510,561 in penalties through 7 enforcement actions.

JP Morgan Chase - US\$5,263,171 to settle potential civil liabilities for operating an airline net settlement mechanism among various airline industry participants between 2008 and 2012. US\$1.5million of US\$1 billion of processed transactions attributed to the interests of designated entities.

Societe General - New York State Department of Financial Services levied fines totalling US\$420 million (out of a global US\$1.34 billion settlement agreement) for non US individuals originating US\$ transactions contrary to US sanctions programmes.



# “Facilitation”

“directing, approving, assisting or otherwise supporting a transaction by a third party with a sanctioned party that would be unlawful if undertaken by a US person .....”.

31 CFR 560.208 (Iran sanctions) - US persons may not approve, finance, insure or guarantee any transaction in which they themselves are prohibited from engaging...

# *Mamancochet Mining -v- Aegis*

English High Court - whether insurers under a marine policy could rely on a sanctions clause to avoid payment of a first party claim arising from the theft of steel billets on arrival in Iran.  
Insurer an EU subsidiary of a US insurer.

*“No (re)insurer shall be deemed to provide cover and no (re)insurer shall be liable to pay any claim or provide any benefit hereunder to the extent that the provision of such cover, payment of such claim or provision of such benefit would expose that (re)insurer to any sanction,....”.*

Held that it was insufficient for insurers to simply demonstrate that there was a risk of payment being prohibited, but rather the defendant underwriters must evidence that, on the balance of probabilities, payment *would be* prohibited.

# OFAC Sanctions Compliance Programme (SCP) Guidelines

2 May 2019: OFAC issued guidance on what constitutes an effective SCP:

1. Management commitment;
2. Risk assessment;
3. Internal controls;
4. Testing and auditing; and
5. Training.

 @KennedysLaw

 [linkedin.com/company/Kennedys](https://www.linkedin.com/company/Kennedys)

 [facebook.com/KennedysTrainees](https://www.facebook.com/KennedysTrainees)

[kennedyslaw.com](https://www.kennedyslaw.com)

Kennedys



*HFW*

AEROSPACE

**IATA RIM 2019  
EU261 – WHERE NEXT?**

**GILES KAVANAGH  
HEAD OF AEROSPACE  
T: +44 (0)20 7264 8778  
[giles.kavanagh@hfw.com](mailto:giles.kavanagh@hfw.com)**

*“The clearest and most  
comprehensive air  
passenger rights protection  
in the world”*

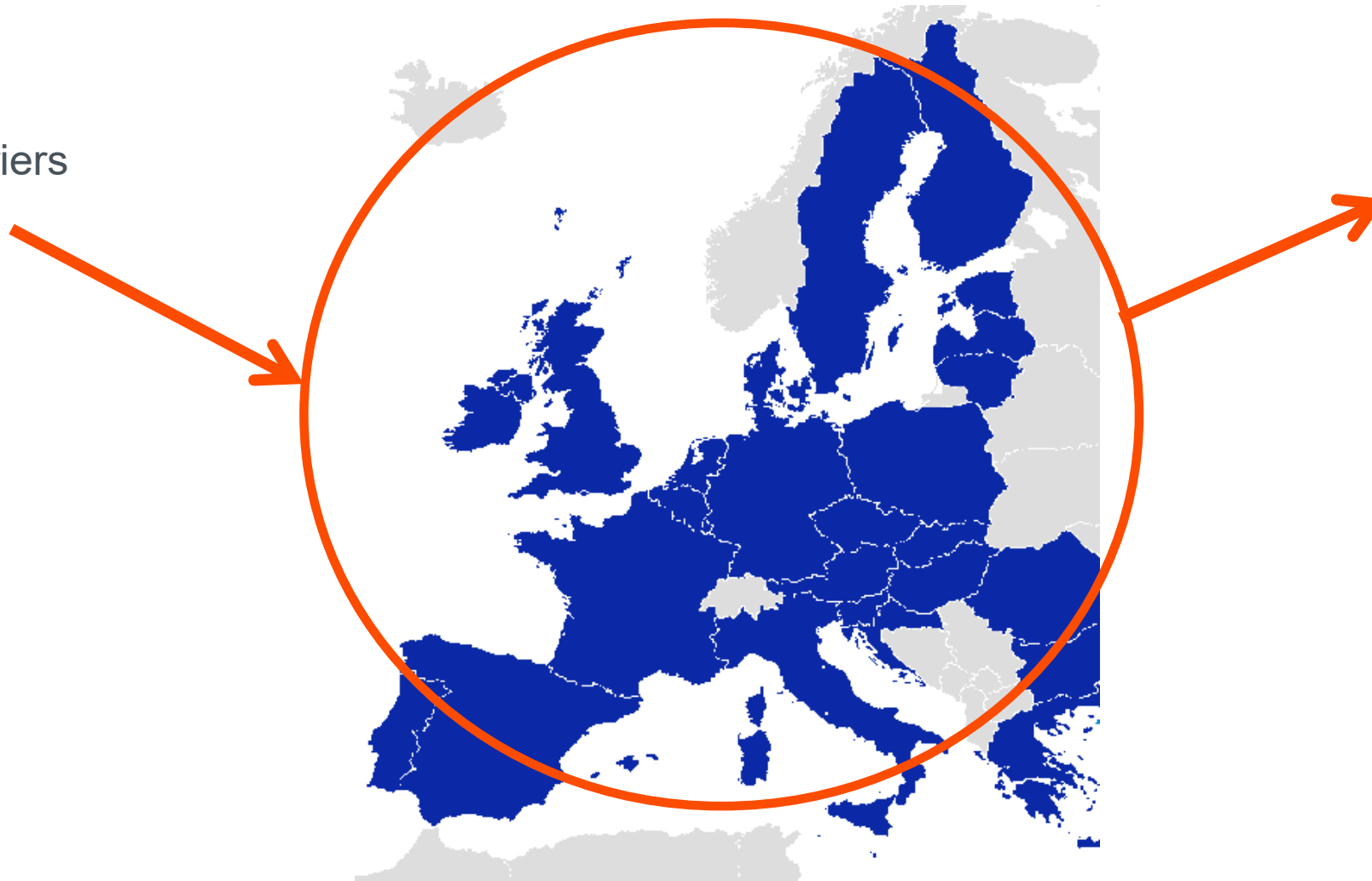
2017 Loughborough University briefing paper for the  
UK Department for Transport

- Sets out rules on compensation and assistance in the event of denied boarding, cancellation or long delays
- Entered into force on 17 February 2005
- Fixed compensation up to €600 set in line with distance travelled
- Limited defences
- Sits outside the scope of any carriage by air convention and is a complementary regime to it

- *Recital 1*: “....should aim... at ensuring a high level protection for passengers ...”
- *Recital 2*: “Denied boarding and cancellation or long delay of flights cause serious trouble and inconvenience to passengers”
- *Recital 4*: “the Community should therefore raise the standards of protection ... to strengthen the rights of passengers”



EU carriers



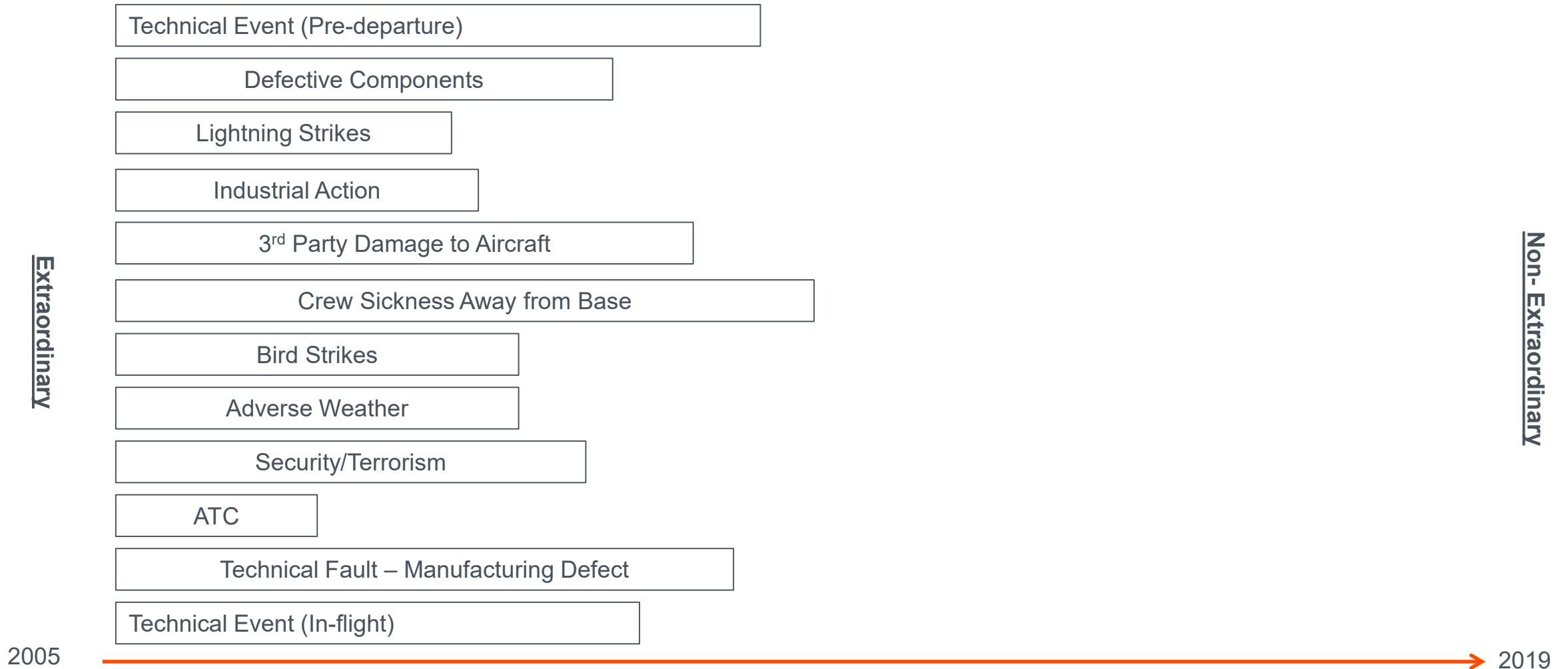
All carriers



- Two strands of compliance
  - Civil liability and court proceedings
  - NEB enforcement
- Scope of care and assistance obligations tested during 2010 volcanic ash disruption. Unambiguous expectation of regulators that they applied in full despite not being designed for extended waiting periods
- Civil liability has significantly expanded since inception through case law (both domestic and CJEU)
  - Widened scope for compensation to delayed flights (*Sturgeon, 2009*)
  - Arguably extra-territorial effect (*Gahan, 2017*)
  - Reduced the ability for airlines to rely on ‘extraordinary circumstances’



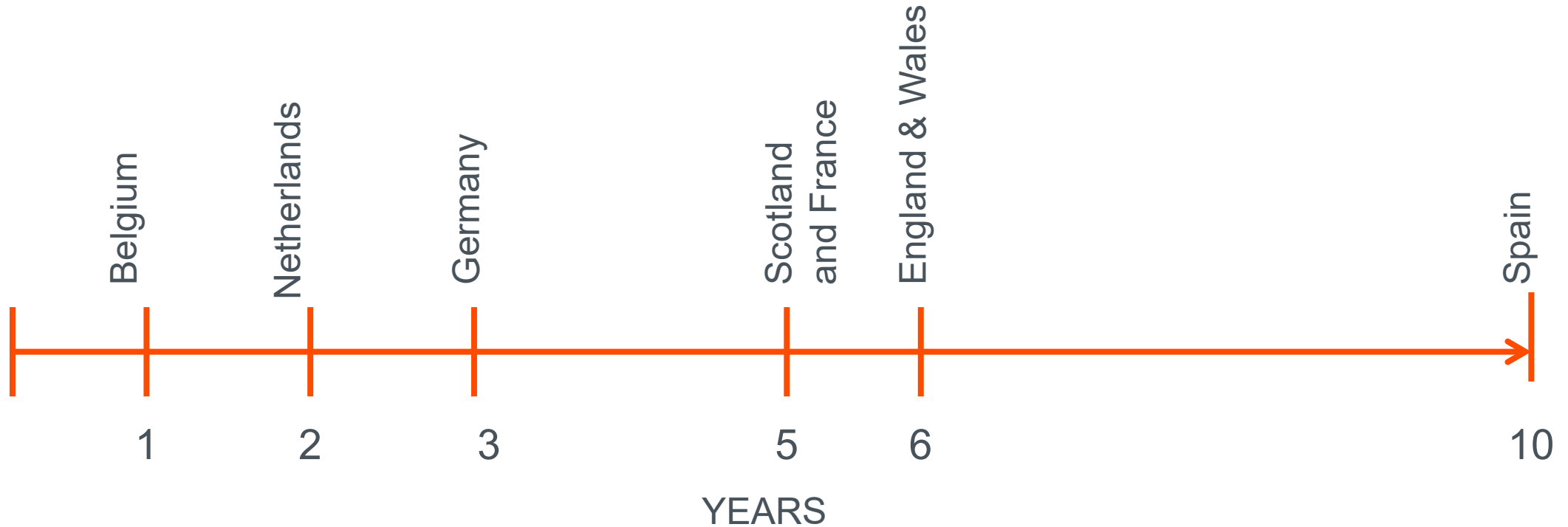
# EXTRAORDINARY CIRCUMSTANCES (ARTICLE 5(3)) EC REGULATION 261/2004





## LIMITATION PERIODS

Claims can be brought in relation to disruption up to 10 years ago because the limitation period varies according to domestic law of each EU state



“In 2016 Bott was handling approximately **1,100** flight delay compensation **claims** against Ryanair per **month**.....fee income from claims against Ryanair was over **£100,000 per month**”

(Judgment in *Bott v Ryanair* [2019] EWCA Civ 143)

- European Commission said in 2014 that the average financial cost to an airline of the Regulation was estimated at between 0.6% and 1.8% of turnover (or approximately €1-3 per one-way ticket)
- But complaints are increasing despite delays decreasing. Percentage of passengers on each flight who claim is increasing. Claims farms are harvesting claims for past delays and making the claims process easier
- Huge administrative burden set against thin profit margins
- Landscape-altering judgments result in rushes of claims when a point of law is clarified

- Impact on ticket prices?

*“It could cripple budget airlines’ pricing models and possibly worsen the financial troubles of airlines already struggling in a tough economy.”*

**Martin Lewis, moneysavingexpert.com**

- Claims companies argue that this is scaremongering

*“the reality is that at the most the airlines are paying out just €4000-€5000 per claimable flight. Their own accounts show that Ryanair make that much money before breakfast.”*

**Bott & Co website**

HFW



INSOLVENCY  
EC REGULATION 261/2004



- EU261 is unlikely to have been the trigger for the failures, but it cannot be discounted as a contributory factor
- Primera was advertising and selling one-way fares from Europe to the US for just \$149. However, the equivalent amount of compensation it would have been required to pay passengers under EU261 was approximately \$700 - almost 5 times what the passenger had paid them.

“The current system of compensation for delay, cancellation and denied boarding provided by EU Regulation 261/2004 provides strong levels of consumer protection, and **the UK will not fall below current standards of protection when we leave the EU**”

“We will put **consumers at the centre** of our aviation strategy. Great customer service through better information, quick and efficient compensation, and support to passengers with reduced mobility, will go a long way to achieving our **objective of a consumer-led aviation sector**”

“the government wants to open a debate on how a compensation scheme should work in the interests of consumers. As part of this, the government will consider what means are available to **increase the claim rates**, such as strengthening or clarifying the requirement for airlines to inform passengers affected by disruption that they might be entitled to compensation”

“other solutions the government will explore further include setting key performance indicators for airlines to respond to complaints so enforcement action can be taken if they are not met, **giving the CAA greater powers to enforce the existing regulations**, and making the compensation arrangements clearer for passengers”

- Revisions proposed in 2013 have been stalled at Council and Parliament level over the Gibraltar airspace dispute. When Britain exits the Union this deadlock could fall away. 2015 Commission strategy paper urged the Parliament and Council to swiftly adopt the amendments
- Certainty is needed; claims farms are exploiting uncertainty
- Airlines will need to lobby hard to preserve the positive proposals, which are under threat
- EU261 has been used as a model for air passenger rights legislation elsewhere in the world – Brazil, Israel, the Philippines and the Middle East. The problems in applying EU 261 have not acted as a deterrent. The shape of a new EU261 is therefore likely also to influence the development of air passenger rights in other parts of the globe – so the legislators need to get it right

### Downside

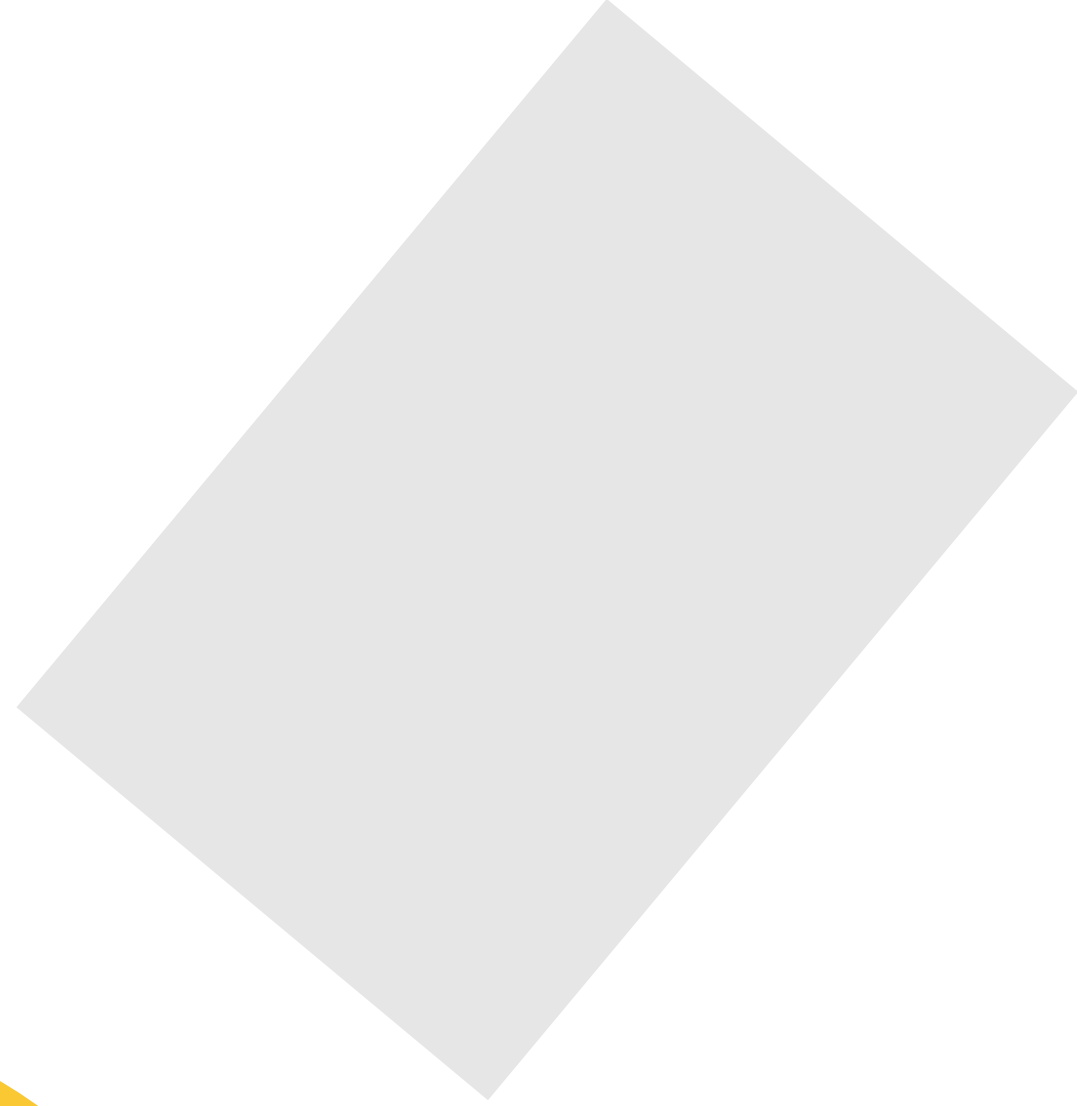
Revised Regulation likely to enshrine judge-made law re compensating for delay, unavailability of extraordinary circumstances defence for technical problems and liability for missed connections

### Potential upsides

Better definition of extraordinary circumstances, proposed minimum 5 hour delay to trigger compensation, proposed cap on care and assistance obligations to three nights at €100 per night



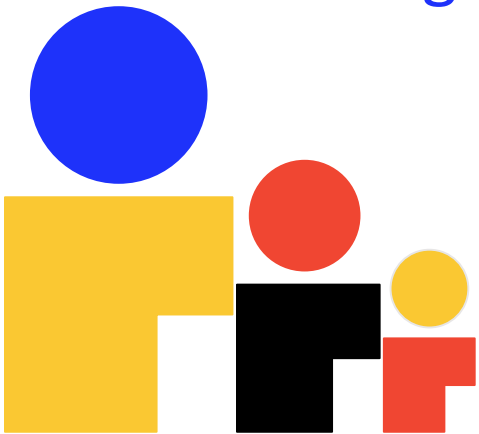
Dexter Morse, PhD  
Director, Industry Risk  
Management & Insurance  
IATA



# Rogue Employees - *The Insider Threat*

A determined “*Rogue employee*” can severely harm an employer by:

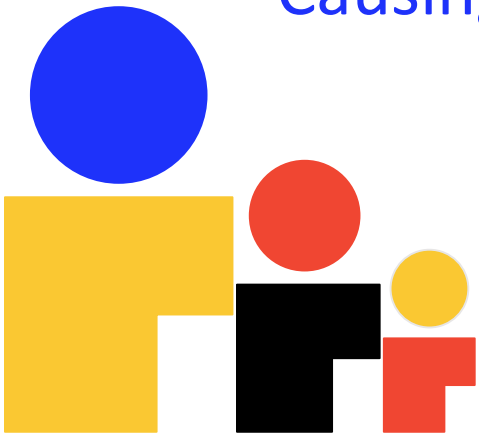
- Destroying computer files
- Embezzling money
- Starting a social media campaign to defame the company
- Ruining the company’s reputation



# Rogue Employees - *The Insider Threat*

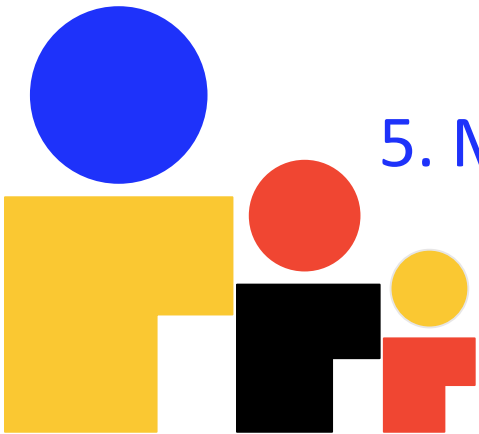
A determined “*Rogue employee*” can severely harm an employer by:

- Shredding important records & documents
- Reporting you to the authorities/regulators
- Stealing trade secrets and sharing with rivals
- Causing the company to incur expenses or liability



# Rogue Employees - *The Insider Threat*

1. Ambitious, Resourceful and Independent individual
2. Disgruntled Employees/Revenge seekers
3. Negligent Employees
4. People with secret political affiliations/loyalties
5. Mentally ill employees



# Rogue Employees - *The Insider Threat*

## Examples:

“Papering over the Cracks” – Georgian Pacific Mill

Employee tries to de-rail the Railway – Canadian Pacific Railway

“Sticking the Boot in” – Texan cowboy boot manufacturer

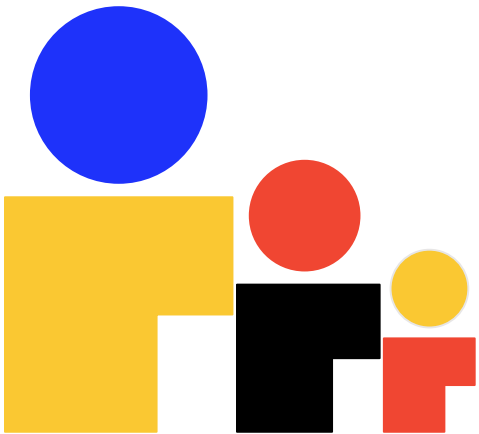
“Tick Tock” - Fanny Mae



# Rogue Employees - *The Insider Threat*

## Intellectual Property

- Financial Trading Codes – KCG
- Outfoxing Fox – LA Times Website
- Morgan Stanley



## Data Protection

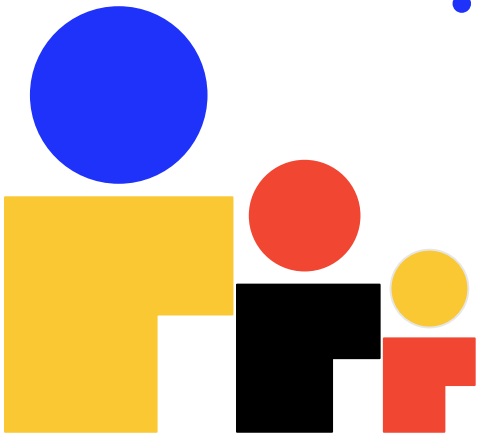
- W.M. Morrison Supermarkets



# Rogue Employees - *The Insider Threat*

## Suicides

- Horizon Air / Alaska Airlines
- Germanwings
- Financial Institutions / Telecoms



# Rogue Employees - *The Insider Threat*

## Final considerations

- Detecting potential “*Rogue employees*” remains very difficult
- Strict data protection and privacy laws prevent finding out problematic details about employee profiles and health issues
- Have proper procedures in place in relation to departing employees, be proactive, act swiftly if foul play is suspected & compile evidence.
- Improving working conditions and creating an inclusive and supportive work culture may help deter a desire to go *rogue*





# Cyber Attack on Business Systems

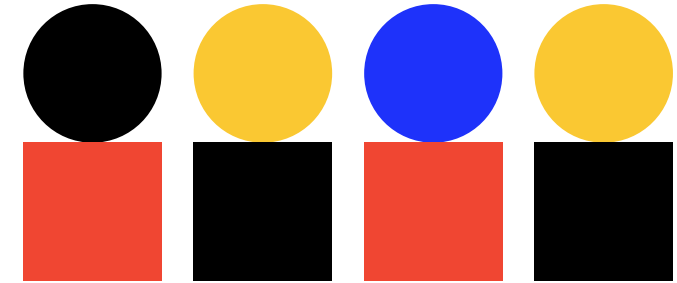
## Part 2

### Co-Chairs:

- Reid Sawyer (Marsh USA) and Rob Lawson QC (Clyde and Co.)

### Panelists:

- Pascal Buchner (IATA)
- Ria Thomas (Brunswick Group)
- Elmarie Marais (Go Crisis)
- Andrew Tsonchev (Darktrace)
- James Tuplin (AXA/XL)
- Felicity Burling (HFW)
- Helen Bourne / Tom White (Clyde and Co.)
- Mark Whitehead (Deloitte)
- Tarquin Folliss (Othrys Ltd.)



# Scenario 1

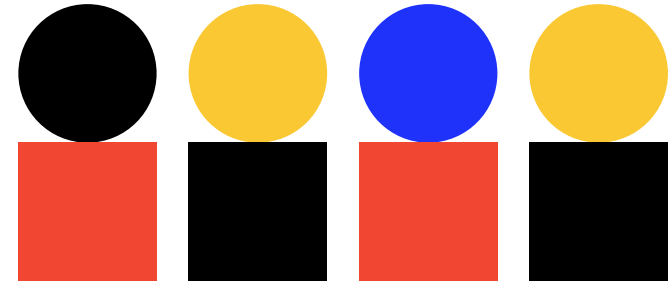
## INCIDENT TAKES PLACE

The DG receives an untraceable email from the hacker who claims credit for the compromise of the DPC at ACCA and attempts to extort money from your organization to avert public disclosure. The message says that the hacker has full control of the DPC and that he has exfiltrated 2 million of credit card information with all the Personal Identifiable Information from the credit card holder. The email includes current, dated admin screen shots of the BSP. The email states that IATA has 24 hours to pay a ransom of \$1 million or the BSP will be shut down and data will be sold on the Dark Web.

One hour after the email to the DG, while ACCA has started their security investigations, the hacker disconnects all ACCA internal logins and shuts down the iBSP production environment by installing a ransomware on the systems;

IATA is now unable to process settlement transactions, meaning funds can't be transferred to Airlines. Some travel agencies might be blocked in selling ticket in case they have reached the limit of the bank guarantees.

The ACCA Backup site has also been locked down with a ransomware and is not available.

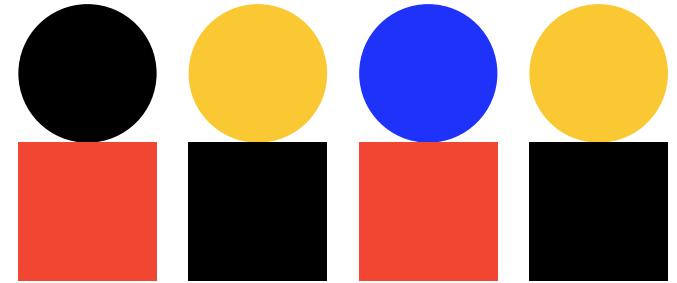


# Scenario 2

## INVESTIGATION DEVELOPS – DATA BREACH DISCOVERED

Meanwhile, cybersecurity experts have completed the assessment and found out the entire ACCA domain has been compromised and the hacker has had access to credit card details of customers, as alleged in the ransom demand.

Rebuilding the production environment is not an option. A new hosting site must be set-up from scratch. It could be at the same location, but it must be segregated from the existing infrastructure and should reuse any of the existing equipment.



# Scenario 3

## PR and Public Knowledge of Incident

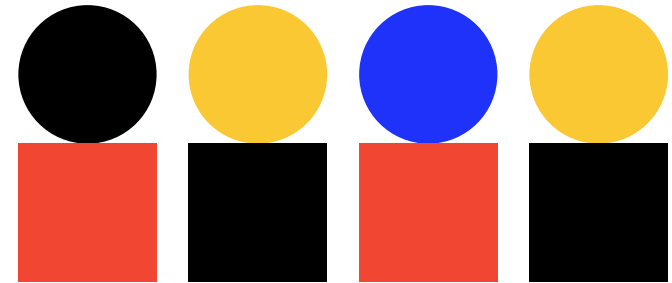
After notifying the police, IATA tries to negotiate with the hacker and delays in paying the ransom; the hacker subsequently shuts down all the IATA domain controllers preventing employees to access their systems from the office.

The media have started calling / emailing account managers / IATA generic emails asking for more information. Reuters have sent a set of questions and said they will publish an article in 30 mins with or without IATA comment.

Social media activity is starting to increase. Direct questions to IATA being asked on Twitter, FB and LinkedIn. Tweets growing as well as direct questions - @IATA has the global billing and settlement system have been hacked? Hash tags being used: #IATAHack #IATAHacked

Questions are being posted on the intranet by staff asking what's going on. Reuters publish their article – sparking major media interest. The article incorrectly alludes to the fact that customer credit card details maybe compromised.

Media enquiries continue to increase. Phones are ringing off the hook with questions from media, passengers, banks, GDS's. IATA employees from across the organization are requesting more info on the situation and asking what they should respond to their stakeholders / customers. CNN, BBC, ABC, Fox News have all requested interviews with DG.



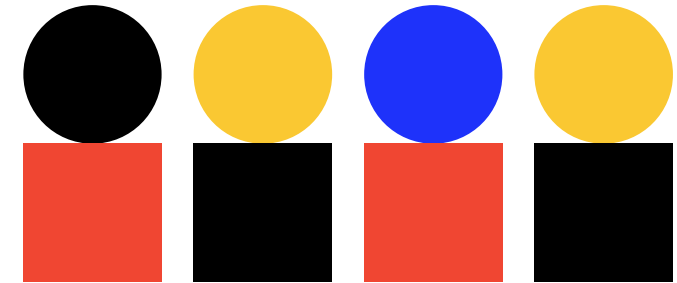
# Legal Panel - Part 2

## Chair:

- Joanna Kolatsis (Themis)

## Panelists:

- John Samiotis (Clyde and Co.)
- Giles Kavanagh (HFW)
- Mark Welbourn (Kennedys)
- Bart Banino (Condon and Forsyth NY)
- Joanna Kolatsis (Themis)
- Saleema Brohi (ASB Law LLP)



# AVN52 – IATA RIM May 2019

## AVN 48B

War, invasion, acts of foreign enemies, hostilities (whether war be declared or not), civil war, rebellion, revolution, insurrection, martial law, military or usurped power or attempts at usurpation of power.

Any hostile detonation of any weapon of war employing atomic or nuclear fission and/ or fusion or other like reaction or radioactive force or matter

Strikes, riots, civil commotions or labour disturbances;

Any act of one or more persons, whether or not agents of a sovereign power, for political or terrorist purposes, and whether the loss or damage resulting therefrom is accidental or intentional

Any malicious act or act of sabotage.

Confiscation, nationalization, seizure, restraint, detention, appropriation, requisition for title or use by or under order of any Government (whether civil, military or de facto) or public or local authority

Hijacking or any unlawful seizure or wrongful exercise of control of the aircraft or crew in flight (including any attempt at such seizure or control) made by any person or persons on board the aircraft acting without the consent of the insured.

## EXTENDED COVERAGE ENDORSEMENT (AVIATION LIABILITIES)

1. WHEREAS the Policy of which this Endorsement forms part includes the War, Hi-Jacking and Other Perils Exclusion Clause (Clause AVN 48B), IN CONSIDERATION of an Additional Premium of ....., it is hereby understood and agreed that with effect from ....., all sub-paragraphs other than ..... of Clause AVN 48B forming part of this Policy are deleted SUBJECT TO all terms and conditions of this Endorsement.

2. EXCLUSION applicable only to any cover extended in respect of the deletion of sub-paragraph (a) of Clause AVN 48B.

Cover shall not include liability for damage to any form of property on the ground situated outside Canada and the United States of America unless caused by or arising out of the use of aircraft.

3. LIMITATION OF LIABILITY

The limit of Insurers' liability in respect of the coverage provided by this Endorsement shall be ..... or the applicable Policy limit whichever the lesser any one Occurrence and in the annual aggregate (the "sub-limit"). This sub-limit shall apply within the full Policy limit and not in addition thereto.

To the extent coverage is afforded to an Insured under the Policy, this sub-limit shall not apply to such Insured's liability:

(a) to the passengers (and for their baggage and personal effects) of any aircraft operator to whom the Policy affords cover for liability to its passengers arising out of its operation of aircraft;

(b) for cargo and mail while it is on board the aircraft of any aircraft operator to whom the Policy affords cover for liability for such cargo and mail arising out of its operation of aircraft.

4. AUTOMATIC TERMINATION

To the extent provided below, cover extended by this Endorsement shall TERMINATE AUTOMATICALLY in the following circumstances:

(i) All cover

- upon the outbreak of war (whether there be a declaration of war or not) between any two or more of the following States, namely, France, the People's Republic of China, the Russian Federation, the United Kingdom, the United States of America



**(ii) Any cover extended in respect of the deletion of sub-paragraph (a) of Clause AVN 48B**

**- upon the hostile detonation of any weapon of war employing atomic or nuclear fission and/or fusion or other like reaction or radioactive force or matter wheresoever or whensoever such detonation may occur and whether or not the Insured Aircraft may be involved.**

**(iii) All cover in respect of any of the Insured Aircraft requisitioned for either title or use**

**- upon such requisition**

**PROVIDED THAT if an Insured Aircraft is in the air when (i), (ii) or (iii) occurs, then the cover provided by this Endorsement (unless otherwise cancelled, terminated or suspended) shall continue in respect of such an Aircraft until completion of its first landing thereafter and any passengers have disembarked.**

## **5. REVIEW AND CANCELLATION**

**(a) Review of Premium and/or Geographical Limits (7 days)**

**Insurers may give notice to review premium and/or geographical limits - such notice to become effective on the expiry of seven days from 23.59 hours GMT on the day on which notice is given.**

**(b) Limited Cancellation (48 hours)**

**Following a hostile detonation as specified in 4 (ii) above, Insurers may give notice of cancellation of one or more parts of the cover provided by paragraph 1 of this Endorsement by reference to sub-paragraphs (c), (d), (e), (f) and/or (g) of Clause AVN 48B - such notice to become effective on the expiry of forty-eight hours from 23.59 hours GMT on the day on which notice is given.**

**(c) Cancellation (7 days)**

**The cover provided by this Endorsement may be cancelled by either Insurers or the Insured giving notice to become effective on the expiry of seven days from 23.59 hours GMT on the day on which such notice is given.**

**(d) Notices**

**All notices referred to herein shall be in writing.**

## **EC 785/2004**

- 1. Air carriers and aircraft operators referred to in Article 2 shall be insured in accordance with this Regulation as regards their aviation-specific liability in respect of passengers, baggage, cargo and third parties. The insured risks shall include acts of war, terrorism, hijacking, acts of sabotage, unlawful seizure of aircraft and civil commotion.**

## AVN52 XS

- Cover provided for 3<sup>rd</sup> party losses above limited provision in primary policy.
- Cancellation:

*This insurance is subject to, and shall be deemed to incorporate the same Automatic Termination and Review and Cancellation provisions as are set out in the Extended Coverage Endorsement (Aviation Liabilities) AVN52E except that the cancellation notice period ... is amended ... to **thirty (30) days.***

## Special provision

In the event of the coverage provided under the Extended Coverage Endorsement (Aviation Liabilities) specified in Item 3 of the Policy Schedule contained in the Primary Policy is cancelled or withdrawn for any reason by the primary insurers this Policy is extended to apply as primary insurance to the fullest extent of the coverage provided by the said Endorsement including the Insured's liability:

- a) to the passengers (and for their baggage and personal effects) of any aircraft operator to whom the Primary Policy affords cover for liability to its passengers arising out of its operation of aircraft;
- b) for cargo and mail while it is on board the aircraft of any aircraft operator to whom the Primary Policy affords cover for liability for such cargo and mail arising out of its operation of aircraft

subject always to the Total Limits stated in Item 4 (b) of the Policy schedule

## Special provisions - continued

### Non-Cancellable

This Policy is non-cancellable except by mutual agreement between Insured and Insurers hereon, however all cover hereunder in respect of the deletion of subparagraph (a) of Clause AVN48B is automatically terminated

(a) upon the hostile detonation of any weapon of war employing atomic or nuclear fission and/or fusion or other like reaction or radioactive force or matter wheresoever or whensoever such detonation may occur and whether or not the Insured Aircraft may be involved.”

**Saleema Brohi  
Consultant**

**[saleema.brohi@asb-law.com](mailto:saleema.brohi@asb-law.com)**

**+44 (0) 7843 358935**

# Cyber Attack on Business Systems

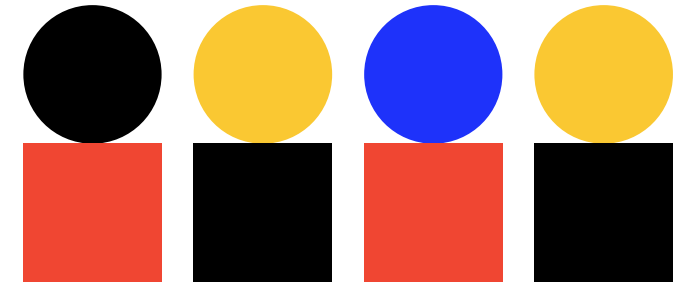
## Part 3

### Co-Chairs:

- Reid Sawyer (Marsh USA) and Rob Lawson QC (Clyde and Co.)

### Panelists:

- Pascal Buchner (IATA)
- Ria Thomas (Brunswick Group)
- Elmarie Marais (Go Crisis)
- Andrew Tsonchev (Darktrace)
- James Tuplin (AXA/XL)
- Felicity Burling (HFW)
- Helen Bourne / Tom White (Clyde and Co.)
- Mark Whitehead (Deloitte)
- Tarquin Follis (Othrys Ltd.)



# Scenario 1

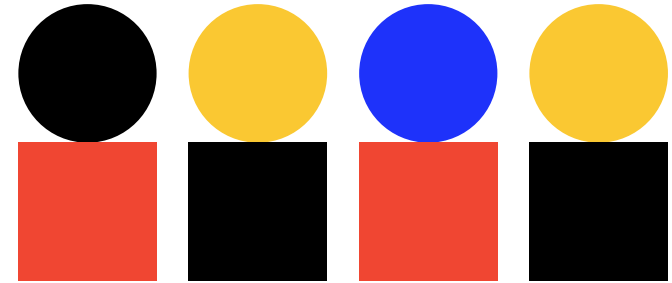
## INCIDENT TAKES PLACE

The DG receives an untraceable email from the hacker who claims credit for the compromise of the DPC at ACCA and attempts to extort money from your organization to avert public disclosure. The message says that the hacker has full control of the DPC and that he has exfiltrated 2 million of credit card information with all the Personal Identifiable Information from the credit card holder. The email includes current, dated admin screen shots of the BSP. The email states that IATA has 24 hours to pay a ransom of \$1 million or the BSP will be shut down and data will be sold on the Dark Web.

One hour after the email to the DG, while ACCA has started their security investigations, the hacker disconnects all ACCA internal logins and shuts down the iBSP production environment by installing a ransomware on the systems;

IATA is now unable to process settlement transactions, meaning funds can't be transferred to Airlines. Some travel agencies might be blocked in selling ticket in case they have reached the limit of the bank guarantees.

The ACCA Backup site has also been locked down with a ransomware and is not available.



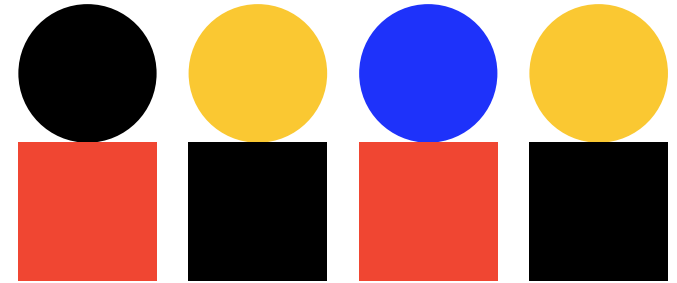


# Scenario 2

## INVESTIGATION DEVELOPS – DATA BREACH DISCOVERED

Meanwhile, cybersecurity experts have completed the assessment and found out the entire ACCA domain has been compromised and the hacker has had access to credit card details of customers, as alleged in the ransom demand.

Rebuilding the production environment is not an option. A new hosting site must be set-up from scratch. It could be at the same location, but it must be segregated from the existing infrastructure and should reuse any of the existing equipment.



# Scenario 3

## PR and Public Knowledge of Incident

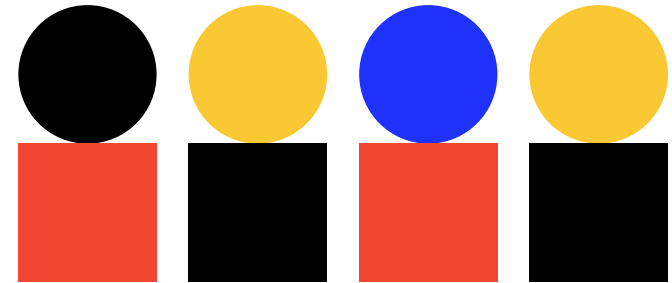
After notifying the police, IATA tries to negotiate with the hacker and delays in paying the ransom; the hacker subsequently shuts down all the IATA domain controllers preventing employees to access their systems from the office.

The media have started calling / emailing account managers / IATA generic emails asking for more information. Reuters have sent a set of questions and said they will publish an article in 30 mins with or without IATA comment.

Social media activity is starting to increase. Direct questions to IATA being asked on Twitter, FB and LinkedIn. Tweets growing as well as direct questions - @IATA has the global billing and settlement system have been hacked? Hash tags being used: #IATAHack #IATAHacked

Questions are being posted on the intranet by staff asking what's going on. Reuters publish their article – sparking major media interest. The article incorrectly alludes to the fact that customer credit card details maybe compromised.

Media enquiries continue to increase. Phones are ringing off the hook with questions from media, passengers, banks, GDS's. IATA employees from across the organization are requesting more info on the situation and asking what they should respond to their stakeholders / customers. CNN, BBC, ABC, Fox News have all requested interviews with DG.



# Thank-you to our Sponsors

