AIG

Claims Intelligence Series

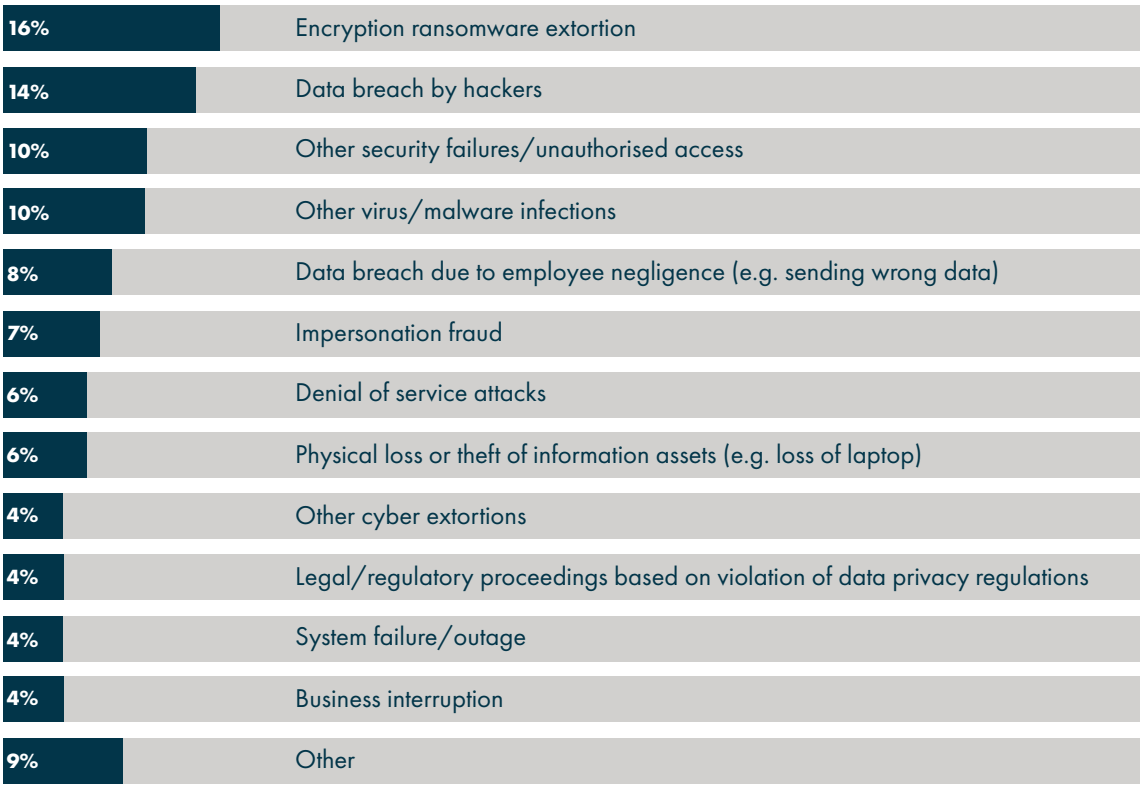
# Behind the numbers:
# Key drivers of cyber insurance claims

AIG EMEA (Europe, Middle East & Africa) cyber claims statistics reveal how cyber extortion and ransomware is one of the fastest growing sources of cyber loss for organisations large and small. From a severity perspective, business interruption and data breach will continue to be significant drivers of loss now and into the future.

Major data breaches and more recently, audacious Distributed Denial of Service (DDoS) attacks exploiting the Internet of Things (IoT), are the types of cyber intrusion that are most likely to capture headlines. But it is cyber extortion and ransomware that is one of the fastest growing cybercrimes, a trend that is captured by AIG EMEA cyber claims statistics from the period between 2013 through to September 2016.

Encryption ransomware extortion claims accounted for 16% of claims during that period, with a further 4% of claims relating to other cyber extortions. 2016 in particular has seen a proliferation of cyber extortion attacks. "For the first nine months of this year we have had a lot of notifications from businesses that were victims of ransomware type attacks, and nearly all of them had extortion elements to them as well," says Kathy Avery, Financial Lines Major Loss Adjuster. "A lot of quite small businesses have been affected."

## Cyber claims received by AIG EMEA (2013-2016) - By type




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

She offers the example of an online gardening business that discovered ransomware had got onto their system and was encrypting their files. While the SME did not have a significant amount of sensitive data that could have been compromised, they were unable to contact customers and access invoices. The firm decided to pay the ransom in order to unlock their files and AIG's forensic provider supported the process, supervising the application of the decryption key.

There is some overlap between extortion claims and denial of service (DoS) and DDoS claims, as many of these have an extortion element. Six percent of AIG EMEA cyber claims over the past three years have been categorised as denial of service attacks. "A number of DoS attacks would fall into the extortion group," says Avery. "In some of these attacks they use a SQL injection and they can take data out and threaten to publish the data unless you pay the ransom."

While take up of cyber insurance is increasing, resulting in more notifications of cyber extortion attacks, it is thought that a high number of ransomware losses remain unreported. "Ransoms are typically paid in Bitcoin and what can happen, if you're not experienced, is you're then vulnerable to yet another attack while you think you're decrypting your files," says Avery. "People are sometimes surprised at how small some of the ransom demands are."

Nevertheless, given the high frequency of attacks, extortion is a lucrative and relatively straightforward way of accessing 'fast cash' for cyber criminals. Malicious actors are thought to have generated around $325m in revenue over the past three years by using the CryptoWall code, according to research by the Cyber Threat Alliance, while the Cryptolocker gang made over $30m in 2015 using relatively simple ransomware.

McAfee Labs kept ransomware at the top of its threat predictions for 2016, anticipating a new focus on industry sectors including financial services and local government. Hospitals and doctors' surgeries have also been a particular target. "In the case of healthcare, encryption ransomware has the potential to have an immediate impact on patient care and breach of trust, and that makes them very sensitive as a sector," says David Ferbrache, technical director at KPMG.

"Around January February time we saw a complete change and an explosion in different types of ransomware - different families and tools - which suggested that the whole thing had become a 'crime-as-a-service' model," he continues. "The whole thing became commoditised. And we're beginning to see some signs that the groups conducting the ransomware attacks are becoming a little bit more savvy."

In cases of cyber extortion, claims severity depends on the type of organisation, the level of business interruption caused and need for forensic investigation and system restoration. Ransom demands typically remain small. In the case of DoS or DDoS attacks, the costs associated with websites being taken down can be particularly high, as the online retailer example in the case study section below demonstrates.

"Denial of Service attacks have also become very heavily commoditised," explains Ferbrache. "Cyber criminals can buy a DoS attack for $5 or $10 an hour and that will beat upon a public-facing website and generate quite a lot of traffic."

"The one that is worrying everyone right now are the large-scale DDoS attacks," he continues. "We're seeing botnets of the Internet of Things now - where digital video recorders, CCTV cameras and home routers are being compromised - and that's generating extremely high levels of disruptive traffic."

**Malicious actors are thought to have generated around $325m in revenue over the past three years by using the CryptoWall code**

In October 2016 a massive DDoS attack hit servers at domain name system provider Dyn, resulting in widespread disruption. The DDoS involved a botnet coordinated through tens of millions of connected devices including surveillance cameras, webcams, smart thermostats and even baby monitors infected with the Mirai malware. Large DDoS attacks are on the rise, up 138% year-on-year, according to Akamai's latest State of the Internet/Security Report.

For those affected by ransomware or Denial of Service attacks, business interruption costs are highest during peak trading periods. Half of respondents to one recent survey revealed they could lose over $100,000 per hour during critical periods. "I know of one case where the ransom demand was £262 and the business interruption claim was in seven figures," says Stephen Tester, partner, CMS Cameron McKenna. "They took down a website over a weekend."

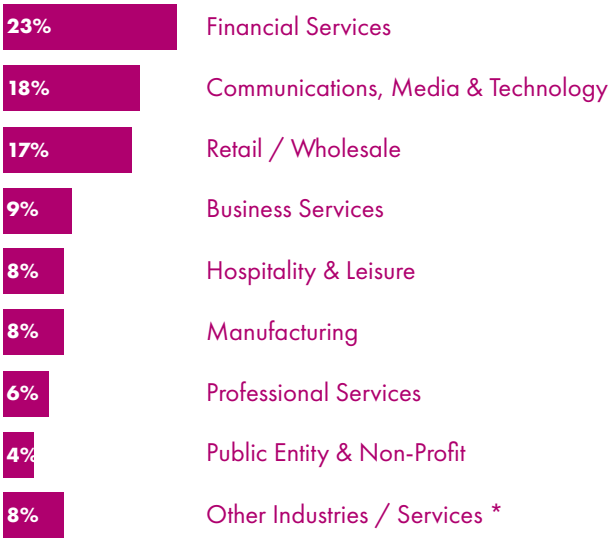
While business interruption currently accounts for just four percent of AIG EMEA cyber claims (with a further four percent of claims falling under system failure/outage), BI cyber claims are expected to increase in frequency and severity in the future. Rapid breach response is one way of mitigating the potential impact.

# Regulation to drive data breach claims

AIG EMEA's data breach losses fall into two separate claims categories - those caused by hackers and breaches resulting from employee negligence. Together they account for over a fifth of cyber claims (22%) received over the past three years (see p2). The growing cost of data breach, associated reputational impacts and increasing notification requirements are likely to impact both the frequency and severity of such claims going forward.

Perhaps unsurprisingly, the majority of cyber claims currently emanate from industries that are required to notify customers if sensitive data has been compromised, with financial services accounting for almost a quarter of all AIG EMEA cyber claims received during the past three years, followed by communications, media & technology (18%), a category that includes telecommunications.

## Cyber claims received by AIG EMEA (2013-2016) - By industry

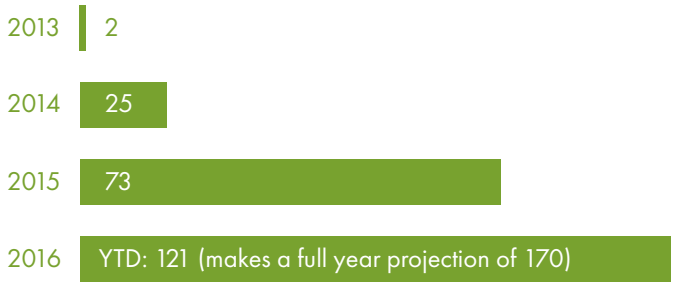



*Construction, Food & Beverage, Information Services, Other Services, Transportation, Agriculture & Fisheries, Energy and Real Estate

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

Under the General Data Protection Regulation (GDPR), companies based in the EU and those based outside of the EU who process EU citizens' data will be required to report a breach within 72 hours of it occurring – if that is feasible. There will be significant fines for those firms that have failed to adequately protect data. A company can be fined up to two percent of their global annual turnover for not having records in order, failing to notify the supervisory authority about a breach or failing to conduct impact assessments. More serious infringements could merit a four percent fine.

## Cyber claims received by AIG EMEA (2013-2016) - Volume




It is anticipated the new data protection rules and headline-hitting data breach exposés will continue to drive greater demand for cyber cover, one of the factors resulting in increased cyber claims frequency. José Martínez, VP Financial Lines Major Loss Claims, observes that AIG EMEA has seen annual claims under cyber stand-alone policies grow from just two in 2013 to 121 by September 2016, with a full year projection for 2016 of 170

The average total cost of a data breach globally is now $4m, up by 29% since 2013, according to research by Ponemon and IBM. In spite of this increasing expense, the severity of some claims can be mitigated through a swift and professional response, explains Avery. "Because of the way the policy operates we can contain quite a lot of incidents in the first 48 hours."

"Certainly with the European data protection regulations that are coming in, if you can show you dealt with a breach well and that you had good systems in place, the fines should be lower," she adds.

**The average total cost of a data breach globally is now $4m, up by 29% since 2013**

There is, more often than not, a human element to cyber claims, whether a result of employee negligence or the deliberate actions of a disgruntled current or former employee. The risk of staff falling for phishing scams or sending out the wrong data can be reduced through training and have proper controls and systems in place. The loss or theft of laptops, datasticks or hard drives was responsible for six percent of AIG EMEA cyber claims between 2013 and 2016.

Human error and/or insider knowledge is a common vulnerability that is exploited by so-called "Friday afternoon fraud", a particular target being law firms, which are often attacked on a Friday afternoon so the fraud is unlikely to be discovered until the following Monday. Criminals are becoming increasingly sophisticated in how they persuade firms to part with sensitive information by using details of genuine transactions to appear legitimate.

While emails are typically used to defraud companies in this way, there is a question mark whether such claims should fall under cyber policies or professional indemnity insurance, thinks Tester, particularly where a spoof email uses a similar but not identical email address to a client. "We see quite a few claims which are on the edges of cover," says Tester. "In many cases it's conventional fraud that is committed electronically, with no actual breach of security."

Fake president fraud is another issue. These typically involve an employee, usually somebody in the accounts department, being contacted - typically by phone and email - by someone purporting to be a senior officer and instructing them to make an urgent payment. Losses from "business email compromise", as they are called in the US, had risen to $3.1 billion as of May 2016, according to the FBI's Internet Crime Complaint Center, a massive increase of 1,300%.

"That's the tip of the iceberg, because that's only US and partial international reporting into the FBI," thinks KPMG's Ferbrache. "It is a massive issue. Sometimes these scams involve compromising a legal firm or accountant first and they are then the channel which are used for generating the emails which are used to spoof and phish the target organisation."

"The average value of a CEO fraud right now is $160,000," he adds. "And the biggest one we've seen reported in Europe was €40m. But I don't know if those are cyber crimes or just really well-organised confidence tricks."

# Drilling down: Cyber claim case studies

The following selection of actual AIG cyber claims demonstrates the broad scope of losses that are triggered under our CyberEdge insurance product. They also illustrate the spectrum of insureds impacted by cyber events, ranging from SMEs through to major corporates.

## Ransomware attack on online embroidery company

Shortly before Christmas 2015, an online embroidery company in the UK suffered a ransomware attack. The attacker created two user accounts and attempted to encrypt and remove customer details and information regarding orders, stock and accounts. The attacker also left a ransom note instructing the insured to contact a specified email address.

Whilst the attacker failed to encrypt the data, they were successful in deleting numerous files and moving data around. With data having been relocated, the insured could not rely upon its accuracy and was unable to operate its business via the system. The last data backup had taken place four days prior to the attack so information from the previous week had also been lost.

The insured received legal and IT advice in connection with the attack. Third-party data did not appear to have been compromised so the insured was not advised to make a notification to the data protection authority.

The insured's IT consultants provided recommendations on how to mitigate the effect of the breach and take precautions to minimise the prospect of a further incident. In particular, the insured was advised to save the data from the affected server in order to investigate how the breach occurred and review its disaster recovery plan.

## Encryption of files on insurance intermediary's internal network drive

One of the insured's computers was infected with CryptoWall malware that had encrypted certain files stored on the computer and the insured's internal network drive. The names of the files had been altered to "help_your_files.png" and a ransom was demanded to regain access to the files.

The insured, based in the UK, thought the encrypted files contained customer data such as names and addresses but the insured did not believe that the encrypted files contained customers' other personal data or financial information. There did not appear to be any evidence suggesting that the data within the encrypted files had been accessed or exported, or any loss of data due to the routine back-ups of the insured's IT system.

The insured received legal advice regarding the extent of its notification obligations to Lloyd's and the FCA. External IT consultants also advised the insured to implement immediate measures to contain the incident (such as restricting file sharing between users) and suggested implementing defence measures to prevent such incidents occurring in the future.

## Distributed denial of service (DDoS) attack on online retailer

The insured's website was the subject of a DDoS attack, which resulted in the website being inaccessible or experiencing reduced performance. Prior to the attack the insured received an online message claiming that the insured's website protection was extremely low and would be taken offline unless a payment of £3,000 was made. Further ransom demands of £500 were made during the attack.

The insured was likely to have lost sales as a result of the website being unavailable, but the extent of this loss was unknown. The insured did not believe that any data had been accessed or extracted. The insured was advised that there were no legal notification requirements arising from the attack.

However, various IT and PR issues arose that warranted further consideration. In addition to external IT consultants, the insured was advised that PR consultants were at its disposal to assist with any fallout from the insured's website being temporarily unavailable.

## Unauthorised mail-out by debt recovery company

The insured experienced an unauthorised mail-out caused by an error with a third-party software platform. A third party claimed £11,275 from the insured for work undertaken as a result of this mail-out. The insured was seeking to recover this sum from the platform provider but there was a real risk it would have to pay this amount.

A breadth of issues arose from this incident. Legal advice was provided to the insured in respect of the scope of its contract with the platform provider and the insured's ability to recover the sum claimed from the provider. Data protection advice was also given to the insured, although there did not appear to be any loss, release, compromise or corruption of any personal data as a result of the incident.

External IT consultants provided advice to the insured, which included gathering evidence to demonstrate that the incident was not caused by a fault in the insured's systems or of the insured's employees. Finally, as letters of complaint had been received by a number of recipients of the mail-out, the insured was advised to consult its in-house or external PR advisers to consider whether a PR response would be appropriate.

## Cryptolocker attack on a bank

Shortly before the start of the weekend on a Friday at 8pm, a retail bank in Ireland was attacked with crypto locker malware. The crypto locker blocked different laptops and desktops. It encrypted shared drives which contained important customer details and information regarding orders, stock holdings and loan agreements. Over 11.000 files were affected.

The implemented anti-virus system was not able to detect the crypto locker when it entered the systems of the bank. Within a short period of time the insured was able to identify all affected hardware and removed them from the network, effectively placing them in quarantine. With a data backup from the shared drive, the bank was able to restore the encrypted information.

After calling the AIG Cyber-Hotline, the insured received legal and IT advice in connection with the attack. Third-party data did not appear to have been compromised. Therefore, the insured was advised by the involved law firm not to make a notification to the data protection authority.

The insured's IT consultants provided recommendations on how to mitigate the effect of the breach and take precautions to minimise the prospect of a further incident. In particular, the insured was advised to save the data from the affected server in order to investigate how the breach occurred and review its disaster recovery plan.

## Customer Data in the DarkNet

In winter 2016, the CISO of a financial service provider was informed that customer data was offered on a platform in the DarkNet. With the support of IT-forensics provided by the AIG Cyber-Hotline the whole amount of compromised data was detected and confirmed that the available data matched with recently stored data of the financial institution. Also the evidence of the data breach was determined and properly secured. A SQL injection attack a few weeks before the data release on the DarkNet was the reason for the incident.

Over 60.000 data-sets with sensitive customer IDs and trading accounts details were affected. Due to those circumstances, the insured reported the incident immediately to the regulator and to the stock exchange. Furthermore the affected clients were informed. Legal and PR advise in connection with the incident was provided via the AIG Cyber-Hotline and the event management team.

Further support is available from PR consultants which agreed a strategy with the financial institution to communicate with the clients and media. To avoid fraudulent actions with the compromised data, different service providers were engaged to monitor the affected data-sets.

With support of lawyers, as well as IT- and PR consultants, the insured was able to react professionally to the incident and had access to further resources outside the company which supported the insured to decrease the impact of the attack and to reduce the risk of incidents in the future.

## Key questions to ask a cyber insurer

1. *Does the insurer have a history of handling and paying claims?*
2. *Does the insurer continuously explore new ways to help insureds stay ahead of emerging cyber risks?*
3. *Will the insurer be able to provide certainty of protection around the world?*
4. *Does the insurer have a pre-approved panel with access to top forensic IT, legal and PR experts?*
5. *Does the insurer take a holistic approach to underwriting and claims by offering pre-loss services and breach response expertise to help mitigate the risk?*
6. *Is the insurer communicating and handling claims through outside counsel or does it have an internal team of specialised claims adjusters, enabling a continuous dialogue between claims and underwriting?*

## About the authors

Kathy Avery is Financial Lines Major Loss Adjuster at AIG Europe Ltd. and specializes in high value professional indemnity and cyber claims in the UK and internationally. José Martínez is VP Financial Lines Major Loss Claims in EMEA.

## Methodology

In October 2016, AIG Europe carried out an analysis of 221 claims notified under its cyber policies between 2013 and September 2016.

## Contacts

AIG has dedicated cyber claims and underwriting capabilities across Europe. Our experienced team is dealing with a wide range of cyber claims every year. For more information, contact your local AIG office.


**Nepomuk Loesti**
Head of Liability and Financial Lines
Deutschland/Österreich/Schweiz
Financial Lines | AIG Property Casualty
AIG Europe Limited, Direktion für Deutschland
Speicherstraße 55, 60327 Frankfurt
T +49 (0)69 97113-271
nepomuk.loesti@aig.com

**Alexander N. Shopov**
Direktor Vertrieb Österreich Distribution
AIG Property Casualty
AIG Europe Limited, Branch Austria
Herrengasse 1-3 | 1010 Vienna
T +43 (0)1 5332500-38
alexander.shopov@aig.com

**Elisabeth André-Raecke**
Senior Underwriter
Practice Leader Financial Institutions Switzerland
Central Zone (Austria/Germany/Switzerland)
Financial Lines | AIG Property Casualty
AIG Europe Limited | Avenue Louis-Casaï 18 | 1211 Genève, Switzerland
T +41 (0)22 747 75 75
elisabeth.andre@aig.com

**Giv Kahrom**
Underwriter
Commercial Institutions & Cyber Risks
Financial Lines | AIG Property Casualty
AIG Europe Limited | Sägereistrasse 29 | CH-8152 Glattbrugg, Switzerland
T +41 43 333 37 35
giv.kahrom@aig.com


**www.aig.com**

AIG Bring on tomorrow®