CYBER DECODER

FINANCIAL LINES GROUP NEWSLETTER ISSUE 43

WAR CLAUSE
Zurich uses war clause to deny property insurance cyber claim
Page 3

TOP THREAT
Cyber ranked top threat for businesses, alongside the closely related risk of business interruption
Page 5

GDPR NOTICE
UK's ICO serves Canadian data analytics firm first enforcement notice under GDPR
Page 6

ALSO IN THIS ISSUE
Cyber certification 7
Securing USB devices 8
Rootkit 10
Top tweets 11

Shift towards affirmative cover to gain momentum in 2019

As organisations become increasingly dependent on technology, cyber risk has entered the top ranks of the corporate risk agenda. According to the Global Risks Report 2019 from the World Economic Forum (WEF), rising cyber dependency is the second most feared interconnected risk.

Rapidly evolving cyber and technological threats are the most significant potential blind spots for businesses that do not fully appreciate the vulnerability of networked societies, it warned.

Major cyber incidents, coupled with far tougher data protection and privacy laws, have resulted in a gear-change when tackling cyber risk. Over the past year, large clients have increased their understanding of technology related risks, and are now seeking more sophisticated and comprehensive cyber insurance solutions.

We would expect this trend to continue and broaden further into the mid-market in coming years. Despite increased claims, the cyber insurance market has shown remarkable resilience and stability, with only slight hardening on excess layers and for loss affected sectors, like banking and airlines. The vast majority of clients should find the cyber insurance market receptive to their needs, with consistent pricing and a willingness to innovate.

However, the wider insurance market is looking to clarify cyber cover offered under property/casualty policies, a trend that is likely to gather momentum in 2019. This will result in a gradual shift towards affirmative cyber as property/casualty insurers increasingly exclude or explicitly include cover for cyber perils.

Continued on page 2 ▶▶

In the mid-market and below, we are also likely to see a move towards standardisation. Driven in large part by brokers, industry-wide agreements on standard wordings should make life easier for clients and create more certainty of cover.

WATERSHED YEAR

Last year witnessed some of the largest data breaches and IT system outages of all time. It was also the year that finally witnessed the implementation of the General Data Protection Regulation (GDPR), amid growing concern for privacy and the use of personal data in political campaigns.

At the start of 2018, experts warned of further large data breaches, a prediction that soon became true. The compromise of data belonging to 500 million customers at the Marriott Hotel group was one of several mega data breaches last year, and one of the largest data breaches of all time. In April, Facebook revealed some 87 million users may have been affected by a breach, while fitness app provider Under Armour said some 150 million records had been compromised. At the start of 2019, there is no reason to believe that further large data breaches will not continue.

Data breaches involving personal data, similar to the British Airways breach in August 2018, are increasingly likely to be covered by more stringent data protection regulation. The GDPR introduced new rights for consumers and requirements for companies in May 2018, as well as the prospect of greatly increased fines. While still early days for GDPR enforcement, data breach notifications are reportedly significantly higher under the new regime.

Data breach class actions have also emerged as a potential source of sizable liability in Europe. A number of data breaches under the GDPR, including British Airways, have sparked group actions, while a landmark class action against UK retailer Morrisons in 2018 showed that organisations may face large claims for damages, even when appropriate safeguards are in place to protect personal data.

The market will carefully watch the development of regulatory enforcement under the GDPR and data breach litigation in 2019. Combined, regulatory and legal liability are likely to become a significant driver for cyber liability and insurance buying.

BUSINESS INTERRUPTION

IT outages also came to the fore in 2018. The IT systems outage at UK bank TSB – caused by a failed platform migration - was one of the most high profile examples of systems failure in 2018. It cost the company GBP 176 million, and resulted in the departure of its CEO. An outage at payment processing company Visa in June affected bank customers and retailers across Europe, while customers of Telefónica and other companies were left without data services in December after a software glitch at Ericsson disabled its network.

2018 also saw experts predict further ransomware and malware attacks. While 2018 escaped the scale of a global malware outbreak seen in the 2017 WannaCry and NotPetya attacks, last year continued to see companies report disruption from such attacks. Taiwan Semiconductor Manufacturing Company—the world's largest maker of semiconductors and processors—was forced to shut down several of its plants in August 2018 after it was infected by a variant of the WannaCry virus.

At the start of 2018, cyber security analysts also predicted an uptick in cyber conflict and warfare. Political tensions were heightened in 2018, with Russia, China and other states blamed for a number of cyber attacks and detected intrusions. Nation state groups have been accused of stealing trade secrets from businesses and universities, as well as probing critical infrastructure, possibly with the intention of causing property damage or business interruption.

Cyber war will no doubt remain a feature of 2019, as governments look to create definitions and rules for cyber conflicts, as well as promote cyber resilience through cyber security regulations and guidance. Cyber warfare is likely to become a talking point among insurers in 2019, as carriers focus on the effectiveness of war and terrorism exclusions, and can possibly spark a conversation about the need for a market or government-backed solution. ■

Zurich uses war clause to deny property insurance cyber claim

A coverage dispute between Zurich Insurance and Mondelez International, following 2017's NotPetya, is likely to prove to be an important test for the application of war exclusions by property insurers for incidents of suspected cyber warfare. The move also gives further credence to the need for affirmative cyber cover.

On 10 October 2018, food manufacturer Mondelez filed a lawsuit in Cook County Circuit Court of Illinois against Zurich North America after the insurer denied a claim made under the company's all-risk property insurance policy. Mondelez, which owns the Cadbury, Toblerone and Oreo food brands, says the incident damaged some 1,700 servers and 24,000 laptops, halting production and disrupting sales.

According to the court filing, Mondelez says it suffered "property damage, commercial supply and distribution disruptions, unfulfilled customer orders, reduced margins and other covered losses aggregating well in excess of USD 100 million".

The complaint says the property insurance policy underwritten by Zurich covers "physical loss or damage to electronic data, programs, or software" caused by "the malicious introduction of a machine code or instruction". The policy also extends cover to include business interruption and additional expenses "resulting from the failure of the insured's electronic data processing equipment or media to operate resulting from malicious cyber damage".

Initially, Zurich offered a USD 10 million interim payment. However, it is said to have later withdrawn the offer after it reclassified the NotPetya attack from a criminal act to an act of war. Zurich then denied cover under the property policy in June 2018, evoking an exclusion in the policy covering any "hostile or warlike action in time of peace or war" carried out by a government, military force or a government "agent or authority". In the case of NotPetya, the UK, US, Canada and Australia have all blamed Russia for the attack, although Russia has denied any involvement.

Zurich now has to prove in court that the exclusion applies. However, the attribution of cyber attacks can be highly problematic.

TESTING TIMES

The dispute between Zurich and Mondelez raises important questions for both buyers and insurers, about how they can approach the problem of cyber conflict.

Recent years have witnessed an apparent rise in the threat posed by nation states. For example, cyber security experts suspect Chinese state hackers were behind the recent cyber attack at Marriott Hotel group, which compromised the data of some 500 million customers. Nation states are thought to be behind numerous cyber attacks aimed at obtaining trade secrets, personal data or funds, as well as intending to cause physical damage and disruption.

War and terrorism exclusions are standard in both property and cyber policies, although wordings in specialist cyber policies are drafted with cyber loss events in mind. For example, war clauses in a property policy are intended to exclude physical damage from conventional acts of war, and not business interruption from a cyber attack.

The effectiveness of war and terrorism exclusions in the context of cyber attacks is untested. In its filing, Mondelez says the application of a war exclusion to deny coverage for a malicious cyber incident – or for anything other than a conventional armed conflict or hostility - is unprecedented. It is also challenging, as determining culpability for a cyber attack is fraught with difficulty.

Lines between nation states, hackers, cyber criminals and terrorist groups are blurred. The tools and exploits developed by nation states can also trickle down to hackers – WannaCry, for example, was based on the Eternal Blue exploit developed by the US National Security Agency, and leaked by the Shadow Brokers hacker group. Even where a cyber attack can be traced back to a nation state (the US blames WannaCry on North Korea), establishing whether an incident was an act of war or something else - such as espionage or state-sponsored theft - is another story.

The Mondelez dispute also highlights diverging views on cyber risk between the property and cyber insurance markets. The latter has shown no sign of evoking war and terrorism exclusions for malicious cyber incidents – in fact the market has paid out on a number of NotPetya claims, sometimes up to full policy limits. However, the property insurance market, which in all likelihood never intended to cover losses from events like NotPetya, has been more circumspect.

SILENT CYBER

Malware attacks like NotPetya and coverage disputes like the one between Mondelez and Zurich reinforce the need to purchase standalone cyber insurance with appropriate limits.

Mondelez was not the only company to suffer losses from the NotPetya attack. Shipping group Maersk, logistics company FedEx, US pharma group Merck, French construction materials company Saint-Gobain and UK-based consumer goods group Reckitt Benckiser all disclosed losses as a result of the attack. Maersk and FedEx reported losses of around USD 300 million each.

Claims analytics firm PCS says insurers face claims amounting to USD 3.3 billion for the NotPetya attack, but 90% are for non-affirmative cover. Merck, for example, is looking to claim USD 2 billion from its insurers, of which USD 250 million has been paid by the firm's affirmative cyber insurance policy. The remaining USD 1.75 billion is being claimed under non-affirmative cover.

The NotPetya attack helped bring non-affirmative, or 'silent cyber' cover, into sharp focus. However, property/casualty insurers are also under pressure from regulators to clarify cyber cover under traditional policies. The UK's Prudential Regulatory Authority issued a supervisory statement in July 2017 calling for UK insurers to take steps to identify, quantify and manage cyber insurance underwriting risk. A number of international insurers, including Allianz and AIG, are also moving towards affirmative cover in their commercial property/casualty offerings.

PRECEDENT

The dispute between Mondelez and Zurich could set an important precedent, assuming it is not settled out of court. Should Zurich be able to prove that war exclusions are effective in denying claims arising from a state sponsored cyber attack, it would most likely trigger changes to policy wordings and coverage.

The view taken by the reinsurance market could have implications for primary cover. While cyber underwriters would understand the need to provide cover for alleged state sponsored cyber incidents attacks like NotPetya, in the absence of reinsurance support, underwriters may need to apply sub-limits. One solution would be a reinsurance pool for cyber war losses, much like facilities that already exist for terrorism cover in the property market. In the UK, Pool Re recently extended its cover to include cyber property damage resulting from a terrorist attack.

CYBER WAR COVERAGE CHECKLIST

Buyers should consider the following:

- Whether cyber cover under a property policy is affirmative
- The scope of war exclusions and terrorism wordings
- Coverage for replacement of hardware damaged by a cyber incident
- Buying bricking cover for hardware damaged beyond repair. ■

Cyber business interruption ranked as top risk

Cyber is now a top threat for business, ranked alongside the closely related risk of business interruption, according to the Allianz Risk Barometer 2019.

The annual survey, which polls over 2,400 risk professionals from 86 countries, ranked cyber as the top risk for business, tied with business interruption and up from second place in the 2018 report. According to Allianz, cyber risk is now a core concern for global businesses – it was marked as the single biggest risk for the aerospace, media, financial, professional services, technology and telecom sectors.

The insurer says its clients now view cyber on par with major traditional exposures, like natural catastrophes, fire and explosion. Allianz estimates the average insured loss from a cyber incident is now EUR 2 million, more than the EUR 1.5 million average insured loss from a fire/explosion incident, while losses from major events can be in the hundreds of millions or higher.

The report notes cyber crime now costs an estimated USD 600 billion a year, almost three times the 10-year average economic loss from natural catastrophes of USD 208 billion. Cyber incidents are increasingly likely to spark litigation, including securities and consumer class actions, while data breaches or IT outages can generate large third party liabilities as affected customers or shareholders seek to recoup losses from companies.

MOST FEARED

Increasingly, cyber incidents are accompanied by business interruption (BI) losses. In fact, cyber incidents rank as the BI trigger most feared by businesses, while cyber is seen as the second biggest cause of financial loss for businesses after a BI incident, the report found.

BI loss scenarios are becoming ever more diverse and complex in a globally connected economy, according to the report. Significantly, cyber and

BI risks are increasingly interlinked, as ransomware attacks or accidental IT outages often result in disruption of operations and services costing hundreds of millions of dollars.

Given that BI and cyber are driving some of the biggest exposures for businesses in today's networked society, Allianz urges companies to plan for a wide range of disruptive scenarios and triggers. Disruptive risks can be physical or virtual, such as an IT outage, and can occur through malicious and accidental means. They can stem from their own operations, but also from a company's suppliers, customers or IT service providers, the insurer says.

Just weeks before the Allianz report was published, a cyber attack caused major printing and delivery disruptions for a number of US newspapers. The malware attack led to delayed distribution of The Los Angeles Times, Chicago Tribune, Baltimore Sun and other titles belonging to Tribune Publishing that share the same print facility. The company said it first detected the malware on Friday, and had to rely on "workaround systems" several days after the attack.

Insurers have seen a growing number of BI losses triggered by cyber incidents, with industry claims exceeding USD 100 million, according to Allianz. BI losses, for example, were a hallmark of the WannaCry and NotPetya malware attacks in 2017, which disrupted shipping, logistics and manufacturing companies. However, Allianz notes that many incidents are the result of technical glitches or human error, rather than malicious acts. Analysis conducted by the UK's financial services regulator revealed a 138% increase in technology outages over a year, but just 18% of reported incidents were cyber attacks.

Reliance on IT service providers – such as cloud services, online booking platforms and supply chain systems – also brings potential contingent business interruption (CBI) exposures, according to the report. A software glitch at network equipment provider Ericsson disrupted services for millions of mobile phone customers in Europe and Japan in 2018. In 2017, a four hour outage at Amazon's AWS cloud computing division impacted internet services, websites and other businesses. Companies lost approximately USD 150 million as a result, yet longer outages could see losses much closer to a billion dollars, Allianz says. ■

Regulator issues first GDPR enforcement notice

In 2018, the UK's Information Commissioner's Office (ICO) served Canadian data analytics firm Aggregate IQ with an enforcement notice, its first under the EU's General Data Protection Regulation (GDPR), which came into force on 25 May 2018. The enforcement notice was first filed in July 2018, but amended in October after it was appealed.

The notice demonstrates the regulator's willingness to exercise the extra-territorial scope of the new data protection regime. It also shows the UK regulator's willingness to take action where it finds evidence of the misuse of personal data, rather than focusing on data breaches.

DATA MISUSE

The enforcement notice was issued as part of the ICO's investigation into the use of data analytics in political campaigns. In particular, the ICO looked into Aggregate IQ's use of personal data belonging to UK citizens – the Canadian company had worked under contract for a number of political organisations during the EU referendum campaign in 2016. Aggregate IQ is also being investigated in Canada by the federal Office of the Privacy Commissioner and the Office of the Information and Privacy Commissioner of British Columbia.

When contacted by the ICO in May 2018, Aggregate IQ confirmed it still held personal data on UK citizens. It was said to be stored on a code repository, although the data had been subject to unauthorised access by a third party.

The ICO concluded that Aggregate IQ failed to comply with Articles 5 and 6 of the GDPR, having processed data in a way that data subjects were not aware of, and for purposes that they would not have expected, and without a lawful basis. It also found the processing of data was incompatible with the purpose the data was originally collected for, and that it failed to comply with Article 14 of the GDPR, which requires the data controller to provide data subjects with certain information.

When deciding whether to issue an enforcement notice, the Commissioner was required to consider whether Aggregate IQ's failings had caused personal damage or distress. It concluded that damage and distress was likely, as the data subjects had been denied the opportunity to understand what data was used and were not able to exercise their various privacy rights.

PRAGMATIC RESPONSE

Following the investigation, the ICO issued an enforcement notice in July requesting that Aggregate IQ erase "any personal data of UK or EU citizens obtained from UK political organisations or otherwise for the purposes of data analytics, political campaigning or any other advertising purposes."

The notice shows the regulator is willing to enforce the GDPR with little leeway in compliance. Interestingly, the ICO gave Aggregate IQ just 30 days to comply with the notice, a relatively short period to identify the data (that could also be held by third parties), and take the required action. The notice adds failure to comply could result in a penalty notice and a fine of up to EUR 20 million, or 4% of total worldwide turnover.

However, the ICO's actions also suggest that the regulator is taking a pragmatic approach to enforcement. Aggregate IQ initially denied any wrongdoing and said it would challenge the enforcement notice. It appears that the ICO listened and clarified its notice, amending the notice to require the Canadian company to only delete UK personal data held on its servers as of May 2018. Aggregate IQ withdrew its appeal and agreed to delete the data as soon as Canadian regulators allowed it to do so. ■

EU cyber certification moves a step closer

EU institutions have reached agreement on new cyber security legislation, which will give new powers to the region's cyber security regulator and establish a cyber security certification framework.

In December, the European Parliament, the Council and the European Commission reached political agreement on the Cyber Security Act. Proposed in 2017 as part of a wide-ranging set of measures to deal with cyber attacks, the Act will strengthen the powers of the EU Agency for Network and Information and Security (ENISA), transforming it into a permanent EU Cyber Security Agency.

Going forward, ENISA will enjoy increased resources and a permanent mandate to improve cyber security in Europe. The organisation will continue to assist EU member states in responding to major cyber attacks, but with a greater role in cooperation and coordination at an EU level. In its new responsibility, ENISA will develop an EU crisis response and act as an independent centre of expertise, promoting cyber security awareness and assisting EU institutions and member states in policy development and implementation.

IOT REGIME

Significantly, the Act also establishes a single pan-EU framework for cyber security certification, aimed at improving cyber security for online services and consumer devices. The ground-breaking legislation is the first EU law seeking to enhance the security of so-called Internet of Things (IoT) devices, including consumer products and those used in critical infrastructure.

The cyber security certification framework will require developers and manufacturers of IoT devices to adopt security by design, incorporating cyber security features in the early stages of their design. National cyber security certification authorities will be established to issue a common cyber security certificate for a range of products and services, from connected toys and smart wearables to industrial automation control systems, smart energy grids and banking systems.

Certification, which is voluntary, is intended to help consumers choose between products and build trust through improved cyber security. There will be three levels of the certification process; basic, substantial and high. At the basic level, suppliers are allowed to self-certify, while certification at higher levels will involve a third party. The certificate will be valid throughout the EU.

Now that the Cyber Security Act has gained political agreement, the text of the Act will need to be formally adopted, first by Parliament and then by the Council. Following adoption, the regulation will be published in the EU's Official Journal. It will enter into force 20 days after publication, although member states will have two years to implement the legislation and establish a cyber security certification regime. ■

Visibility and granular control: the secret to securing USB devices in the workplace

Special feature from Charles Groves, Global Director of Business Development at CrowdStrike, JLT's Cyber Consortium Partner.

Social engineering continues to be exploited by hackers and feared by security teams. Due to attackers' subtlety and users' natural curiosity, hackers succeed daily in baiting users to click on a link or answer a phishing email.

Baiting is a highly successful technique that relies on an organisation's weakest security link: the end user. This type of attack is so effective that it is used in over half of all successful breach attempts today.

"LOST" AND FOUND: THE USB DROP ATTACK

A favorite variant of baiting is the "USB" drop attack, which involves tricking a user into physically picking up a malware-loaded USB device and plugging it into an endpoint. This attack is particularly devastating because removable media can breach any network, from a university to the international space station.

The malicious reprogramming and dropping of a USB device can be accomplished in three ways:

- Malicious Code: Attackers insert malicious code onto a USB and this code is auto-executed when a USB device is plugged in, or when a user clicks on a disguised malicious file once the device is inserted. The code can install anything from a worm to a remote access trojan, immediately infecting an endpoint and giving the attacker a beachhead for downloading additional malware.
- Watering Holes: In addition to the social engineering methods used in the initial drop attack, opening a malicious HTML file on an infected USB can lead the victim to a watering hole site where they unknowingly enter personally identifiable information (PII).
- Human Interface Device Spoofing: In a more sophisticated attack, the device itself is designed to look like a USB drive, but it behaves like an entirely different device, such as a USB keyboard, which can then be used to inject keystrokes that give an attacker remote access to an endpoint.

USB drop attacks succeed almost 50% of the time

A recent study showed that a USB drop attack succeeds almost 50 per cent of the time — and gets past even security-conscious users. The same study showed that 68 per cent of those who knowingly picked up a dropped USB failed to scan the device for malware — they simply plugged it in and accessed the device's content.

THE STRUGGLE CONTINUES

Security teams are faced with a dilemma: how to safely enable USB devices, while reducing the risks they pose. The traditional response has been to either ban all USB devices, or manage them with a device control solution that determines which devices can access an endpoint. Unfortunately, these solutions come up short. USB-related breaches have increased 8 per cent year over year and now account for almost one-third of all breaches.

Security teams have mainly relied on two types of device control solutions:

- **Standalone:** Monolithic solutions offer strict control over USB devices, down to a single drive. However, because they are not integrated with other elements of security, they require additional time and effort to install and manage, and they lack the visibility and context required to verify that device control policies are adequate. To gain visibility into which devices are used in their environments, security teams must deploy additional security tools such as endpoint detection and response (EDR) solutions.
- **Endpoint Suites:** Endpoint security vendors have typically developed and marketed "integrated" device control solutions as part of their endpoint security suites, but their solutions are often not truly integrated. These suites generally require a separate management console and additional agents (and a larger system footprint), and they offer limited device visibility. As a result, security teams have no context or understanding of the devices in their environment, and the solutions themselves consume valuable resources, especially during a USB device-related security incident.

> USB-related breaches have increased 8% year over year and now account for almost one-third of all breaches

Neither solution provides immediate visibility into which devices are in use and where, leaving security teams lacking the necessary knowledge to enforce and manage accurate USB device control policies. As a result, social engineers are thrilled because it leaves the door wide open for opportunistic baiting attacks.

SHUT THE DOOR ON USB DROP ATTACKS

It is imperative that you deploy a solution that can reduce the risk of baiting via USB drop attacks by providing visibility and granular control over USB devices. Most standalone endpoint suite offerings are simply not enough to fully understand and see which devices are in use and where. Throughout their environment, we recommend deploying an endpoint solution with top tier EDR that specialises in the capabilities included.

The core capabilities you should look for include:

- **Visibility:** The ability to see everything in the environment in order to make informed security decisions.
- **Granular control:** Visibility prompts action — the ability to define policies and enforce them, both online and off, down to the specific device.
- **Cloud-native architecture:** A cloud-based solution will help security teams identify all relevant USB device information in one place, enabling swift, effective action.

Armed with these capabilities, security teams can effectively address USB device risks, including the dreaded USB drop attack.

Learn more about CrowdStrike Device Control ■

BUZZWORD OF THE MONTH

ROOTKIT

What does it mean?

Rootkits are a particularly pernicious family of malware. They are considered one of the most serious types of malware, as they give hackers high-level access to computers and networks, enabling them to steal data, spy or control systems remotely, while deliberately hiding their presence.

The rootkit's purpose is to gain "root" access to a computer. By logging in as the root user, an attacker is free to perform almost any operation, undetected. The "kit" refers to software files that effectively implement the attack.

There are different types of rootkits, but generally speaking they target a computer's core operating system, including the virtual machine monitor, the kernel, or even firmware. Because they operate at the same level as the operating system, a rootkit will typically give unrestricted access.

Rootkits are typically installed by exploiting system vulnerabilities or security breaches. They can also be introduced through a Trojan, hidden inside file attachments distributed via email or downloaded from a website. Once installed, the rootkit gives an attacker backdoor access, enabling them to steal data, inject malware or change system configurations.

Why does it matter?

A rootkit is usually difficult to detect because it can deactivate anti-malware software, as well as hide traces of unauthorised access by modifying drivers or kernel modules. Once detected, rootkits are hard to remove - the only option may be to completely rebuild the compromised system.

Most operating systems and programmes seek to prevent unauthorised access via rootkits so it should be difficult to use a rootkit to gain access to modern systems. However, security researchers recently discovered the first known instance of a rootkit that targets the Windows Unified Extensible Firmware Interface (UEFI) boot system.

Research firm ESET says the rootkit, known as Lojax, is being used by Russian hackers Fancy Bear to carry out cyber attacks. It is typically delivered via spear phishing emails. When opened, it runs code that hijacks a vulnerable driver, installing the rootkit in flash memory.

Lojax uses malware tools that can read and overwrite parts of the UEFI firmware's flash memory. The malware embeds itself within the motherboard firmware of infected computers, enabling hackers to spy on the user and evade detection by the operating system or any antivirus tools. According to ESET, Lojax is capable of surviving the re-installation of the Windows operating system or even hard drive replacement.

Interestingly, the developers of Lojax borrowed code from legitimate commercial software. Lojax is a modified version of Absolute Software's Lojack anti-theft software (also known as Computrace), which helps owners locate stolen laptops. ■

JLT 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 that are carefully considered from all angles.

Our Cyber/Technology E&O 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 E&O,
JLT Specialty
cyber@jltgroup.com

Top Tweets

Denmark warns of cyber risk to shipping sector

Philippine financial service provider reveals data breach

US Senator Rubio introduces federal privacy bill

Neiman Marcus settles data breach litigation for USD1.5m

ICO gives advice on non-deal Brexit privacy issues

Weak password security leads to German data breach