CYBER DECODER

FINANCIAL LINES GROUP NEWSLETTER ISSUE 23

WannaCry won't be the last global attack

The global ransomware event, called WCry, WannaCry or WannaCrypt, is a wake-up call for governments and business alike, but it is unlikely to be the last large scale cyber attack.

On May 12, the first news of the attack broke when hospitals and doctors in the UK reported being locked out of files, causing some to cancel operations and close accident and emergency departments. However, it soon became evident that the attack was global, affecting a wide range of industries and public sector organisations.

The ransomware caused widespread disruption, from petrol stations in China, to car manufacturing plants in Europe, rail operators in Germany, telecoms companies in Spain, electronics firms in Japan, and cancer hospitals in Indonesia.

Kaspersky Lab counted 45,000 attacks by WannaCry, which targets a vulnerability in unpatched and older versions of Windows, in 74 countries in just the first day. It is now thought to have infected more than 300,000 computers in 150 countries.

UNPRECEDENTED

The scale of the attack and the rapid spread of the ransomware was "unprecedented" according to Europol. Cyber security firm Symantec said that it had blocked some 22 million attempted WannaCry ransomware attacks globally, making the attack the largest of its kind ever.

While unprecedented, the WannaCry attack was, however, not unexpected, and can be seen as part of the evolving global cyber threat landscape, which has seen a broadening of attack methods and targets in recent years.

The global ransomware attack underscores the potentially widespread impact of a single cyber vulnerability, as well as the threat of a catastrophic or systemic cyber attack.

Continued on page 2 ▶▶

According to catastrophe modelling firm RMS, the WannaCry attack was arguably the first ever cyber-catastrophe, clearly demonstrating the systemic nature of cyber risk.

But there are many other scenarios that would cause widespread disruption and economic damage. The Cambridge Centre for Risk Studies (CCRS) ran a scenario stress test that envisages malicious interference with updates to a popular brand of data base software. The total predicted losses to global GDP output over a five-year period ranged from USD 4.5 trillion to USD 15 trillion.

Other potential catastrophic cyber scenarios include an attack against a major internet infrastructure service provider, cloud service provider or a key payment processing company. In one scenario developed by CCRS and Lloyd's, a cyber attack on the US electric grid was estimated to cause USD 1 trillion in economic damage and USD 70 billion in insurance claims.

"Kaspersky Lab counted 45,000 attacks by WannaCry, which targets a vulnerability in unpatched and older versions of Windows"

ESCALATION

Security experts have also warned that the WannaCry attack may not yet be over. Cyber criminals may yet adapt the malware or use the vulnerability in new attacks.

The ransomware uses a vulnerability called Eternal Blue, which was stolen from the USA National Security Agency (NSA) by a cyber crime group known as the Shadow Brokers. That group has threatened to release other vulnerabilities from the NSA on a regular basis.

Cyber security firms have already identified another attack using vulnerabilities released by Shadow Brokers. Cryptocurrency miner Adylkuzz also uses Eternal Blue and is potentially larger than the WannaCry attack, although so far less disruptive.

INSURANCE RESPONSE

Cyber insurance policies will respond to ransomware attacks, and depending on policy wordings will pay ransoms, as well as the cost of the breach response, data loss and business interruption. However, many cyber policies require companies to maintain regular updates.

It is early days to count the cost of the WannaCry attack, and the true cost will probably never be known. And while insurance claims are not expected to be catastrophic, the attack will be seen as a test for this relatively young market.

DRIVING DEMAND

The impact on the insurance industry is also likely to be limited by the global nature of the attack. Cyber insurance up-take is highest in the US, which accounts for as much of 90% of policies.

Most businesses outside the US do not yet purchase cyber insurance, and Europe has been slow to catch on. But this is changing. Tougher data protection laws, such as the EU's General Data Protection Regulation and Australia's mandatory breach notification laws, are expected to drive demand.

WannaCry is also likely to raise awareness and drive increased demand for cyber insurance outside the US, and not just from companies holding large amounts of personal data.

WannaCry showed just how vulnerable all companies are to a wide spread cyber event. The attack saw manufacturers in Europe shut down production lines as they sought to fight off the attack, while a coal port in New Zealand temporarily closed to upgrade its systems.

LESSONS

WannaCry is a salient reminder of the consequences of not taking cyber security seriously. Despite the prevalence of ransomware, many organisations still rely on out-of-date security solutions and aren't investing in security precautions, according to Verizon.

The chief of Europol, Rob Wainwright, noted that companies with robust cyber security, such as banks, appear to have been largely unaffected. He said that other sectors, such as healthcare, should "sit up and take notice" and follow the example of the banking sector, which has learned from painful experiences how costly cyber incidents can be.

Yet saying that companies should "just patch" and avoid this sort of incident is perhaps overly simplistic. There are a myriad of reasons, particularly in industries reliant on legacy systems and internally developed software, in which simply applying a patch isn't feasible. However this underlines the importance of taking mitigating steps when a patch can't be applied, for example in this case disabling the feature where the vulnerability lies. As cyber criminals become more sophisticated, organisations must protect themselves against threats and update their systems.

WANNACRY?

WannaCry (also known as WannaCrypt) is a form of malware that infects a computer and then encrypts critical data, demanding a ransom payment for its release.

Ransomware is a well-known and growing form of cyber crime – according to Verizon, ransomware attacks increased 50% last year. However, WannaCry has added another dimension.

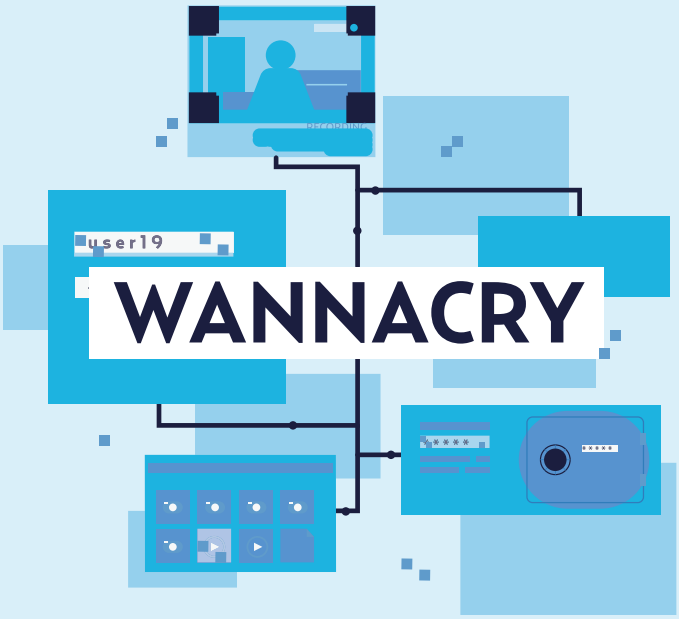
Ransomware threats do not usually spread rapidly. They typically involve phishing or social engineering, as users are required to click on a link in an email or on a website to download a malicious file. But WannaCry uses a vulnerability in Microsoft to infect a computer or network without the user doing anything wrong.

According to Microsoft, WannaCry uses a Windows vulnerability called Eternal Blue to infect computers and execute the ransomware. The exploit code targets unpatched Windows 7 and Windows Server 2008, or earlier operating systems.

This exploit enabled WannaCry to spread rapidly, infecting entire networks. Once one computer is infected, WannaCry scans the local network looking for other vulnerable computers to infect, much like a computer worm.

Microsoft issued a patch for Eternal Blue on March 14 2017, with additional security updates issued for older operating systems since the attack. While the patch protected newer Windows systems and computers using Windows Update, many computers remained unpatched globally, according to Microsoft.

Microsoft advises installing security update MS17-010 as soon as possible, although it also offers possible workarounds to reduce the attack surface.



Airlines cyber exposures

With its high dependency on technology, the aviation industry faces a broader spread of cyber exposures than most other sectors. From business interruption and privacy liabilities, to fears over the potential threat to airline safety, cyber risk cuts across almost all parts of the airline industry.

PRIVACY AND SECURITY

The majority of our aviation clients have shown most interest in protecting the data and liability elements of cyber risk, primarily around personal identifiable consumer data.

Last year, hackers released confidential data on 400,000 members of Vietnam Airlines' frequent fliers club. This followed a 2015 cyber attack that saw British Airways Executive Club accounts compromised and the 2014 attack against Japan Airlines, where hackers stole the details of up to 750,000 customers.

Our analysis shows that the number of reported aviation breach incidents doubled between 2008-2011 and 2012-2015. On average 78,000 records were compromised per airline breach. The majority (58%) of airline data breach incidents were the result of hacking, while 14% were due to lost or stolen laptops.

Airlines appear to have relatively effective controls in place to prevent data breaches, at least when compared to other sectors. And experience has shown that insurable losses for large data breaches are below USD 400 million, in-line with available cyber insurance capacity of USD 300 million to USD 500 million.

But data breach exposures are likely to rise with the introduction of tougher data protection laws.

In Europe, the General Data Protection Regulation (GDPR) will introduce mandatory breach notification requirements and increased penalties when the new rules come into force in May 2018. Aviation companies headquartered outside the EU will be subject to the GDPR if they collect data on EU citizens.

EMERGING RISKS

However, airline executives are also now confronting a new set of cyber risks. For example, major technological advances in the industry, such as tablet-based electronic flight bags (EFB) and the installation of the in-flight entertainment and Wi-Fi connectivity systems (IFEC), have provided an enlarged environment for threat actors to operate within.

Last year, security researchers showed that IFEC's used by major airlines are vulnerable to hacking, which could enable attackers to alter flight information displays. In 2014, a security researcher revealed he had repeatedly hacked aircraft in-flight entertainment systems, on one occasion briefly taking control of the airliner's engines.

The International Civil Aviation Organization (ICAO) has acknowledged that on-board and ground-based aviation systems are potentially vulnerable to outside cyber-attacks. And in April, the organisation committed to developing a global cyber security framework for the aviation industry and working towards achieving effective cyber resilience for the industry.

BUSINESS INTERRUPTION

As reliance on technology has grown, the airline industry has also been plagued by a series of system outages, which caused major disruption to services and reputational damage.

On Saturday 27th May a major IT failure brought down the networks of British Airways, affecting its major London hubs of Heathrow and Gatwick. To date detailed information has been scant. Alex Cruz BA's Chairman and Chief Executive went on record saying that a power surge "had a catastrophic effect over some communication hardware which eventually affected the messaging across our systems." However numerous data centre designers have come forth suggesting that it is unlikely that a power surge would be able to bring down a data centre, let alone a data centre and its back up. Data centres are built with surge protection technology designed to specifically protect against exactly this incident. They also have an uninterruptible power supply, a UPS, which is in place to condition the power – i.e. smooth out the peaks and flows in current. What can be confirmed is that 1,000 flights were cancelled and 75,000 passengers were affected by the disruption. Analysts forecast that the episode will cost the airline over GBP 100 million.

In July 2016 a faulty router at the Southwest Airlines caused a major system outage, while Delta and United Airlines both suffered disruption in January 2017 after they experienced IT problems. Initial losses for the Southwest loss are between USD 60 million and USD 100 million after 2,300 flights were cancelled over five days.

Many of these key cyber risks can be effectively covered by insurance. For example, we recently launched a dedicated cyber insurance policy for the airline industry. Data and Reliance on Technology (DART) protection for airlines provides cover for the operational impact of a cyber incident impacting an airline, such as an unplanned outage or a security breach. The policy also covers security and privacy liability, data restoration and breach response costs, as well as covering liabilities associated with the GDPR.

The airline industry appreciates that IT fundamentally underpins the success of organisations, and that vulnerable legacy systems are exposed to both malicious and non-malicious cyber incidents. As a result, more and more airlines are protecting their balance sheets through cyber insurance. Approximately half of our airline clients are discussing insurance with 40% currently buying.

Aviation insurance has long been a core specialism of JLT, and our cyber team has placed policies for a number of the world's largest airlines and service providers. ■

AIRLINE CYBER INCIDENTS

Delta Air Lines | 8 August 2016

Flights were grounded for six hours by a global computer system outage, causing large-scale cancellations and stranding hundreds of thousands of passengers. The outage was caused by a power surge disabling Delta's command centre in Atlanta.

Southwest Airlines | 20 July 2016

A router failure caused a system crash, and all back-ups failed, causing flight delays and cancellations nationwide.

United Airlines | 8 July 2015

A failed computer network router disrupted the airline's reservation system leading to 59 cancelled flights and more than 800 delays. Experts suggested that the computer problems originated when United merged its reservation system with that of Continental Airlines in 2010.

Virgin Blue | 26 September 2010

Former airline Virgin Blue used Navitaire's New Skies system for internet booking, reservations, check-in and boarding systems. A USD 10 million upgrade to the system was completed in June 2010 resulting in two system failures in the first three months. A hardware failure and subsequent outage of the system affected around 50,000 passengers and 400 flights.

Vietnam Airlines | 29 July 2016

A website breach by hackers released confidential data including names, dates of birth and addresses of 400,000 members of Vietnam Airlines' frequent flyers club. The hackers gained access to screens displaying Vietnam Airlines' flight information and took over the sound systems, airing political messages regarding China's claims to the South China Sea.

LOT | 21 June 2015

More than 1,400 passengers at Warsaw's Frederic Chopin Airport were grounded due to a cyber-attack. The incident prevented the airline from creating flight plans grounding scheduled flights until the issue was resolved.

British Airways, Avios loyalty scheme | 27 March 2015

Tens of thousands of British Airways Executive Club accounts were hacked into as a result of a third party using information obtained elsewhere on the internet. The attackers redeemed members' Avios reward points.

SMEs cyber security exposed

Despite the rise in both awareness and incidents, many small-to-medium sized enterprises (SMEs) are still not addressing cyber in their risk management strategy.

A survey published in April from the UK Department for Culture, Media & Sport has shown that many SMEs are still not taking basic steps to deal with the threat of a cyber attack, despite an increasing reliance on the digital economy.

The Cyber Security Breaches Survey 2017 of over 1,500 companies, almost all of which were SME firms, found that all are exposed to cyber security risks in some way. It also found that these exposures are rising, with a growing reliance on cloud services and an increase in firms holding personal data electronically.

SME's can suffer significant financial loss from a cyber attack that impacts a critical operating system or that results in the loss of sensitive information. An insurer partner of JLT has handled many cyber claims from SMEs, ranging from a UK retailer that incurred costs of almost GBP 500,000 following a payment card data breach, to a small hotel that spent GBP 15,000 dealing with a ransomware attack.

Despite this growing reliance on digital services, the survey found that a sizable proportion of businesses still do not have basic cyber protections or have not formalised their approaches to cyber security.

> "SMEs can suffer significant financial loss from a cyber attack that impacts a critical operating system or that results in the loss of sensitive information"

For example, only a third have a formal policy that covers cyber security risks, or document these risks in business continuity plans, internal audits or risk registers. Only one in ten have a cyber security incident management plan in place.

SLOW PROGRESS

The survey findings suggest that UK business has yet to make significant progress on improving cyber security, and many lack the resources to protect their business or respond to a cyber attack.

Although 74% of UK businesses say that cyber security is a high priority for their senior management, just 43% have yet to even attempt to identify cyber security risks to their organisation. Only 58% have sought information, advice or guidance on cyber security while only half of the firms surveyed comply with the government's Cyber Essentials scheme.

This is despite the fact that almost half of those surveyed had experienced at least one cyber security breach or attack in the past year. The most common types of breaches were related to staff receiving fraudulent emails (in 72% of cases), followed by viruses, spyware and malware (33% of cases), people impersonating the organisation in

emails or online (27% of cases) and ransomware (17% of cases).

CYBER INSURANCE

The report found that 38% of respondents purchased cyber insurance, although uptake was more prevalent among mid-sized firms. However, the real proportion is probably much lower because many businesses wrongly assume they are covered for breaches under their traditional insurance policies.

The survey also shows there are very disparate levels of awareness around cyber insurance, while smaller businesses tend not to be aware of it at all, the report found.

Smaller companies are more likely to benefit from standalone cyber insurance, as they have limited resource and expertise when it comes to cyber security. Standalone cyber insurance puts SMEs on the front foot, providing automatic outsourcing of incident response, while the process of purchasing cyber insurance gives a sense check of cyber preparedness.

We have put together a cyber insurance facility tailored to the needs of SMEs. Backed by leading insurers, the facility offers broad cover to address key risks faced by SMEs at competitive premiums.

In addition to covering the costs of a breach response, the cover also gives SMEs access to an established panel of cyber security, legal and crisis management consultants. ■

Standalone cover will be key to a robust cyber market

The development of cyber insurance as a standalone product will be crucial if businesses, governments and insurers are to deal with escalating cyber threats, according to a Viewpoint Report from JLT Re and JLT Specialty *Unlocking the Potential of the Cyber Market*.

Organisations' are increasingly calling for innovative and comprehensive insurance products but concerns around cyber exposures potentially buried in traditional policies have so far held back carriers from providing these solutions.

There is considerable concern among insurers for potentially catastrophic and/or systemic cyber events, where one cyber event is capable of triggering multiple claims under different policies at national, or even global levels.

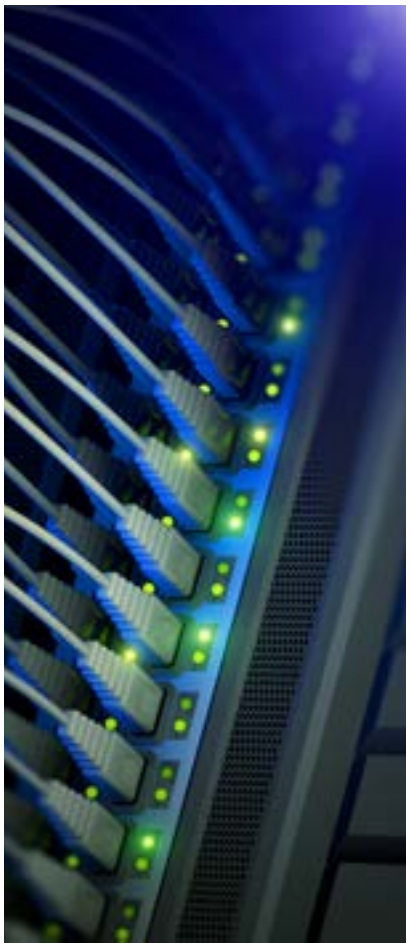
These concerns have been growing as technology has become further embedded in the operations and strategies of organisations and as malicious actors look to exploit the vulnerabilities associated with innovations such as the Internet of Things, cloud computing, automation and connected devices.

Within the insurance market there has been a debate about whether cyber is a peril that falls under the scope of traditional products or a line of coverage in its own right. However, a more resilient cyber insurance market should result from the development of the cyber insurance market with a standalone product at its core, according to the Viewpoint Report.

This shift would benefit insurance buyers in the form of greater certainty, expertise, capacity and stability from the insurance market in what is an increasingly complex and expanding area of risk.

> "Organisations' are increasingly calling for innovative and comprehensive insurance products"

The standalone market is best placed to facilitate innovative and comprehensive solutions that address buyers' changing needs and future cyber risks. It will also be more resilient to future catastrophic cyber losses and better positioned to trade through future systemic losses, concluded the report. ■



Teenage hacker jailed for malware attacks

Last month a UK man was sentenced to two years in prison having been found guilty of launching a string of cyber attacks from his Hertfordshire home.

Adam Mudd, who was 16-years old at the time, was responsible for hundreds of attacks against businesses, educational bodies and local authorities. During the court case it was revealed that he personally carried out 594 distributed denial of service (DDoS) attacks against 181 IP addresses between December 2013 and March 2015.

Mudd also created and sold malware to cyber criminals, which was used to hack websites around the world, including those of Minecraft, Xbox Live and Microsoft.

BEDROOM BREACHES

Operating from his bedroom, Mudd created the Titanium Stresser malware program, which is thought to have been responsible for more than 1.7 million cyber attacks worldwide. The malware had 112,000 registered users and was used to attack 666,000 IP addresses globally, according to the court.

He is thought to have earned GBP 386,000 from selling the program to cyber criminals, although his activities were thought to have cost his victims millions of pounds. Gaming website RuneScape spend GBP 6 million trying to defend itself against the attacks.

He attacked over 70 schools and colleges, including the University of Cambridge, University of Essex and University of East Anglia, as well as local councils.

In sentencing Mudd, who has autism, the judge said that he hoped the sentence would be a real deterrent to others. ■

TITANIUM STRESSER MALWARE:

1.7 million

Cyber attacks worldwide

112,000

Registered users impacted

666,000

IP addresses attacked globally

Buzzword of the month

ARTIFICIAL INTELLIGENCE

What does it mean?

Artificial intelligence (AI) is very much a live topic, with much talk of smart machines and robots driving cars and taking over jobs. But there are also implications for cyber security.

AI is broadly speaking the science of making computers or machines intelligent. The technology, which encompasses areas like machine learning and deep learning, enables machines to carry out tasks that require a degree of intelligence, like understanding natural language, recognising faces in photos or being creative.

The concept of AI has been around since the 1950s – mathematician Alan Turing was an early pioneer, setting out his thoughts in a 1951 paper *The Imitation Game*. Some argue that progress has been slow since, but the pace has picked up and limited forms of AI are now powering machines that can interact with humans as well as learn from their mistakes.

For example, AI is already powering Google's search engine, Amazon's shopping recommendations, and Uber's taxi App. It is even being used to pilot a network of balloons that provide broadband in Peru.

The technology is also behind developments in automation, such as self-driving cars, as well as in data analytics, where it is being used to diagnose cancer in healthcare, fight fraud in banking and understand complex systems like logistics.

Why you should care?

AI is likely to have implications for cyber security and technology risks in the future. On the one hand, an increased use of AI could bring about new risks, while on the other it could become an important tool in the war against cyber crime.

AI is an important driver behind automation. But as more and more tasks and decisions are automated, there is a risk that errors - in data or in an algorithm - could be compounded. In one real case, a pneumonia diagnostic tool wrongly classified asthma sufferers as low risk because it misinterpreted the underlying data.

There are also concerns that AI-enabled hackers could lead to an explosion in complex cyber attacks. According to the Harvard Business Review, AI could result in more sophisticated social engineering, more intelligent computer viruses and an increase in the attack-surface that hackers can target.

AI systems could, in themselves, bring about new cyber security challenges. Data breaches involving intelligent systems are unchartered territory, and could give rise to new privacy risks, revealing new levels of personal information.

The flip side, however, is that AI could play a valuable role in cyber security, helping to detect cyber attacks, to identify system vulnerabilities and create new antivirus software. For example, a version of IBM's AI-enabled system Watson has been trained to spot malicious threats in a company's network.

Keeping count - business interruption in a cyber risk world

In this month's edition Molly McGinnis Stine of Locke Lord, a member of JLT's Cyber Risk Consortium discusses business interruption in a cyber risk world.

Highly publicised recent cyber incidents have raised alarms about business interruption. Business interruption scenarios can affect a single entity, a geographic area, an industry, or a multifaceted combination of all of these or multiples of these. It's not hard to imagine how wide the reach of a cyber attack could be.

As examples, we all know about two situations significant in scope, although, fortunately, apparently relatively contained in effect. Last fall's attack on Dyn, a global company supporting internet infrastructure, hit millions of IP addresses and temporarily brought down major websites around the world. This spring's WannaCry ransomware onslaught created disruptions for numerous entities in 150 countries and spotlighted the potential for such issues for a myriad of others.

Following such incidents, entities can face downtime, lost sales, lapsed production, foregone customers, and other consequences. Outages or reduced capabilities may be brief or prolonged, with effects likely, but not necessarily, scaled to the length. Even after restoration, an entity's reputation can still suffer and the potential economic benefit of customers or clients diverted may not be recovered. These are just some examples but illustrate the importance of the business interruption topic to insureds of all sizes and types.

The insurance industry is rapidly evolving to write possible coverages for business interruption in a cyber context. Such developments merit close watch. Although policy wordings and applicable limits or sublimits will vary, certain issues, among others, are likely to arise:

Causation: an affected insured must carefully consider its insurance contract to understand what causes of interrupted business may be covered. It must, either on its own or with assistance from a technical expert, timely identify and document what it contends caused the business interruption.

Data: an affected insured must document the lost revenue, lost profits or other economic loss potentially covered under its insurance contract. This will require, for example, comparisons to prior relevant timeframes. As part of its risk management in advance of any incident, an insured should consider whether it maintains or can generate data or reports to demonstrate relevant differences pre- and post-incident. In addition, to the extent that an insured alleges additional economic loss as a result of an incident, an insured should document the amounts involved and how they came to be incurred. The insured should consider the language of its insurance policy to assess whether its insurer's consent is required before incurring any amounts for which the insured may seek coverage.

Mitigation: there may be steps an insured can take to reduce the duration or impact of an incident. An insured's insurance policy may require such remedial measures. Also, depending on the wording, an insured may need to seek an insurer's consent before undertaking such activities. Further, an insured should document the necessity or benefits of any such actions and the reasonableness of the specific amounts incurred.

EVENTS IN MAY

11 MAY 2017
Speaking: Sarah Stephens
IATA Risk and Insurance Management Forum
London

16 MAY 2017
Speaking: Shannon Groeber
Cyber Risk Insights Conference
Chicago, IL

UPCOMING EVENTS

06 JUN 2017
Speaking: Shannon Groeber
NetDiligence Cyber Liability
Philadelphia, PA

06 JUN 2017
Speaking: Sarah Stephens
Risk and Compliance for Law Firms Amsterdam 2017
Amsterdam

14 JUN 2017
Speaking: Shannon Groeber
Advisen Cyber Risk Awards
New York, NY

Cyber threat intelligence

Brought to you in partnership with JLT Specialty's Cyber Risk Consortium Partner CSC

SHADOW BROKERS

On 14 April 2017, a hacker group known as "The Shadow Brokers" released multiple exploits which were purportedly stolen from the National Security Agency (NSA) along with classified details of NSA cyber operations.

The April data dump is part of an on going eight-month campaign in which the group plans to release volumes of exploits. The Shadow Brokers first gained notoriety last year when they began releasing exploits and classified details on NSA cyber operations.

This has seen the group publish previously unknown zero-day vulnerabilities, a theme continued in the April data dump. These included exploits that target personal computers and servers running Windows, except Windows 10.

Among the exploits made public was the Windows Eternal Blue exploit used in the global WannaCry ransomware attack in May, which is believed to have infected over 300,000 computers in 150 countries.

These releases drastically increase the risk of exploitation for many systems, especially for personal computers and servers running Windows. These exploits are likely to be heavily employed while many vulnerabilities remain unpatched. It is paramount to monitor fix releases and patch all systems as soon as possible upon patch release. ■

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

JLT Specialty Limited
The St Botolph Building
138 Houndsditch
London EC3A 7AW

www.jltspecialty.com

Lloyd's Broker. Authorised and regulated by the Financial Conduct Authority. A member of the Jardine Lloyd Thompson Group. Registered Office: The St Botolph Building, 138 Houndsditch, London EC3A 7AW. Registered in England No. 01536540. VAT No. 244 2321 96.

Top Tweets

WannaCry shows threat of the Dark Web

Attacks spur demand for cyber insurance

How to prepare for a global cyber event

Hackers made millions from insider trading

Germany passes data protection laws

Survey finds SMEs not made aware of cyber cover