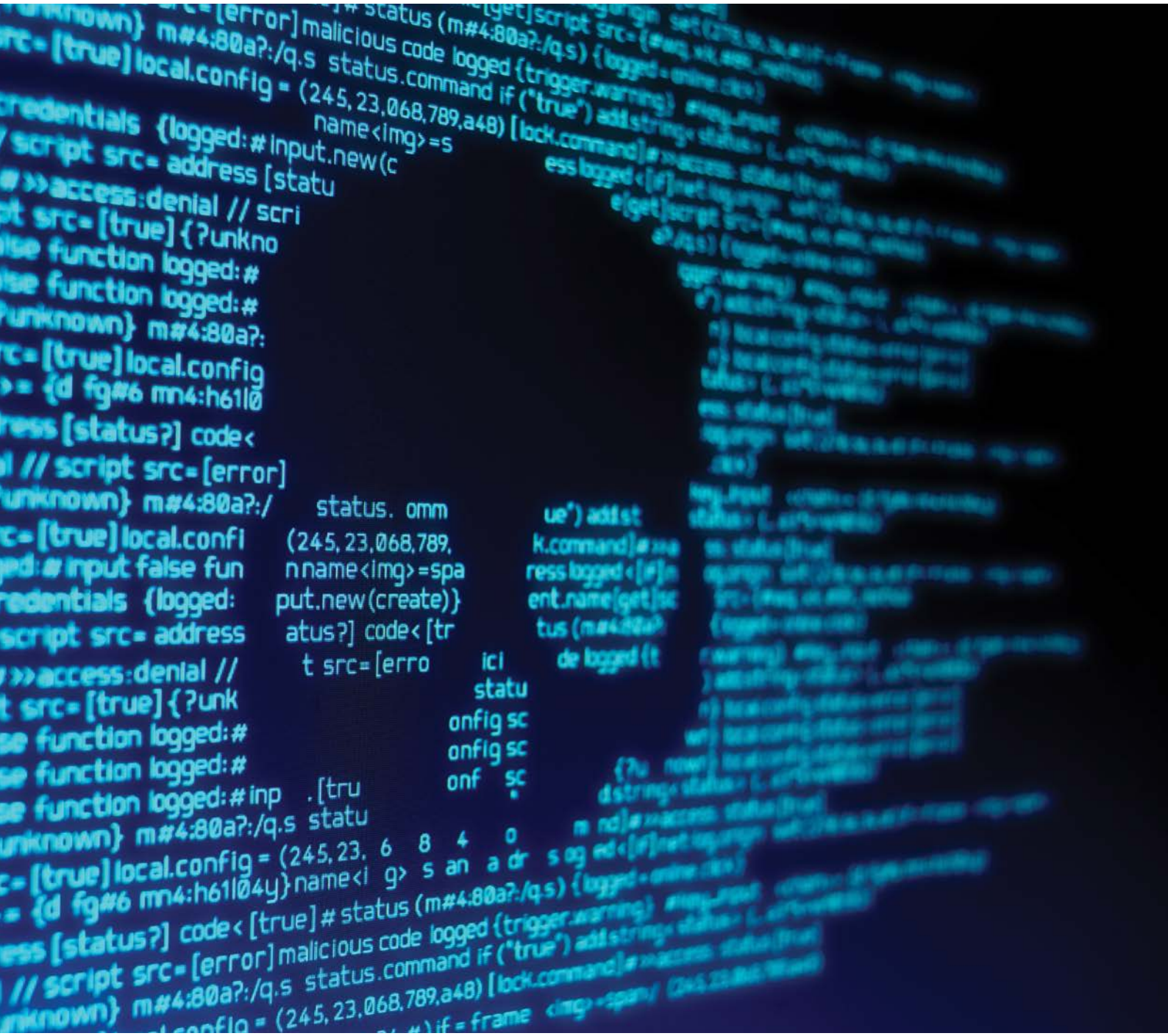


Cyber insurance claims: Ransomware disrupts business

AIG's 2017 cyber claims statistics reflect both the growing maturity of the cyber book of business and a threat environment which has, in recent months, been characterised by a series of sophisticated, systemic malware and ransomware attacks, including WannaCry and NotPetya. While business/network interruption was a significant issue for many European organisations, the majority of these losses were underinsured.

As had been predicted early last year by AIG's cyber experts, 2017 was a year of widespread ransomware attacks and cyber business interruption. AIG's claims statistics show that over a quarter of cyber claims (26%) received in 2017 had ransomware as the primary cause of loss. This is a significant leap from 16% of claims in the years 2013-2016.

"The combination of leaked National Security Agency (NSA) tools plus state-sponsored capabilities triggered a systemic event," says Mark Camillo, head of cyber for EMEA at AIG. "The Wannacry outbreak, which hit hundreds of thousands of machines around the world, could have been worse in terms of scale and insured losses if a UK researcher hadn't quickly found and activated the kill switch."

After ransomware, data breach by hackers, other security failure/ unauthorised access and impersonation fraud were the other main breach types. While the proportion of claims caused by employee negligence reduced marginally to 7% in 2017, human error continues to be a significant factor in the majority of cyber claims.

At a Glance

- AIG saw as many claims notifications in 2017 as in the previous four years combined, receiving the equivalent of one claim per working day.
- Ransomware remains the top cause of loss for cyber claims (the key impact being business interruption), reflecting an increased incidence of such attacks worldwide.
- Professional Services, Financial Services and Retail are at the top of the list when it comes to cyber claims, but incidents are spreading more broadly among a range of sectors, indicating that no industry is immune to cyberattack.

Fig 1 **Cyber Claims received by AIG EMEA (2017) – By reported incident**

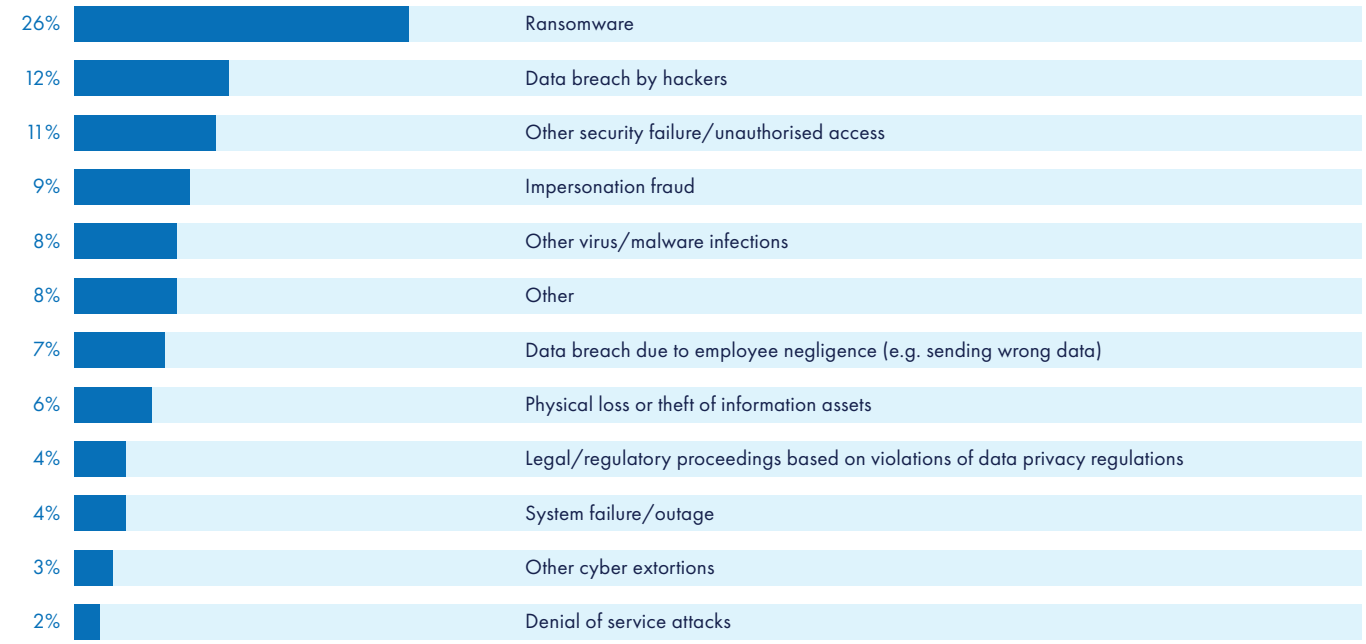
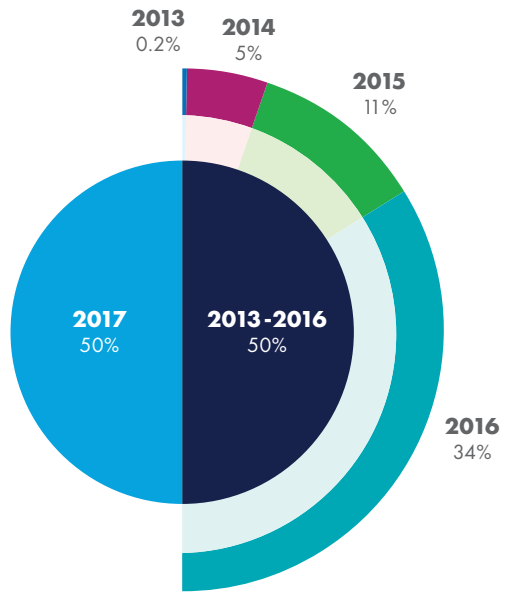


Fig 2 **Cyber Claims Received by AIG EMEA (2013-2017) - Volume**

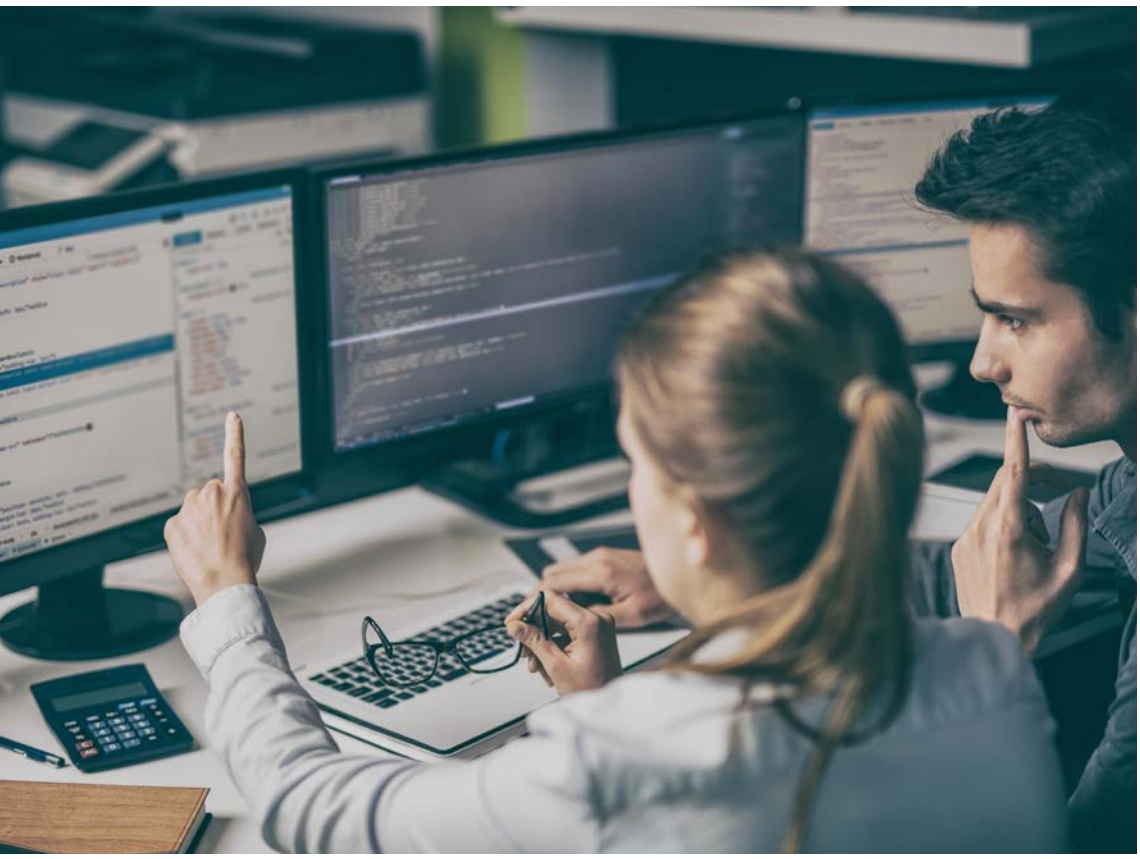


Claims frequency has also increased yet again in the last year. In 2017 AIG's specialist cyber claims staff were handling the equivalent of one claim per working day. The growth in claims frequency reflects a broader trend of cyber loss escalation.

As cyber insurance becomes a more common purchase for many organisations, buyers are also becoming more familiar with the product. They understand more fully the scope of their cover and what incidents can and should be notified to their insurance carrier.

Take-up of cyber insurance grew substantially in the wake of a wave of systemic ransomware and distributed denial of service (DDoS) attacks. This in itself is likely to contribute to greater claims frequency going forward. "We're seeing a lot more interest now from non-traditional buyers of cyber insurance, so can expect an increase year-over-year in the number of claims, just based on the growth of the premium," says Camillo.

"The Wannacry outbreak, which hit hundreds of thousands of machines around the world, could have been worse in terms of scale and insured losses..." Mark Camillo

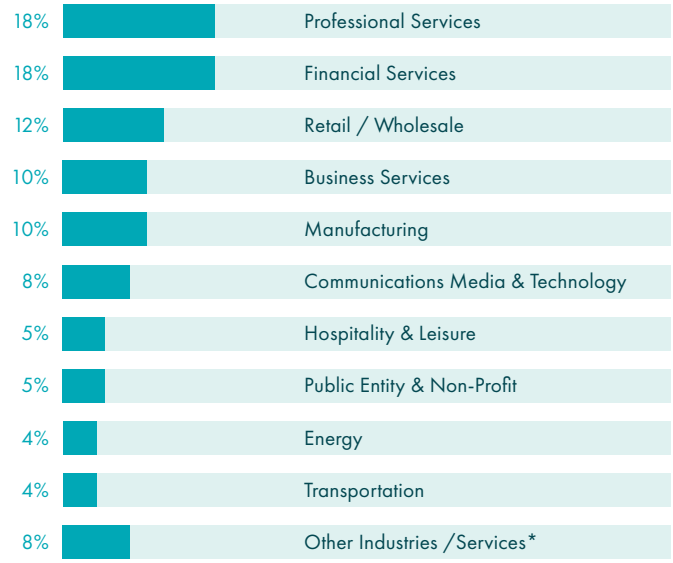


A threat for all industry sectors

AIG's claims statistics reflect the fact that no sector is immune to cyber attack. In 2017, cyber claims notifications were made by insureds in eight sectors that had previously not featured at all in AIG's cyber claims statistics. This is a continuing trend, whereby a larger number of notifications each year are coming from an increasingly broader range of industry sectors, such as energy and transportation, and not just those traditionally associated with cyber risk.

While financial services continues to be a major contributor of claims, the sector made up a lower percentage in 2017 (down to 18% compared to 23% in the years 2013-2016). The very nature of the business of banking and insurance, the fact that financial institutions (FIs) collect and store vast amounts of data and are subject to stringent regulation (and potentially steep fines), has meant that financial services firms have always needed a robust approach to cyber risk.

Fig 3 **Cyber Claims received by AIG EMEA (2017) – By industry**



*Food & Beverage, Construction, Real Estate, Agriculture, Information Services

Note: Figures may not add up to 100% due to rounding

However, the reduction in the proportion of claims coming from FIs could simply reflect the steady growth in claims from other industry sectors, as a result of the growing maturity of AIG EMEA's cyber book of business. According to Camillo, "Historically the financial services segment has always been one of the biggest segments for us, but since last year we started to see a lot of other industries taking out our coverage. This was particularly driven by the events over the summer."

"Many of the recent ransomware attacks have been indiscriminate in terms of which industry they hit," he continues. "If the users of the software that's being targeted have a particular vulnerability they are going to get impacted by these blanket attacks that we saw a lot of in 2017. But it will be interesting to see if we get more targeted attacks in 2018, particularly with the current political environment ripe for state-sponsored activity."

Professional services saw a significant increase in its proportion of overall claims (up to 18% from 6% in 2013-2016), while other sectors more commonly associated with cyber claims saw their shares decrease. "Professional services have become more of a target for data theft," says Kathy Avery, financial lines major loss adjuster, AIG. "Certainly solicitors and accountants with large databases of clients are attractive to cyber-criminals because of the quality of the data they hold, and are vulnerable to cybercrimes that target regular financial transactions."

"There's still an attitude that company leaders think, 'it won't happen to me' or 'I don't have any interesting data so why would I be a target?' But even if a business doesn't hold interesting data it can still fall victim to ransomware extortion, and if files are encrypted the business cannot function," she adds.

"Professional services firms – including solicitors and accountants – have become more of a target for data theft." Kathy Avery

Ransomware becomes commoditised

Major systemic events impacted organisations in many European countries last year. WannaCry targeted a Windows vulnerability that was used to spread malware to hundreds of thousands of machines in over 150 countries. It impacted companies in numerous sectors, including healthcare, financial services, logistics, education and manufacturing.

Over the past 24 months ransomware has become increasingly commoditised with the creators of more recent variants offering revenue-sharing agreements to "affiliate partners". There is no longer a guarantee that insureds will get their data back, even if they pay the ransom. The "professionalism" associated with earlier strains of ransomware – where call centres were provided to talk victims through accessing Bitcoins in order to pay the ransom and get their data restored – has now all but gone.

However, Ransomware-as-a-Service still poses a threat to organisations. Companies may not think their data is important or likely to be compromised, but the claims experience in 2017 demonstrated that ransomware attacks are largely indiscriminate and can impact organisations from all sectors and of all sizes. AIG anticipates that the automation and commoditisation of ransomware will continue to be a trend with businesses and individuals facing an increasing number of attackers.

There is also an expected shift in emphasis towards "cryptojacking"[1]. Over the course of 2017, the crypto market appreciated more than 1,200%[2]. But the increase in the value of electronic currencies has drawn the attention of cybercriminals, who are increasingly taking over networks and using malware to mine for cryptocurrency.

Looking ahead, the more traditional forms of extortion are expected to become an issue in data breaches and become more targeted. This is currently a trend in the US market but has also resulted in losses for European companies, particularly those with a US presence. The EU General Data Protection Regulations (GDPR) is likely to become another tool for negotiation by extortionists, who will threaten to compromise an organisation's data unless a payment is received, knowing that the consequences will be more significant under the new regime.

Network interruption: A severity loss

The claims statistics show that disruption to business (described as 'network interruption' in describing cyber business interruption) as a primary source of loss was down year-on-year compared to 2013-2016, despite evidence that business interruption was a significant issue for many European organisations in 2017. While network interruption loss was one of multiple causes of loss for a significant number of claims, it was not always cited as the primary cause and – as a result – is underrepresented in the claims statistics.

"Quite often insureds don't understand at the initial notification what's going to be the problem," explains Martin Overton, cyber specialist EMEA at AIG. "They just think it's malcode or somebody trying to do an extortion attempt on them. It's not until a forensic team has been brought in and a deeper dive has been done that they find out this is going to have an impact on their business, because they can't get access to their data or their systems have been knocked offline."

[1] https://www.forbes.com/sites/jasonbloomberg/2018/03/04/top-cyberthreat-of-2018-illicit-cryptomining/#48b90c4d5ae8

[2] https://www.forbes.com/sites/cbovaird/2017/11/17/why-the-crypto-market-has-appreciated-more-than-1200-this-year/#53e14c226eed

It remains the case that many companies do not have cyber insurance to indemnify them for network interruption. Much of the financial impact incurred during last year's ransomware attacks, for instance, was a balance sheet loss (see box-out).

Of the claims that were received in 2017, it is clear that the severity of network interruption losses can vary significantly depending on duration, company size and industry, with AIG Europe's indemnified network interruption losses in 2017 ranging from $3,250 to $5.2 million.

Insureds that do not have strong cyber security protections in place and/or back-ups of their data are most likely to suffer from network interruption following a ransomware attack, according to José Martinez, vice president of financial lines major loss claims, EMEA, AIG. "This is a particular concern for SMEs because their systems tend not to be as robust and they may only do their backups periodically," he says.

"Generally speaking, when companies have back-ups, in pretty much all the cases that I've seen they are not interested in paying the ransom," he continues. "However, there were a couple of instances last year where this was a real issue and some companies were really on their knees because they did not have good back-ups. So they had to consider making a payment in order to recover their data."

"In these cases, the longer it goes on, the more they suffer financially," he adds. "Certainly in 2017, far more than in previous years, we've seen insureds asking for our forensic partners KPMG to help them deal with ransomware, to try and get information decrypted or to go back to previous backups. And in addition to the forensic support, some of them have started to submit claims for the consequential losses of not having access to their systems and data, having to send staff home etc."

"There were a couple of instances last year where companies were really on their knees because they did not have good back-ups." José Martinez

Business interruption remains woefully underinsured

Much of the business interruption wrought by ransomware encrypting data and other attacks that brought systems offline in 2017 was not insured. The headline-grabbing ransomware attacks were not necessarily motivated by financial gain, but by a desire to cause disruption by state-sponsored actors.

This was achieved on a massive scale and could have been significantly worse had WannaCry continued unchecked. While ransom payments only generated less than $150,000, total economic losses associated with WannaCry are estimated at $8 billion[3], with half a billion dollars attributed to direct costs and indirect business disruption[4].

As malware and ransomware become more sophisticated, losses associated with business interruption are expected to rise. Yet despite the network interruption threat to organisations being so substantial, it is not capturing the attention it deserves.

"When I go and talk to insureds with the underwriters or the brokers quite often they don't appear to be particularly interested in business interruption, which is odd because that is the biggest problem for most companies nowadays," says Martin Overton, cyber specialist, EMEA at AIG.

[3] https://uk.reuters.com/article/uk-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUKKBN1A20AH

[4] https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-cyber-risk-outlook-2018.pdf

GDPR tops list of data breach trends

A surge in data breach and other security failure claims after GDPR comes into force on 25 May 2018 is expected. Companies will be more inclined to report breaches, with the impact on cyber claims similar to that witnessed in the US after state breach notification laws came into effect.

"A lot of smaller insureds receive advice that they should make a notification but they're not obliged to under the current statute," says Avery. "But that's not going to be an option for them when the GDPR comes into force in May. We're certainly anticipating more notifications after that."

She notes there has been a shift in attitudes towards personal data since the Cambridge Analytica and Facebook personal data scandal story broke and expects this could impact the type of claims received in 2018, with consumers being significantly less accepting of their personal data being breached than they were in the past.

"We recently dealt with a claim following a breach at a university," she says. "They made the notification as if GDPR was already in place. That proved to be quite a costly exercise and it was also difficult for them to manage reputationally. When you notify 100,000 people that can snowball into quite a big undertaking. Individuals can be quite upset when they get these data breach notification letters, even if they are precautionary."

The outcome of the collective action in the UK courts against the supermarket giant Morrisons, filed by staff, will be an important test case on how courts are likely to compensate those whose data has been compromised. The employees are seeking compensation for the "upset and distress" caused after the personal data of nearly 100,000 staff was stolen in 2014[5].

There is some anticipation the introduction of GDPR could see more shareholder lawsuits against companies and their directors in the future. The US has had strict notification requirements for a number of years and nearly every high-profile cyber breach is met with at least one class action lawsuit.

While the same level of litigiousness and collective redress mechanisms do not yet exist in Europe, the Morrisons ruling could pave the way for similar actions to be brought in the future. "If in the case of Morrisons there is an award or damages based on the emotional distress caused by the loss of data, that could be significant and set an interesting precedent," says Camillo. "It could fuel more of these types of actions against organisations once they have notified the public of a breach."

[5] https://www.independent.co.uk/news/business/news/morrisons-data-leak-staff-payout-details-sensitive-data-personal-online-hack-a8086521.html

"Most directors and officers (D&O) policies are not going to have an exclusion for shareholder legal action brought following a cyber breach, so they are going to respond in light of those types of claims," he continues. "There is currently quite a lot of uncertainty leading up to GDPR because there's also the element of the fines and penalties. This could be the first year that we start seeing some of those things coming to light, depending upon how aggressive regulators choose to be with the new laws."

Under the GDPR there are two types of fine that can be levied against firms for failing to have the necessary systems and security in place to protect third-party data. The first is up to €10 million, or 2% of annual global turnover of the previous year, whichever is higher. The second is up to €20 million or 4% of annual turnover of the previous year, whichever is higher.

"You may start getting more clarity later in 2018 as to whether the fines and penalties are actually insurable," says Camillo. "In a few countries across Europe we know it will be prohibited, but in other jurisdictions, including the UK, it's not exactly clear. The government has made remarks that insurance policies could possibly pay for the more administrative fines or penalties."

"We know these vast botnet armies are out there right now, and they don't show any sign of slowing down." Martin Overton

Companies failing to install DDoS defences

Two years on from the Mirai botnet that brought down DNS provider Dyn, DDoS vulnerabilities remain a threat and companies are not doing enough to protect their networks from such attacks.

The Reaper botnet is the latest variant. Like Mirai it is comprised of a large number of unsecured home devices that make up the Internet of Things (IoT), including home routers, IP cameras and baby monitors.

"The Reaper botnet is mainly made up of IoT devices that can potentially push out over 1.6 terabits per second... that's a huge amount of data," says Overton. "We know these vast botnet armies are out there right now, and that they don't show any sign of slowing down, but a lot of companies are not putting the necessary defences in place."

While there are now a number of solutions available in the market that are guaranteed to keep systems up and running during an attack, firms are not doing enough to install DDoS protections and SMEs are likely to be put off by the associated costs.

Conclusion: Time for a cyber health check?

AIG anticipates that the significant financial consequences of business/network interruption will continue to be felt through 2018, driving demand for cover and the continued growth of the cyber insurance market across Europe. As the business grows there is the natural expectation that claims frequency will continue to increase, and possibly also the severity of those claims.

Claims trends over the next 12 months will continue to be impacted by the commoditisation of ransomware, an expected spike in data breach losses later in the year due to the influence of GDPR and the continued influence of state actors against an increasingly fragile and politically-uncertain backdrop. Certainly traditional cyber extortion and impersonation fraud are among the trends to watch, and employees remain the first line of defence against such attacks.

Whatever their size or sector, organisations operating in an interconnected and increasingly digital world have never been more vulnerable to attack and to the potentially dire financial consequence arising from such attacks. AIG anticipates the systemic nature of ransomware attacks witnessed in 2017 is just the tip of the iceberg and that this will become even more of a challenge in the future.

While prevention is always better than cure, organisations must prepare for the inevitability that their systems and networks will, at some point, be breached. Cyber-resilient organisations are those that prepare for this and practise their response, in addition to implementing a robust cyber risk strategy and ensuring they are indemnified for the full range of cyber exposures, including network interruption.

Top cybersecurity risks for businesses

Our claims experience suggests that, in terms of security failures, the top risks for businesses are:

- **External servers with remote access combined with weak passwords.** This offers an opportunity for the introduction of malware and ransomware. Remote access should be carefully controlled.
- **Lack of user awareness permitting hacking by phishing for passwords.** The user engages with the content of a phishing email and is directed to a fake log in page where credentials are harvested opening the victim's account to hackers. Users should ask themselves "do I trust this email?" Any request for log-in details is a red flag for phishing.
- **Weak log-in protocols.** The risk from phishing is eliminated if two factor authentication is enabled, requiring a secondary code for account log in. As a minimum, this should be adopted for business directors and partners, and employees involved in payments.

Claims case studies

Manufacturing firm suffers business interruption following ransomware attack

The insured designs and manufactures cranes, excavators and heavy and specialised lifting equipment.

On 1 December, the insured discovered that it had been the subject of a ransomware attack. Up to 85% of its folders and documents had been encrypted. The insured called the AIG CyberEdge hotline and received incident response services from an IT forensic firm. Following advice, it decided to restore data with the back-ups. This work was finalised on 3 December.

As a result of the failure of the IT system, employees of different departments were unable to work on 1 and 2 December because they could not access the server. The insured employs approximately 300 production staff and engineers. Its main business consists of turnkey projects or engineering projects in which the use of IT equipment is essential in carrying out the work.

The engineering team stores information on the company server in order to enable sharing of information amongst employees. The engineering staff bills their chargeable hours directly to a project. The inability to perform work by the engineers during this two-day period therefore directly impacted the numbers of hours the company could bill for. It was difficult to recoup these hours at a later stage because the insured had deadlines to meet on its various projects and not meeting those deadlines would result in customers invoking penalty clauses.

Coverage was provided for the extra cost of engineering staff to guarantee the continuity of the operation and timely completion of the projects.

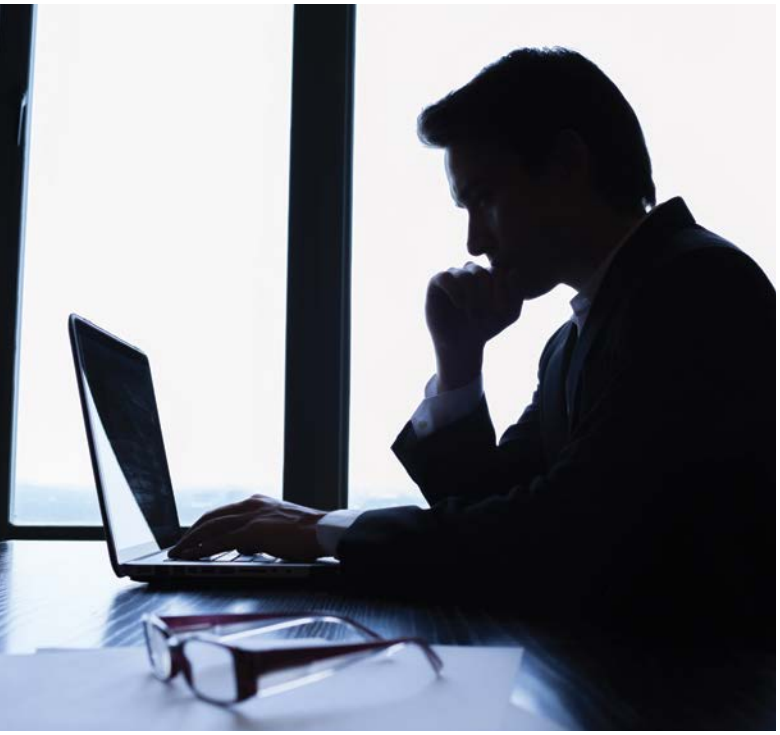
DDoS and extortion threat against a financial institution

The insured financial institution received an email ransom demand for one bitcoin, or the attackers would launch a DDoS attack against the insured. If the ransom was not paid, they also threatened to increase the ransom to ten bitcoins.

With assistance from AIG the insured engaged a DDoS protection service to mitigate the impact of any attack and notified their ISP of a potential attack, rather than trying to manage the situation on their own with inadequate resources such as firewalls.

Investigations into the incident suggested that the would-be attackers were based in Latvia. The group claimed to be 'XMR Squad', a group that had launched DDoS attacks against several companies over the previous week and hence it appeared to be a credible threat. However, intelligence received from the Bank of England suggested that the email was likely to have originated from a copycat rather than the official group.

There was no indication that the prospective attacker obtained access to personal data controlled by the insured. Ultimately the threat did not materialise, and there was no negative impact to the confidentiality, integrity or availability of the insured's data assets.



The insured's website and digital platform both remained online and operational, albeit with increased and ongoing monitoring and traffic analysis in place. The financial institution did not suffer any serious financial loss, aside from costs associated with securing outside legal and other crisis-management advice relating to the incident, and indeed significant management time spent investigating and resolving it. The incident response costs were paid by AIG.

Targeted phishing attack on luxury goods business

The insured business appeared to have been the victim of a phishing email scam, first targeting its employees and then its clientele.

The preliminary investigation into the incident revealed that an employee had clicked on a link contained in a phishing email nine months before the insured became aware of any issues, thereby exposing his mailbox to the perpetrators. At least two other employees' email inboxes were affected when they clicked on a link in similar phishing emails they received. The perpetrators may have obtained contact information for clients by gaining access to these three inboxes

Subsequently, over the course of 12 months, and with increasing frequency, the insured received queries from clients who had received "spoofed" phishing emails claiming to be from the insured but which, in fact, were from the scammers. These emails, like the one originally received by the three employees, prompted the clients to click on a false link where they were asked to provide login credentials, payment card information and other personal information used to support the insured's "know your customer" analysis.

Several clients who had reported receipt of this phishing email were listed on a spreadsheet found in one of the employee's email boxes. This spreadsheet was a master list of clients, containing approximately 21,000 email addresses.

Forensic IT specialists engaged on advice from AIG blocked access to the suspect URL and performed a targeted investigation of affected mailboxes determining what data was accessed. Following a deep analysis of the data the compromise was narrowed to less than 1,000 data records. This allowed the insured to formulate a bespoke, personalised response for affected clients, many of whom were high-net-worth, high-profile individuals.

CLAIMS FIRST

Methodology

In March 2018, AIG Europe carried out an analysis of more than 600 claims notified under its cyber policies between 2013 and December 2017.

www.aig.com

Mark Camillo
Head of Cyber,
EMEA

Tel: T +44 (0)20 7651 6304
mark.camillo@aig.com

Kathy Avery
Financial Lines
Major Loss Adjuster

Tel +44 (0)20 7063 5423
kathy.avery@aig.com

Martin Overton
Cyber Specialist,
EMEA

Tel: +44 (0)20 7954 7129
martin.overton@aig.com

José Martinez
VP, Financial Lines
Major Loss Claims, EMEA

Tel: +34 91 5677 431
jose.martinez@aig.com

GBL00002769 05/18