Claims Intelligence Series

Cyber Claims: GDPR and business email compromise drive greater frequencies

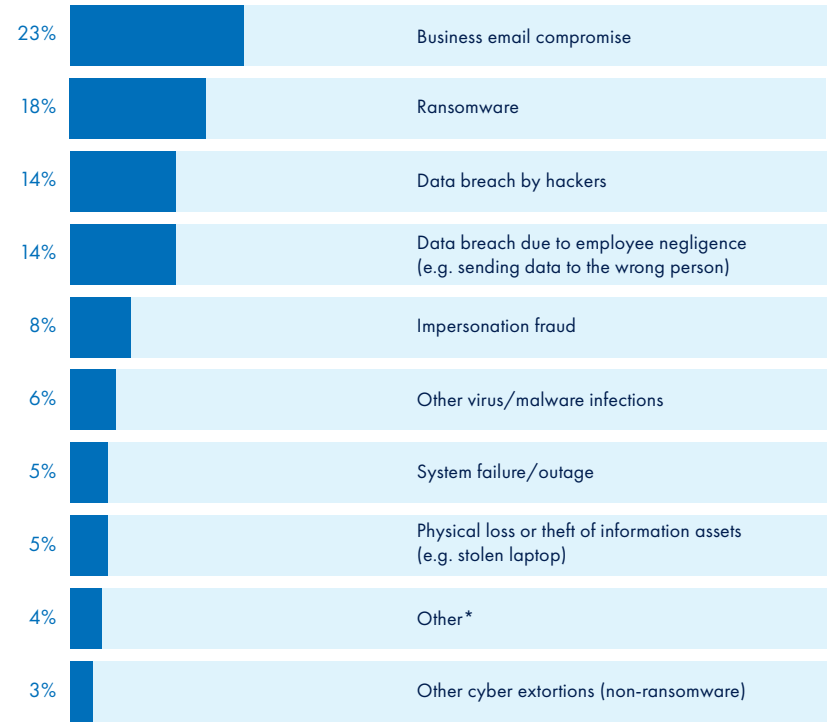
Business email compromise (BEC) has overtaken ransomware and data breach by hackers as the main driver of AIG cyber claims, according to the latest cyber claims statistics. Nearly a quarter of reported incidents in 2018 were due to business email compromise (BEC), up significantly from 11% in 2017. Ransomware, data breach by hackers and data breach due to employee negligence were the other main breach types in 2018.

BEC[1] has entered the report this year under a new category given the high number of BEC-related claims received by AIG over the past 12 months.

In most cases the compromise can be traced back to a phishing email containing a link or attachment. If the recipient engages with the content of a phishing email it may allow intrusion into the user's inbox. The majority of users are familiar with the concept of phishing emails but there remains a high number of incidents where the user follows a link directing the recipient to a bogus login screen. As soon as the victim enters their credentials, they are captured by the cyber-criminal who then has the necessary information to login to the victim's email account.

The perpetrator is then able to send and receive emails from the victim's email address and access all the information in the victim's email inbox. In many cases the BEC is exacerbated by malware that spreads the scam to contacts in the recipient's inbox. A relatively simple type of scam, BEC attackers often target individuals responsible for sending payments, using spoof accounts to impersonate the company C-suite or a supplier and requesting money transfers, tax records and/or other sensitive data.

Fig 1 **Cyber Claims received by AIG EMEA (2018) – By reported incident**



*Denial of Service Attacks, Legal/Regulatory Proceedings based on violations of data privacy regulations

[1] Previously, such attacks fell within the scope of 'other security failure/unauthorised access'.

At a Glance

- Business Email Compromise (BEC) is now the top cause of loss for cyber claims followed by ransomware which is becoming increasingly targeted and disruptive, affecting business interruption costs. All cyber attack impacts are still greatly influenced by human error.
- Professional Services is now the sector hardest hit by cyber claims, followed by Financial Services. However, incidents continue to spread among a range of sectors, indicating that no industry is immune to cyberattack.
- The long term trend of increasing claims frequency continued in 2018 with around as many claims as the previous two years combined.

Methodology

In March 2019, AIG carried out an analysis of more than 1,100 claims notified under its cyber policies between 2013 and December 2018. The results of this analysis show general insights into this area only. It should be noted that other industries and sectors not highlighted in this report may also experience frequent and severe claims. In 2018, the number of claims notified under AIG's cyber policies were broadly commensurate with AIG's premium growth for this product.

Other attacks focus on the content of the recipient's inbox, harvesting client and employee information, including personal data. They may also target confidential corporate information, including trade secrets, but most are motivated by monetary gain.

"Ultimately what's behind a lot of these compromises is organised crime," says Jonathan Ball, partner at Norton Rose Fulbright. "They're not interested in stealing personal data and selling it on the dark web. It's pure financial fraud."

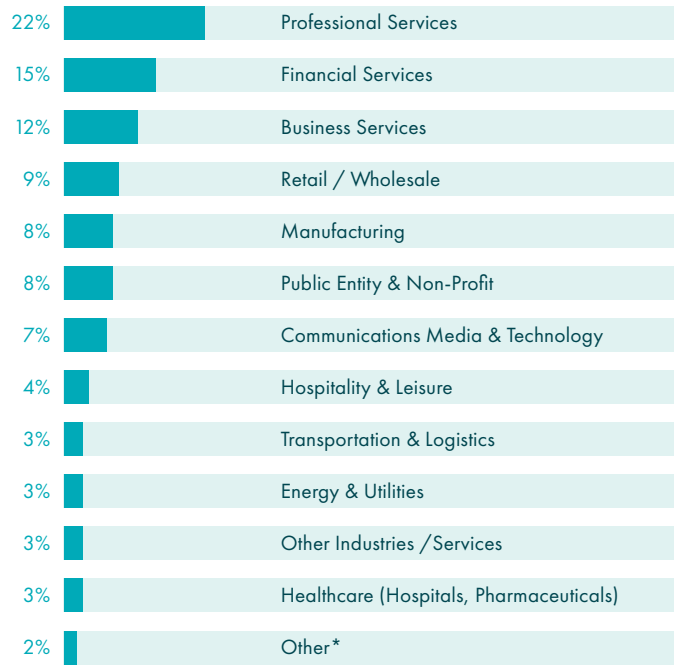
BEC attacks are often successful because they use social engineering to create emails that appear legitimate. Even larger organisations may fall for the scams, explains Jose Martinez, vice president of financial lines major loss claims, EMEA, AIG, suggesting more investment is needed to train staff to better identify rogue messages. "We're still seeing a surprisingly high level of these forms of fraud being perpetrated and some are affecting quite large and sophisticated clients. You may think that every CFO at a large company would know about this by now, but it's still happening."

For BEC and impersonation fraud claims the cyber policy will cover the cost of an IT forensic investigation to determine whether the insured's system was compromised and identify the compromised data. It also covers legal advice on reporting and notification obligations to data subjects and regulators though insurance cover for financial loss due to criminal activity is often restricted.

"These incidents are becoming more expensive to investigate," notes Mark Camillo, head of cyber for EMEA at AIG. "When a malicious actor gains access to the mailbox you have to do a deep dive, understand what information they may have gained access to and whether it has triggered any GDPR requirements."

Although financial services firms were the first buyers of cyber insurance and the largest sector, we saw professional services firms move ahead in 2018 in the number of reported claims. This is also the sector most vulnerable to business email compromise. Year-on-year, the number of claims emanating from professional services firms including law firms and accountants, increased from 18% to 22%.

Fig 2 **Cyber Claims received by AIG EMEA (2018) – By industry**



*Food & Beverage, Construction, Education
Note: Figures may not add up to 100% due to rounding

Camillo thinks such firms can be more prone to BEC because of a lack of sophistication when it comes to cyber security. "The criminals are going to go where they can make the most money," he says. "Because they are so heavily regulated you tend to find that financial services firms have better controls than other sectors, including professional services."

He hypothesises that when the Revised Technical Standard as part of the Payment Services Directive (PSD2) comes into place in September 2019, there may be a decrease in the frequency of BEC attacks. Under the directive, payment services providers will be required to comply with requirements for strong customer authentication (SCA) and third party access to bank accounts, which should make it more difficult for fraudsters to steal and divert funds.

Poor password hygiene is a recurring issue for firms targeted by BEC, with cyber-criminals exploiting companies that have not activated their Microsoft Office 365 security functions, where the default settings do not enable all the necessary security features such as multi-factor authentication. This remains a high frequency incident that is reported to AIG's cyber claims team on almost a daily basis, according to Kathy Avery, financial lines major loss adjuster, AIG.

"For businesses affected by BEC, it can be very damaging reputationally," she continues. "There is always a lot of concern from insureds about how they are going to notify their clients. And often they only find out about the compromise because their clients are receiving spoof and phishing emails that appear to be coming from the insured and they have arisen as a result of the compromise."

The security concern around passwords and multifactor authentication is valid, but it remains the case that many simple attacks can be prevented by improving staff awareness of phishing emails and through implementing a clear protocol for dealing with suspect emails.

Financial services is now the second sector responsible for the most cyber claim notifications. Having previously commanded the top spot, it is now responsible for 15% of claims in 2018, down from 18% the previous year. However, the percentages do not reflect the whole story. Total claim notifications from financial services customers in fact nearly doubled between 2017 and 2018, showing the sector is still highly targeted in spite of its more sophisticated approach to cyber risk.

The same is true for hospitality and leisure. While proportionally down from 5% to 4% year-on-year, real claims numbers again nearly doubled in 2018. "We see a lot of loyalty scheme breaches, with hospitality firms and airlines typically affected," says Ball. "Many of the hospitality brands are franchises but they share their member data and often anybody at any hotel in the world can access this membership data."

The Human Factor

Human errors and behavior continue to be a significant driver of cyber claims. Despite encouragement by many organisations, employees often use weak passwords or the same passwords across multiple applications, for instance.

"One household name we insure foiled an attack after they detected a presence in their system," says Kathy Avery. "They decided they should reset all the passwords and asked all employees to adopt new passwords, but found they could not get rid of the intruder because of this password hygiene issue. So they had to do it a second time using randomly-generated passwords for every user and that, finally, succeeded in shutting down access."

In this year's claims statistics, claims notifications for employee negligence doubled from seven percent to 14%. Losses are driven by staff sending out emails containing company data to the wrong individuals or losing laptops and other devices. And under GDPR there has been an increase in notifications for such incidents.

"We're seeing issues such as where attachments to emails are not properly checked before they are sent, and, inadvertently, the sender of what he or she believes is a single confidential personal data record being sent to the relevant data subject, ends up sending out a much larger collection of confidential personal data records of other data subjects," says Jonathan Ball.

Another common error involves Excel spreadsheets. "Too many employees don't understand how Excel works and that, for example, it might be that you can only see certain data on the spreadsheet on your screen, but that's because you've got the filtering button switched on," says Ball. "And then they send the document out without realising that if the recipient goes to the top line and presses 'filter off' another hundred thousand lines of data appear. We recently dealt with quite a big breach incident that occurred in this way for one of the banks."

"You get all sorts of human error still creeping in," he continues. "People are still clicking on phishing emails all the time, despite training. And one of the things that really exacerbates the cost of dealing with incidents, including increasing the need for and costs of notifications to regulators and data subjects, is the use by employees of company email for private matters, particularly private financial matters."

Targeted ransomware on the rise

Ransomware, the leading breach type in 2017 when it was responsible for 26% of notifications, has become marginally less prevalent, causing 18% of cyber claims notifications in 2018. However, as predicted in last year's report, there are a number of instances that show ransomware and extortion type attacks are becoming more targeted, with the attack on Norsk Hydro one of the more high-profile examples.

The Norwegian aluminium smelting giant fell victim to a difficult-to-detect strain of ransomware known as "LockerGoga", through which cyber-criminals gained access to the company's networks in a targeted attack. The company was forced to halt production at a number of plants across Europe and the US and was forced to switch to manual operations as it attempted to contain the issue, causing widespread business interruption (BI) losses.

The decision whether or not to pay a ransomware or extortion demand continues to be influenced by how well an organisation has backed up its data, and the potential business interruption that may ensue. "The impact of ransomware can be very much mitigated if there is good practice with backups," says Avery. "But time and time again we see there are poor procedures."

Meanwhile, the ransom requests have increased in size. While the initial amounts demanded by WannaCry ransomware attackers were between $300 to $600, in 2018 there have been cases where cyber-criminals have requested tens of thousands to millions of dollars.. Meanwhile, the disruption and BI costs associated with such attacks have risen. And in an era of GDPR, there is also the need to establish whether sensitive data has been compromised.

"We've seen a higher incidence of extortion in 2018 and a bigger expense in enabling systems to get back online," says Camillo. "Even if you pay a ransom in order to decrypt your files, it is a very laborious process of double checking that the decryption will work, and then isolating your data to make sure you don't get re-infected and cleaning your files before reinstalling everything. It's very expensive and it's very disruptive as well as being a last resort, where allowable by law."

He anticipates that cyber business interruption claims will continue to be significant going forward, as ransomware and extortion attacks become more targeted, as insureds become more aware of the scope of their cover and as brokers offer more assistance in preparing proof of loss documentation. Some of the larger insurance brokers now employ teams of forensic accountants to help clients prepare their BI claim for submission.

"We anticipate an increase in claims on a global level," says Camillo. "Targeted incidents, such as the attack at Norsk Hydro, could become more of a concern in 2019. The rapid spread of malware or attack of a critical service provider by state-sponsored actors could cause widespread business interruption losses and impact a wide range of industries, potentially also causing significant physical damage."

Claims frequency and the GDPR effect

There has been a pronounced "GDPR effect" on the overall claims frequency in 2018, with a spike in notifications following implementation of the EU General Data Protection Regulation in May 2018. The provisions of the new rules, including strict breach notification guidelines, is resulting in timely notifications from clients.

"There is a very strict time limit, particularly for notifying the regulator, and the effect of that is an increase in initial costs," says Avery. "Under our policy, we have a 48 or 72-hour period where we pick up the initial costs, and we're seeing an impact on the amount we're paying out early doors as a result of GDPR. In addition, the legal forensic and IT costs have also increased, which is leading to bigger payouts under the policy."

Just under 20% of AIG's claims received in 2018 included a notification under the GDPR, with the adjusting costs significantly higher in comparison to claims where there was no data breach notification. Pay-outs from our First Response hotline have increased by over 50% for claims where data subjects and/or the data authority were notified, with insureds receiving legal advice and assistance in preparing their regulatory notices.

"We're seeing a lot of work for our firm, and obviously increased fees incurred by the insured and/or by the insurer, in managing GDPR issues for breaches that are really quite minor," says Norton Rose Fulbright's Jonathan Ball. "The kind of incidents that pre-GDPR an organisation would probably have dealt with themselves without external legal counsel."

Within Europe there is a clear north/south divide when it comes to GDPR data breach notifications, with northern Europe responsible for the vast majority of notifications, suggesting a difference in compliance culture. For example, where in Ireland 48% of the claims reported resulted in notification to a regulator, less than 10% of claims reported in Spain were notified. GDPR may also apply to clients based in jurisdictions outside of Europe. This is borne out by an increase in notifications from the Middle East and Africa region, where there has been more claims activity over the past 12 months.

Breaking down AIG's cyber claims statistics by region, it shows there have been significant increases in notifications coming from Belgium, the Netherlands, Germany, France and Ireland over the past 12 months while claims from Sweden and Greece have also grown.

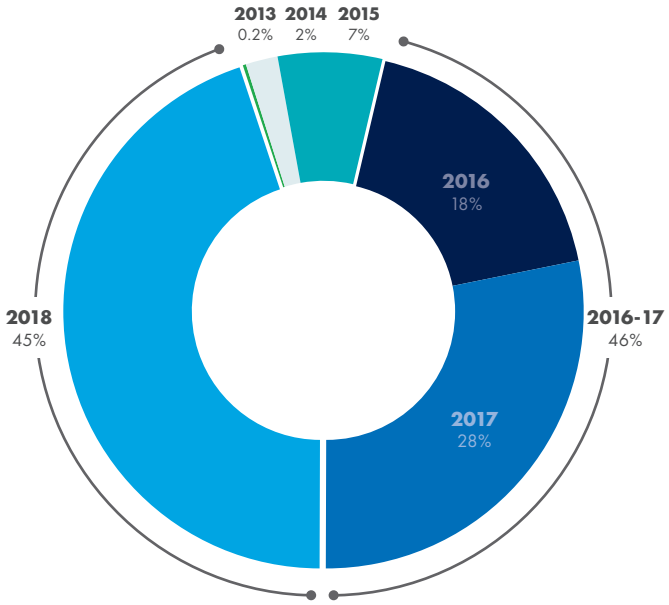
Looking Forward: Move towards affirmative cover

The long-term trend of increasing claims frequency has continued in 2018 as it did over the previous five years, reflecting both the growth and maturity of AIG's cyber book of business as well as the increasing sophistication of buyers and knowledge of the scope of the product. As cyber becomes a growing exposure for many organisations, based on our claims experience anticipated losses will continue to grow in both frequency and severity across different industries.

Camillo notes a continued move towards affirmative coverage by clients keen to ensure that their policies respond as anticipated. "There have been some misperceptions recently in the press about cyber coverage, following disputes over war exclusions in property and K&R policies, with the suggestion that cyber products may also be limited in scope, which is simply not true."

"What our claims numbers clearly show is that more people are buying the coverage and the product is paying out," he continues. "It includes very broad and flexible coverage and it is very easy to notify us about an event through the hotline. Clients are showing a preference for affirmative cyber cover, which will indemnify them against a wide range of losses, including privacy events, cyber extortion and broad network business interruption coverage including outsourced service providers and system failure."

Fig 3 **Cyber Claims Received by AIG EMEA (2013-2018) - Volume**



Claims case studies

Manufacturer pays €25,000 ransom after suffering business interruption

An attack on the IT systems of the insured took place through a malicious program of the ransomware type known as "Detractor". Three servers of the infrastructure were affected, which were encrypted, leading to encryption of the folders. The available back-ups, which were on a different server, were deleted (presumably by the cyber-criminals). Therefore, the affected systems could not be restored through the back-ups.

Simultaneously, the attackers demanded that the insured pay a ransom in order to decrypt the system. The insured's operation had ground to a halt as a result of not being able to restore the affected systems. It could not deliver shipments or receive materials and was not able to make payments or to collect accounts receivables.

The aim of the ransomware was not to steal information and there had not been a breach of personal information. On Event Day 10 therefore, the insured paid a ransom of €25,000 in BitCoin and was able to restore its operations. AIG covered the cost of the ransom, incident response costs and the extensive network interruption, which included an increased cost of working and cancelled orders.

Email account compromised at Financial Services Intermediary

The insured, an SME professional services firm, was alerted to a cyber incident after receiving notifications from various clients who had received a suspicious email from an employee of the firm. The email contained various links and attached a PDF invoice requesting payment from the recipients.

Upon initial investigation it was determined that the employee's email account had been compromised and a phishing email containing an attached invoice had been sent to 5,500 email addresses. The insured was proactive in taking corrective action regarding the phishing email, notifying the 720 email contacts of the compromised account, urging them not to click on the attachment PDF. The passwords of both the compromised email account and those belonging to other employees in the firm were changed.

AIG recommended the insured notified the ICO as a matter of caution, despite the fact the only identifiable information from the phishing emails was the recipients' names and places of work. The recommendation to notify was partly driven by the nature of the firm's business, including sale of cyber insurance products, and reputational considerations.

Breached network at Middle East-based global energy and logistics firm

Late last year the insured suffered a number of brute force attacks on their network infrastructure, which resulted in the cyber-criminals gaining access to their network, most likely via their Office 365 email cloud host although the specific method of intrusion is still under investigation. The insured's network comprises roughly 5,000 end point devices and, following discovery, an initial sweep identified approximately 2,900 units that may have been compromised. As a result, all users were forced to change their passwords and, subsequently, two-factor authentication was introduced.

The insured engaged with AIG's service providers under the policy's First Response 72-hour cover period. Due to government restrictions, the insured was unable to allow their data to be handled outside of the country and therefore IT forensics were initially restricted to providing advice by telephone and email. But AIG was able to provide a local IT forensics team to carry out investigations on site, alongside the insured and their cyber-security advisors.

The initial focus was to identify access points and ensure these were closed to the cyber-criminals. As a result of identification of the compromised access points, along with network traffic analysis, it was possible to identify how the attackers had gained access to user accounts. It was also identified that the attackers had potentially gained access to user email accounts and in excess of 2,000 files containing personal data, alongside confidential company data including tenders, project details and financials.

Over six months later investigations into a potential compromise to Office 365 email accounts remains ongoing as does the examination and analysis of compromised data. Costs are still being incurred and to date exceed $300,000.

Retailer hit by ransomware and business interruption

The insured is an international retailer with over 100 stores and an online presence. Whilst they were undertaking some changes to their IT systems and data storage they suffered what appeared to be a targeted, sophisticated cyber attack which encrypted all their files, including those held in the cloud. The cyber-criminals demanded a ransom for providing a decryption code.

AIG immediately appointed forensic IT specialists who were onsite non-stop for long periods, initially working to secure the system and attempting to retrieve unencrypted data. This proved very difficult and was not achievable in a timescale to allow resumption of normal business. The shops were still able to trade using manual tills but the attack left them unable to replenish stock in stores or process online orders, which led to a major business interruption.

Although reluctant to engage with the cyber criminals, after a prolonged period of being unable to fully trade the insured decided to pay the ransom demand ($150,000 in Bitcoin). AIG assisted the insured in sourcing Bitcoin. After the ransom was paid the decryption code was provided but all files had to be manually decrypted using the code, a painstaking and costly process in terms of labour, which was paid for by AIG.

AIG also covered the cost of additional fees to the insured's various existing software providers for additional support and equipment to facilitate the decryption process. The insured held only £1M of cover, which proved inadequate and the policy limit was paid to the insured when interim business interruption losses exceeded £550,000. IT forensic fees alone exceeded £500,000. On this occasion there was no evidence any personal data was accessed or extracted, but legal and IT advice to determine this was covered under the policy.

CLAIMS FIRST

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

José Martinez
VP, Financial Lines
Major Loss Claims, EMEA
Tel: +34 91 5677 431
jose.martinez@aig.com

GBL00003595 0519