Airline outages are insurable

Last month’s global IT outage at British Airways (BA) is symbolic of the airline industry’s reliance on technology and associated exposure to business interruption. Yet this is a risk that can in large part be transferred to insurers.

The three-day global IT failure at BA from May 27 affected some 75,000 passengers and 1,000 flights, knocking the airline’s share price and reputation. The company now faces a sizable bill from compensating passengers and business interruption.

The initial estimate by BA’s owner International Airlines Group (IAG) put the cost of the outage at around USD 100 million, including lost revenue and the expense of accommodating, re-booking and compensating passengers.

While the outage was first billed as an IT failure, BA says it was in fact the result of “human error” after a contract engineer is thought to have disconnected the power at BA’s data centre. This was followed by an “uncontrolled” restoration of the company’s IT systems, which created physical damage to the systems and significantly exacerbated the problem.

The three-day global IT failure at BA from May 27 affected some 75,000 passengers and 1,000 flights.
ACHILLES HEEL

Airlines are particularly exposed to IT outages. They were early to embrace technology and are now heavily dependent on IT systems, from booking and baggage handling, to flight scheduling and operations. But ageing IT and fragile legacy systems have left them vulnerable.

The sector has experienced a string of outages in recent years. BA suffered a smaller IT failure in September, while in June the airline suffered an unspecified failure of its baggage handling system that saw thousands of passengers depart without their luggage.

A number of US airlines have also been troubled by IT outages. Delta Air Lines experienced several major outages in 2016 and 2017, one in August 2016 cost the airline USD 150 million. An outage at Southwest Airlines, which saw 2,100 fights cancelled last year, cost the airline USD 54 million.

OUTAGE INSURANCE

Although the exact cause of the BA outage has yet to be determined, cyber insurance can be tailored to provide protection for airlines cyber exposures, including IT outages. Some cyber policies will exclude losses from external power supply failure, but the cause of the disruption for BA is said to have been triggered by human error.

Cyber insurance policy wordings differ when it comes to business interruption triggers. Some will only cover business interruption following a cyber attack, while others will cover systems failure on an ‘all-risk’ basis or on a named failure basis.

The insurance industry is beginning to tailor policies to specific industry needs, and JLT’s collaborative approach across cyber and aviation has resulted in innovative thinking around the scope of cyber and IT outage coverage for airlines.

Compensation claims by passengers can also be covered by cyber insurance where an incident is caused by a cyber trigger. In an industry with paper thin margins, this expense could be the difference between making a profit or loss.

CRISIS PLANNING

Outages, like the ones suffered by BA, Delta and Southwest airlines also highlight the importance of a robust incident response plan. For all their resource, many large public companies still find themselves ill-equipped to deal with the fall-out from a cyber incident.

One crisis management expert said that the BA outage provided a “textbook” example of how organisational systems need backup and effective communications when they fail. Denis Fischbacher-Smith, Research Chair in Risk and Resilience, University of Glasgow (who experienced the disruption first hand) said that companies need to plan their response to the catastrophic failure of a critical system.

An outage at Southwest Airlines, which saw 2,100 fights cancelled last year, cost the airline USD 54 million.

Incident response assistance is the keystone of any well-crafted cyber insurance policy allowing for a structured, multifaceted response to a range of issues insureds are unlikely to have incurred before.

There are also a number of insurers that will provide “reputational harm” coverage to insureds as part of their cyber risk solution. The wordings available are quite broad and can cover any income loss, increased cost of working and PR expenses incurred during the ‘reputation indemnity period’.
GDPR already influencing cyber insurance buying

As companies struggle to prepare for the EU’s General Data Protection Regulation (GDPR), European companies are increasingly turning to cyber insurance.

We have experienced a noticeable up-tick in demand for cyber insurance from European companies ahead of the GDPR. And the prospect of stricter data protection laws has also seen a move towards higher limits, especially among first time buyers.

Previously, buyers of cyber insurance would often test the water with limits starting at 10 to 20 million, but we have recently observed new buyers starting out with programs as large as GBP 275 million.

MATERIAL FINES

From 25 May 2018, the GDPR will place a raft of data protection requirements on organisations and increase the powers of data protection regulators.

For serious breaches, firms will have to pay fines of up to 4% of their global annual turnover, or EUR 20 million, whichever is the greater. This suggests that companies can expect much larger fines under the new regime. For example, TalkTalk was fined GBP 400,000 for its October 2015 data breach. Under the GDPR the fine could have been more like GBP 59 million.

According to analysis by Oliver Wyman, FTSE 100 companies could face fines of up to GBP 5 billion for breaches of the GDPR. Had the regime been in place for the past five years, the top listed UK companies could have been fined GBP 25 billion, it said.

A separate survey from Consult Hyperion predicts that GDPR fines could cost European banks USD 5.2 billion in the first three years (not including compensation, lost business and damage to reputation). The company expects to see 120 breaches resulting in million-euro-fines, with several fines in triple digits.

FINDING SOLUTIONS

The insurability of fines for breaches of the GDPR has been a key focus for many of our cyber insurance clients.

Standalone cyber insurance will cover fines to the extent they are insurable by law. However, the extent to which insurance proceeds can be used to recoup the costs of regulator penalties under the GDPR is a grey area and one that will need to be tested in the courts.
One strategy adopted by some companies has been to shift some of their excess cyber insurance capacity to the Bermuda market. Since the Bermuda regulators do not prohibit payment of fines and punitive damages, insureds have a greater chance of recovering such fines from their Bermuda-based insurers. The cost tends to be only incrementally higher, and the capacity functions just as it would on an excess basis if purchased in the insured’s home country.

COMPLIANCE CHALLENGE

Recent surveys paint a mixed picture of GDPR readiness. Some companies may not be taking the GDPR seriously enough, even those that are finding compliance challenging.

Three quarters of organisations surveyed by Varonis Systems say they will struggle to meet the May 2018 deadline. The survey of IT decision makers in the UK, Germany, France and the US also found that 42% do not even view compliance with the GDPR as a priority.

Half of those surveyed say they are struggling with ensuring the security of information while one third of respondents had not yet conducted a data impact assessment in order to determine who has access to personal data.

In March, a survey from Crown Records Management found that one in four UK businesses have cancelled all preparations for the GDPR on the mistaken belief that it will not apply after Brexit. Worryingly, 44% of those surveyed said they didn’t think the regulation will apply to UK business after Brexit.

This is despite warnings from the Information Commissioner’s Office that it intends to implement the GDPR in the US by the deadline, and that UK data protection laws after Brexit will be aligned to those of the EU.

£59m
Could possibly have been the fine for TalkTalk under GDPR for its October 2015 data breach

£5bn
FTSE 100 companies could face this fine for breaches of the GDPR, according to analysis by Oliver Wyman

$5.2bn
Predicted GDPR fines for European banks in the first three years according to a survey by consult Hyperion

In March, a survey from Crown Records Management found that one in four UK businesses have cancelled all preparations for the GDPR on the mistaken belief that it will not apply after Brexit.
Insurers in talks to establish cyber incident database

As organisations and businesses recover from last month’s ‘WannaCry’ cyber-attack, the Association of British Insurers (ABI) is calling for a national database to record details of cyber incidents.

Increased transparency of data on cyber losses will be vital to both the development of the cyber insurance market and to better cyber security by companies.

In the case of insurance, the sharing of robust impartial data on cyber incidents could accelerate the growth and development of the cyber insurance market, potentially enabling insurers to offer more capacity and broader cover.

The lack of data on cyber losses is a “huge inhibitor” to the development of the cyber insurance market, according to the ABI. Insurers have access to over 350 years of fire data and 100 years of motor and aviation data, but have just a few years of cyber data, it says.

A central database would enable insurers to more accurately price cyber risk. More data should allow insurers to be more consistent in their pricing, reducing volatility in the market following large cyber attacks.

The lack of data on cyber losses is a “huge inhibitor” to the development of the cyber insurance market.

ABI’S PLAN

The ABI proposes to establish a not-for-profit database to record the details of cyber incidents including business interruption losses, ransom demands, loss of confidential data and damage to IT systems.

The database would build on the European Network Information Security Directive and the General Data Protection Regulations (GDPR), which require companies to report certain cyber incidents to regulators. The ABI believes that this data could be anonymised and made accessible to insurers.

The Association and other insurance industry representatives are reportedly in talks with the Information Commissioner’s Office (ICO) about establishing a cyber incident information sharing platform. It believes that such a national database would be a world first, although several states in the US already require firms to report any cyber breaches to the authorities.
Yovan Garcia reportedly accessed payroll records to inflate his wages, as well as steal data to set up a rival business.

Whether with malicious intent or just a case of human error, insiders are a significant cause of cyber incidents.

A recent survey of 4,500 CIOs by Harvey Nash and KPMG revealed that the insider threat is among the fastest-growing security risks. It found that insiders were responsible for 47% of attacks compared with 40% in the previous survey.

Analysis of cyber incidents by IBM in 2016 also identified an increasing threat to companies from employees and contractors.

It found that some 60% of cyber incidents involve an insider, up from 55% in the previous year's survey. According to IBM, one third of attacks involved “inadvertent actors” - such as an employee that mistakenly enables a cyber criminal to access systems - while almost 45% of attacks involved a malicious insider.

Whether with malicious intent or just a case of human error, insiders are a significant cause of cyber incidents.

Last month, a former private security officer in California was ordered to pay nearly USD 319,000 in damages for attacking his employer's computer systems.

Of these 77% were human error while the remaining 23% were caused by rogue employees.

30% of cyber insurance claims in 2016 were attributable to the actions of insiders.
A separate study by NetDiligence in 2016 revealed that 30% of cyber insurance claims were attributable to the actions of insiders. Of these 77% were unintentional and caused by human error while the remaining 23% were caused or abetted by rogue employees.

**GAPS IN COVER**

Cyber security procedures can help reduce incidents of human error, but the malicious actions of insiders are a more difficult risk to prevent. Pre-employment screening and cyber security procedures and processes can go only so far, but cyber insurance can cover losses associated with insider related cyber incidents.

But not all incidents that involve IT systems are cyber. Comprehensive protection from the financial impact of malicious insiders calls for both a modern, broadly drafted crime policy as well as a cyber policy.

Crime insurance and standalone cyber will both cover cyber crimes perpetrated by malicious insiders, and if both policies are as broad as current market conditions allow, there are neither gaps nor overlaps.

**COMBINED SOLUTION**

A recent development in the market has seen insurers offer combined cyber and crime insurance. These policies should be attractive for smaller companies, but they can also be used to provide larger companies with additional capacity.

Financial institutions, for example, have come to realise the need for larger limits as the true extent of their cyber crime exposures have been revealed. In 2015, criminals attempted to steal USD 1 billion from the Bank of Bangladesh. In contrast, crime insurance policies have limits of around USD 200 million to USD 400 million.

The global ransomware event that began on May 12 was a wakeup call to many, highlighting the potentially widespread impact of a single cyber vulnerability. Known as WannaCry, WCry or WannaCrypt – the ransomware is thought to have affected several hundred thousand computers in over 150 countries.

**WannaCry: Lessons for insurance**

The global ransomware attack in May is not expected to result in a material loss for the cyber insurance market. But it could prompt underwriters to review cyber related business interruption cover offered under traditional insurance policies.

The global ransomware event that began on May 12 was a wakeup call to many, highlighting the potentially widespread impact of a single cyber vulnerability. Known as WannaCry, WCry or WannaCrypt – the ransomware is thought to have affected several hundred thousand computers in over 150 countries.

**COUNTING THE COST**

Estimating the total cost of the incident is difficult, although some media reports have put the bill at around USD 4 billion. But while ransom attacks are insurable – and insurers have been notified of potential claims - cyber insurers are unlikely to foot much of the bill for WannaCry.

Cyber insurance purchasing outside the US is still relatively slow. And where companies have purchased cyber insurance, losses from WannaCry will probably fall within deductibles.

Ransom demands were also small - total ransoms paid to the cyber criminals is thought to be under USD 100,000. And business interruption does not appear to have been prolonged.

With losses contained, the market is showing no signs of reacting to WannaCry with increased rates or changes to terms and conditions.

While companies took services offline to stem the spread of the attack or to carry out updates, business interruption was not material. For example, WannaCry caused Renault-Nissan to temporarily shut down systems at five plants, but the motor manufacturer was quickly able to make up for lost production.

But companies should consider how their insurance policies would react to cyber incident like WannaCry. For example, will business interruption triggered under existing policies cover a voluntarily shutdown of IT systems.

**MARKET REACTION**

With losses contained, the market is showing no signs of reacting to WannaCry with increased rates or changes to terms and conditions. But the incident may have implications for other lines of insurance. The WannaCry underlined the potential for cyber extensions in the kidnap and ransom insurance market to be widely triggered.
The kidnap and ransom (K&R) market offers ground up cover for cyber extortion and the market is seeing claims from WannaCry. The incident may yet see the K&R market move to exclude business interruption for cyber extortion offered under K&R policies.

WannaCry is also likely to trigger more discussion around patches, and insurers could well ask more questions around updates. The answers may not always be straightforward, but we expect insurers will not take a reactive position and simply decline risks that have exceptions to their patch deployment policy or worse, attempt to reintroduce restrictive “failure to patch” exclusions.

**LIFE AFTER WANNACRY**

Speculation on WannaCry’s origins suggests it may have been an unusual example of a state-sponsored ransomware attack.

In June, UK intelligence services and the National Security Agency (NSA) concluded that the global ransomware attack in May was carried out by individuals linked to North Korea. A number of security firms say there are similarities in the code used by WannaCry and that previously linked the Lazarus attacks.

**PATCH ACT**

Following the WannaCry attack, US legislators have proposed a bill that would increase transparency for cyber security vulnerabilities. The Protecting our Ability To Counter Hacking (PATCH) Act would require government agencies to make zero-day vulnerabilities known to vendors and corporations.

The WannaCry attack spread malware that used a vulnerability in unpatched Microsoft programmes, which was stolen by the NSA and published by a cyber crime group called Shadow Brokers.
SYSTEM FAILURE
What does it mean?
The global IT systems failure at airline British Airways (BA) has once again highlighted the potential for catastrophic IT system failure. IT systems fail for a host of reasons. Hardware or software glitches, a cyber attack, human error, power surges, physical perils like a fire or a flood and botched upgrades are all potential causes.

BA is by no means the first large company to suffer a catastrophic IT system failure. Last year saw a number of airline IT outages, including those at Delta Air Lines and Southwest Airlines. In 2014, the New York Stock Exchange ceased trading for four hours after reporting a technical glitch. Human error during a routine software upgrade left millions of RBS banking customers without access to their accounts in 2012.

What could this mean for your company?
Companies are becoming increasingly dependent on IT systems - to manage supply chains, communicate with customers and trade - and are therefore exposed to the risk of significant disruption from IT system failures.

Cyber insurance has evolved over recent years and broad forms of system failure coverage are now available. However it is important to examine wordings as significant differences exist between policies.

Cyber insurance can cover business interruption losses from a wide range of systems failures, but will not generally cover outages caused by power supply or telecommunications failures. Depending on the policy, other exclusions may also apply, such as the failure of new software roll-outs or upgrades.

System failure cover typically falls into one of two camps: all risks or named perils. All risks provides the broadest cover, but the market is more limited in terms of insurer options and capacity, and the pricing is frequently higher. Underwriters are also likely to require more information from insureds.

For companies that require system failure it is critical to be aware of the type and scope of cover under their cyber insurance policies. It is also important to work with a specialist broker to understand the implications of wordings.

The evolution of cyber crime – ransomware as a service
By Jason Rebholz, Vice President of The Crypsis Group, a member of JLT’s Cyber Risk Consortium.

The evolution of ransomware has brought new and innovative approaches for cyber criminals to find profit at the expense of their victims. The barrier of entry for these cyber criminals is extremely low, allowing even the most unskilled threat actors to gain access into an environment and infect systems with ransomware. Over the last year, The Crypsis Group has observed cyber criminals establishing Ransomware as a Service (“RaaS”) “businesses” to accommodate other evil-doers looking to enter the ransomware market.

These businesses focus solely on two core issues: i) providing ransomware binaries that will encrypt files and ii) facilitating the delivery of ransomware to unsuspecting victims. For cyber criminals looking to enter the ransomware game, these new vendors provide them with a fast track to profiting from malicious activity.

RaaS websites have emerged recently to fill the gap for cyber criminals looking for ransomware binaries. Historically, cyber criminals had to purchase ransomware up front or they had to write their own programs. RaaS removes that burden from cyber criminals by providing a service where malware authors write and update ransomware binaries that can be used to infect victim systems. The RaaS vendor acts as a development team, testing and ensuring that major anti-virus
programs will not detect it, freeing other cyber criminals to focus on infecting systems. The RaaS service provider often provides free copies of the ransomware binary to anyone who signs up via their web page. The RaaS vendors profit when victims pay the ransom by skimming a percentage of the profits from the ransom payment. The balance of the payment goes to the cyber-criminal who infected the victim’s system.

The second obstacle for cyber criminals to overcome is delivering the ransomware payload to victims. As one may guess, there are services for that as well. One such service hacks victim organisations by guessing common user names and passwords to systems and brute forcing access. After securing access by creating new user accounts, the cyber criminal sells access to the compromised machine to other cyber criminals.

The ransomware eco-system continues to evolve in ways that are unfavorable to its victims. Given the lucrative nature of the shady business, we can assume that cyber criminals will continue to build businesses around servicing other cyber criminals to make it easier for them to infect victims. For organisations, they must continue to work to mitigate the impacts of ransomware. The primary defense we recommend to most organisations is maintaining available backups, both online and offline.

---

**Airlines to co-operate on cyber risk and security**

The airline industry is collaborating on cyber security as it faces a growing reliance on technology and IT systems. In this article we interview Pascal Buchner, CIO at International Air Transport Association (IATA).

**Is cyber risk a priority for airlines, if so why?**

Yes, because the airline industry relies on computer systems extensively in their ground and flight operations. Some systems are directly relevant to the safety of aircraft in flight, others are operationally important, and many directly impact the service, reputation and financial health of the industry. There is no question that automation significantly enhances safety and aircraft capabilities while simplifying many routine tasks. But as a result, the number of entry points into systems is increasing steadily.

**What concerns the industry the most?**

The main concerns today are related to financial fraud within the reservation systems and the business continuity of ground systems. Cyber security is not considered a safety issue as impacts are more in terms of financial loss, operation disruptions and reputation of the airline.

The aircraft itself is secure as the critical avionic systems are totally segregated from other embedded systems that might be vulnerable such as the in-flight entertainment system. However, the entire supply chain needs to be addressed to make sure that the integrity of the aircraft is preserved through the maintenance and the operation activities.

We are also concerned by the different communication links from the ground to the aircraft and it will be key to implement basic controls such as authentication and encryption to protect the aircraft against spoofing and jamming. The next generation of air traffic management systems will bring new requirements in terms of risk management that will need to be addressed.

**Do airlines have robust systems for cyber risk?**

Many airlines and airports have robust systems in place to address common
hacking threats, but they haven’t always taken a holistic approach to the IT environment or considered the broader threat to the aviation system.

What is IATA doing in this area?
IATA has developed a three-pillar strategy to understand, define and assess the threats and risk of cyber-attacks, the basis for appropriate regulation and the mechanisms for increased cooperation throughout the industry with the support of governments. Other areas of involvement include the organisation of workshops aimed at raising industry and regulator awareness and ongoing cooperation with member airlines to assess industry needs.

How are airlines responding to the cyber threat?
Airlines cannot respond only individually as they need to be able to perform a global threat assessment. The most profitable airlines have implemented very mature cyber security activities and are sharing already within the Aviation Information Sharing and Analysis Center (A-ISAC). In May, ISAC announced a partnership with IATA and a new tiered membership structure designed to increase accessibility to the organisation’s premier global cyber threat sharing network. A-ISAC and IATA are also to hold a summit in Miami in November 2017 to bring together the best experts from the industry, the academy and the authorities to exchange on continuous cyber security. The continuous cyber security framework aims to build a cyber security roadmap for the aviation industry, including a common, system-wide threat analysis capability and a cross-industry risk management methodology.

What is being done to increase international co-operation?
In December 2014, IATA, the International Civil Aviation Organisation (ICAO), Airports Council International (ACI), the Civil Air Navigation Services Organisation (CANSO), and the International Coordinating Council of Aerospace Industry Associations (ICCAIA), agreed on a common roadmap to align their respective actions on cyber threats. A high-level coordination mechanism has been established through the Industry High Level Working Group (IHLG) which concentrates on the delivery and the promotion of the industry position on cyber security.

In co-operation with other IHLG participants, a proposed declaration on cyber security has been developed and adopted by the 39th ICAO Assembly. The declaration calls upon States to define and align cyber security responsibilities within respective governments and adopt a flexible, outcome-focused approach.

Does IATA provide any practical guidance?
In 2015, IATA published the second edition of the Aviation Cyber Security Toolkit to assist airlines in raising awareness and understanding and better defining the cyber risks to their organisations. The toolkit includes a situational assessment of cyber security in the industry, a framework for assessing risk and guidance material for setting up a cyber security management system.

What role might insurance play?
Cyber security insurance might be important to cover the response activities to recover from a cyber-attack, if the premium is affordable without too many exclusions. The continuous cyber security could be one framework helping airlines and insurers to find an agreement on mitigating the risk, so it can be insured.
JLT Specialty Limited provides insurance broking, risk management and claims consulting services to large and international companies. Our success comes from focusing on sectors where we know we can make the greatest difference – using insight, intelligence and imagination to provide expert advice and robust – often unique – solutions. We build partner teams to work side-by-side with you, our network and the market to deliver responses which are carefully considered from all angles.

Our cyber, content and new technology risks team delivers bespoke risk management and insurance solutions to meet the needs of clients from a variety of industries. The team combines experience and talent with a track record of delivering successful results and tangible value for our clients.

CONTACTS
Sarah Stephens
Head of Cyber, Content and New Technology Risks, JLT Specialty
cyber@jltgroup.com

Jack Lyons
Partner, JLT Specialty
cyber@jltgroup.com

This publication is for the benefit of clients and prospective clients of JLT Specialty Limited. It is not legal advice and is intended only to highlight general issues relating to its subject matter but does not necessarily deal with every aspect of the topic. If you intend to take any action or make any decision on the basis of the content of this newsletter, you should first seek specific professional advice.

JLT Specialty Limited
The St Botolph Building
138 Houndsditch
London EC3A 7AW
www.jltspecialty.com

© June 2017 274792