Watching their profits fly away

IT outages and cyber attacks are costing the aviation industry dearly. It’s time to consider a new type of cover.

No holiday season is complete without pictures of passengers stranded at major airports, and this last summer was no exception. The cause is frequently problems with IT systems.

The Delta Air Lines delays in August are just the latest example. A power cut that crashed the airline’s check-in systems, passenger advisory screens, website and smartphone apps resulted in delays across the US, Japan, Italy and the UK.

Forcing the company to cancel 2,300 flights, and forcing the CEO to issue a video apology, the outage is expected to cost Delta USD150 million.

It is far from alone. In July, a router failure at Southwest Airlines resulting in widespread delays and cancellations cost the company at least USD10 million. United suffered a similar problem last summer.

A LONG HAUL

The frequency and severity of these incidents reflects the industry’s critical reliance on technology.

On the one hand, airlines are keenly aware of the data protection and liability risks they face. As customer-facing businesses taking personal information, they have seen the claims suffered by the retail, hospitality, healthcare and financial services sectors.
On the other, cyber incidents can also cause significant interruption to their daily operations resulting in delays, extra expense, lost revenue and unhappy customers, as Delta and the other examples show.

“Last summer, over 1,400 passengers with Poland’s national carrier LOT suffered delays after hackers attacked its systems. The airline’s chief executive doesn’t expect it to be the last.”

On the evidence to date, the most frequent threat is IT infrastructure failure. One reason is that airlines were early adopters of computerised systems and are now grappling with technology cobbled together over decades.

This has been further compounded by mass consolidation within the industry which has left airlines with a swathe of IT assets. For instance, Delta’s current system once belonged to a defunct airline that went bust in 1982.

New risks are also materialising. Last summer, over 1,400 passengers with Poland’s national carrier LOT suffered delays after hackers attacked its systems. The airline’s chief executive doesn’t expect it to be the last.

“This is an industry problem on a much wider scale, and for sure we have to give it more attention,” he told reporters. “I expect it can happen to anyone anytime.”

It’s not just check-in and other ground systems that may be a worry; as with cars (see next page), there have been claims hackers can access flight controls.

TAKING COVER

The extent to which these scenarios are covered by airline operators’ traditional insurance policies is limited.

Cyber policies, by contrast, can cover the full range of risks: policies respond to both malicious attacks and system failures, and to both data protection breaches and business interruptions. That includes the expenses of dealing with the crisis, the recovery, investigations, customer notifications, litigation costs, liabilities and customer compensation. It can also cover loss of profits caused by system outages after the policy waiting period elapses.

As the cyber risks facing aviation companies expand, cyber insurance looks likely to play an increasing role in helping the industry to keep flying high.
New challenges for a connected world

Increased cyber vulnerabilities in cars point the way to wider challenges – and opportunities.

Doubts persist about whether hackers can access flight controls through other on-board systems on planes. For cars, though, the evidence is overwhelming.

Hackers first really demonstrated the vulnerabilities last year, taking control of a variety of systems on a Jeep Cherokee through its internet-connected entertainment system and ultimately shutting it down. The evidence led the manufacturer to recall 1.4 million vehicles and sparked wider questions about the security and vulnerabilities of the Internet of Things (IoT).

This summer, the hackers returned. Having continued their work, those responsible again shared the results with Wired magazine. As it reports, “They’re now able to pull off even more dangerous, unprecedented tricks like causing unintended acceleration and slamming on the car’s brakes or turning the vehicle’s steering wheel at any speed.”

The new attacks can’t be done remotely, and need a laptop directly plugged into the Jeep’s network, but experts say that’s limited comfort. One researcher told the magazine: “There will almost certainly continue to be remote vulnerabilities in the future.”

A three-year study published by security consultants in August, meanwhile, suggests that half of vehicle components have flaws that could allow hackers to control parts of the vehicles’ core functions, such as braking or steering. Close to three quarters (71%) of vulnerabilities were also easy to exploit, it said.

A ROCKY ROAD AHEAD

There are obvious issues here for automobile manufacturers, as well as, perhaps, those managing fleets. There are also questions for insurers. As we looked at in the last issue of our Cyber Decoder, developments such as the IoT and driverless cars are putting cyber questions at the heart of even traditional car insurance.

As Axa’s technical director noted: “The integration of the multiple levels of autonomous technology into the UK motor market has the potential to disrupt not just existing insurance models, but society entirely.”

More widely, the cases put renewed focus on the potential vulnerabilities the IoT brings. This will require work from insurers, insureds and brokers.

For a start, if they’re not already, manufacturers of any type of connected device need to look at their general and product liability policies and ask how they would respond to damage caused by a cyber attack.

“The integration of the multiple levels of autonomous technology into the UK motor market has the potential to disrupt not just existing insurance models, but society entirely.”

It’s tempting to try to cover risks like this solely by continuing to pile more and more coverage into the cyber insurance market, however a more sustainable approach is possible through collaboration across product groups and industry specialties. The best place to obtain coverage for the physical impacts of security failures of connected devices is not always in a policy called “cyber.” A more nuanced and client-centric approach to addressing cyber and technology related risks will support the entire insurance market as the world adapts to this new reality.
Counting the cost: the problem with cyber loss studies

Cyber-crime is a real and growing risk, but assessing its cost is no easy task.

A new report by the European Union Agency for Network and Information Security (ENISA) reviews previous studies on the economic impact of cyber-security incidents on critical information infrastructures.

It reveals that the lack of a standard approach makes it difficult to compare studies (which makes it difficult to assess their reliability) and means many are relevant only in their particular context.

The studies it looked at take a wide range of approaches to estimating cost. They also disagreed on fundamental issues, such as the most affected countries (the US, according to one; Germany, says another). Identifying "common denominators" between the studies was "almost impossible," ENISA notes.

"In terms of conclusions reached among the most notable one is that the measurement of the real impact of incidents in terms of the costs needed for full recovery proved to be quite a challenging task," the report’s authors write.

Or, as one report summarises it: “Your cybercrime cost studies are rubbish.”

WASTE OF TIME?

However, as ENISA’s report makes clear, the effort to quantify losses is an important one despite obvious challenges.

“Determining cost values that are as close as possible to reality is key to determining the real economic impact of incidents on the EU’s economy. Knowing the real impact can help define proper, coherent and cost effective (beneficial) mitigation policies,” it reads.

Lessons can be drawn from previous studies’ findings. There’s broad agreement that finance, telecommunications / technology and energy sectors appear most affected, for example; most common incidents for finance and telecommunications are denial of service attacks and malicious insiders; and the most expensive attacks are insider threats.

Cyber incident data does help businesses better visualize, model, and treat their own cyber risks. That’s why JLT is working with researchers from Stanford Law School to build a comprehensive cyber incident data set, which will allow much more accurate quantification of cyber risk.

However, it’s clear that existing industry, national and global studies need to be carefully taken in their specific context. They have to be just one source of information feeding into your cyber risk assessment. Ultimately, it’s no replacement for working with advisors to develop your own particular cyber risk profile.
US cyber premiums top $1 billion

Cyber insurance take-up continues to drive growth in insurance, as report reveals a broad, strong market.

US cyber insurance premiums passed USD1 billion in 2015, according to a report from ratings agency Fitch. The company's report assesses direct written premiums for cyber coverage at 120 insurers, with almost half (USD483 million) for stand-alone cyber policies, written by 48 insurers. Cyber is the fastest growing insured peril, it confirms.

Moreover, the size of the market is probably even bigger than stated: the difficulty in attributing the premium for cyber coverage where it’s part of a wider commercial policies means it’s hard to calculate, says Fitch.

Its report states: “Identifying the cyber-related premiums and losses within a policy that includes other property and casualty (P&C) coverage is difficult. As such, significant levels of cyber premium exposure are not reported in this supplemental data as companies are unable to isolate cyber premium from other package risk exposures.”

SUSTAINABLE GROWTH

The report is useful in a number of respects.

First, it provides probably the most accurate estimate to date of the size of the US cyber insurance market (without belittling the brilliant work done in the past by Richard Betterley). It's true that this gives us no insight into the London market; Lloyd's of London estimates the global market for cyber in 2015 at USD 2.5 billion. Nevertheless, it provides the best benchmark to date and a baseline from which to measure future development of the market.

It also should alleviate some of the concerns over insurers’ ability to manage the risk. The data presents some difficulties and it comes from only a single year making it hard to evaluate losses and profits: “The ultimate profitability of the P&C industry’s cyber insurance efforts will take some time to assess as the market matures and future cyber-related loss events emerge,” it notes. Nevertheless, the direct loss ratio of 65.2% (the proportion of premiums paid out directly as claims) looks far from unsustainable. Fears that insurers are unable to cover the risk and that a government pool is required, so far, at least, look unfounded.

A new threat landscape for TelCo providers

Cyber security reports by the likes of Kaspersky, PwC and Verizon show the threat landscape is evolving for telecommunication providers. With the world relying on them to keep connected, telco providers operate hugely complex network infrastructures that present a rich landscape for threat actors.

Attacks are increasingly successful. According to PwC, security breaches suffered by telco providers have risen 45% since 2015. The frequency and scale of reported breaches suggests a traditional technology-centric approach to security is no longer working.

One of the primary reasons for this is that telco providers are under attack on two fronts: Their network infrastructure is a key target; while their systems hold valuable personal data. Cyber criminals want to be where the people are, and, today, the people are on their mobile devices.

DEALING WITH THE DANGER

To tackle the threat, providers should start with two areas.

First, the cyber breach data tells us that they continue to suffer from basic cyber hygiene issues: unacknowledged software vulnerabilities (such as SQL injection), system misconfiguration, and common infrastructure vulnerabilities.

Second, they need to tackle the insider threat. Organisations are highly-focused on meeting cyber threats and vulnerabilities with technology, but criminals are using human weaknesses to thwart high-tech defences. People are the wild card for cyber security.

On the one hand, malware tied to spam and phishing continue to cause problems due to poor training or carelessness. On the other, criminals without the skill or investment to breach telcos’ technological defences are getting through perimeters with the help of current or former employees. Cyber criminals have ongoing recruitment programs targeting those willing to sell their access.

Overall, the threat landscape for telco providers is changing faster than organisations can implement technology-based controls. Cyber criminals, however, will always go for the softer target and choose the easiest path to breach defences. Addressing these goes a long way to minimising vulnerabilities. TelCo’s who overlay a strong IT safety culture, robust training and sound cyber security protocol with a tailored insurance product are best positioned to avoid distress in this area.

This article was contributed by JLT Cyber Risk Consortium partner Dynetics. For more information contact tim.layton@dynetics.com
Advanced persistent threats (APT)

What is it?
Advanced persistent threats are the moles in your network. Highly covert and operating over a long period of time, an APT sees an unauthorised person gain access to a network and remain undetected, continuously monitoring and extracting data.

Unlike typical viruses and malware, APTs are sophisticated, intentional and targeted. Rather than picking its targets opportunistically by identifying where there are vulnerabilities, APTs fix on a specific objective at the outset. An array of tools and expertise are then used to overcome security that stands in the way. Usually a team of hackers is involved; an individual would lack the resources.

Why should you care?
While many APTs are focused against governments and the public sector, any business with valuable intellectual property is at risk. The recent attack on the SWIFT payments system, for example, is viewed by some as the result of an APT.

Three things make APTs a particular concern. The first is the duration (persistent). Allowed to remain in the system undetected, the APTs is a continual, invisible drain on an organisation’s effectiveness or profitability.

Second, they are difficult to defend against due to the covert nature of the attack and expertise usually involved. State actors – with the considerable resources they bring – have been blamed for many of the APTs seen.

Finally, related to this, they are unavoidable. Most hackers’ preference for a soft target, along with good training and security can insulate organisations from many threats. With APTs, the value of the intellectual property or data means they are unlikely to be put off.

That doesn’t mean good practice won’t help mitigate the risk. But if yours is a business that might attract APTs, something more will also be needed.
RECENT VULNERABILITIES AND THREATS

August 17: Kaspersky Lab’s global research and analysis team identified a series of targeted attacks designed to steal sensitive corporate financial data, primarily from industrial and engineering organisations in the Middle East. Nicknamed “Operation Ghoul” by researchers, the campaign saw attacks against 130 organisations in 30 countries, with 70% against companies in the United Arab Emirates. European businesses, particularly in Spain, have also been targeted.

August 3: Researchers uncovered several critical vulnerabilities in Cisco’s small business RV series routers. According to advisories published by Cisco, the RV110W, RV130W and RV215W routers include a default account attackers allowing to gain root access to the device. The default account should normally be read-only and not have root privileges. The networking giant has released patches for some of the security holes.

August 3: The world’s largest bitcoin-dollar exchange was robbed. Criminals stole 120,000 bitcoins, worth up to USD 72 million, from Hong Kong’s Bitfinex bitcoin exchange. Zane Tackett, Director of Community & Product Development for Bitfinex, told Reuters on Wednesday that it had reported the theft to law enforcement and was cooperating with top blockchain analytic companies to track the stolen coins. It hadn’t yet decided how to address customer losses.

July 26: Wireless keyboards from a range of manufacturers have been discovered to send keystrokes in ways that allow others to “eavesdrop” on them from up to 250 feet away, according to researchers. The “KeySniffer” vulnerability could let attackers steal passwords, credit card numbers, security question answers or anything else typed on the keyboards. The vulnerability was found in a range of devices from eight different manufacturers: Hewlett-Packard, Toshiba, Kensington, Insignia, RadioShack, Anker, General Electric and EagleTec.

Cyber Threat Intelligence

Brought to you in partnership with JLT Cyber Risk Consortium partner CSC

The ransomware risk continues to be pernicious. A recent report by Check Point researchers shows Cerber ransomware impacted about 150,000 victims in 201 countries in July alone. Understanding the ransomware threat and knowing how to deal with it are therefore vital.

PREVENTION AND DETECTION

The most common method of infection is via email or downloaded material from a website. In the past, ransomware has usually been spread using email attachments. While many anti-virus and intrusion prevention systems offer good protection, however, creators of malware are often a step ahead.

There are a number of potential indicators of ransomware:

• An unresponsive system after an attachment is opened
• Increased CPU utilisation with no apparent reason
• Recently accessed files that are no longer available
• A “ransom” banner containing instructions on how to pay to recover your files.

If these are identified, you need to move quickly.

RESPONSE AND MITIGATION

As soon as ransomware is detected, users should immediately disconnect the infected systems from the network and power down as quickly as possible to stop the encryption. They should then clearly mark the system as infected, isolate any media in or around it, and notify the security team.

As ever, though, prevention is better than cure. User education and training to avoid risks and identify potential indicators of ransomware are essential; so, too, are backups for data recovery.

Other good practices include ensuring users are assigned the “least privilege” level of access needed to do their job, and limiting programs that allow compiling and running code on user systems.

Ultimately, if an attack is successful, whether or not to pay the ransom is a business decision each group must make for itself. It’s a cost, however, that most would prefer to avoid and those with a cyber policy certainly will.

As soon as ransomware is detected, users should immediately disconnect the infected systems from the network and power down as quickly as possible to stop the encryption.
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, Technology, and Media Errors & Omissions 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, Technology and Media E&O
JLT Specialty
+44 (0) 20 7558 3548
sarah_stephens@jltgroup.com

Lauren Cisco
Partner, JLT Specialty
+44 (0) 20 7558 3519
lauren_cisco@jltgroup.com

Jack Lyons
Partner, JLT Specialty
+44 (0) 20 7528 4114
jack_lyons@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

© September 2016 272878