

# Business, interrupted



Business interruption costs due to cyber events have risen sharply over the years as criminals become more sophisticated. Consequently, related claims will continue to increase as ransomware and extortion attacks become more targeted, says **Mr James Hebert of AIG.**



Cyber is an often-used word – and one with many different interpretations. AIG considers cyber, or more specifically, a cyber attack as an event that attempts to damage, disrupt or gain unauthorised access to an electronic communications network, computer or computer system. These events can be wide ranging, as can their effects.

To combat these risks, companies should implement or improve basic IT hygiene guidelines and best practices. Developing a cyber security programme is a journey for organisations. Cyber security management tends to be limited by the company's current resources as well as the available capital it has to invest in improving its risk profile. Organisations need to give priority to areas that give the best 'returns' on reducing their risk exposure. Some of these include the application of appropriate software, firewalls and employee training.

In addition to the aforementioned, a complementary solution to a company's cyber security programme is a cyber response and liability insurance policy. This contract should include first-party insurance – ideally with a first-response provision and timed, unlimited liability and nil deductible/excess that creates legal privilege, and third-party cover. The structure and additional clauses of such a policy can be discussed with a specialised broker to meet a company's specific insurance requirements. Unfortunately, often the importance of the above approach is only brought to the fore after a cyber event.

## Disturbing trends

AIG has been writing cyber liability insurance since the mid to late 1990s and has vast experience in receiving and successfully handling the attributable claims. It conducted an analysis of 1,100 cyber claims notified in the EMEA

**The ransom amounts have increased in size over the years. While the amounts demanded in respect of the ‘WannaCry’ ransomware attacks were in the region of \$300 to \$600, there have recently been cases where cyber criminals have demanded tens of thousands to millions of dollars.**

region between 2013 and 2018, and continues to generate an annual claims report to review the notifications received and conservatively predict new and emerging events.

For instance, its 2019 report notes that business email compromise (BEC) has overtaken ransomware and data breach by hackers as the main contributor to AIG EMEA cyber claims. Nearly 25% of reported incidents in 2018 were due to BEC, up significantly from 11% in 2017. Ransomware, data breach by hackers and data breach due to employee negligence were the other main types of cyber incidents in 2018.

BEC is a ‘new’ category that has emerged recently given the high number of specific BEC-related claims received by AIG over the past 12 months. Previously, such attacks fell within the scope of ‘other security failure/unauthorised access’.

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

The perpetrator is then able to send and receive emails from the victim’s email address and access all information in their email inbox. In many cases, the BEC is exacerbated by malware that spreads the scam to contacts in the victim’s inbox. In this relatively simple type of scam, BEC attackers often target individuals responsible for sending payments, using spoof accounts to impersonate the company’s C-suite or a supplier and requesting money transfers, tax records or other sensitive data. These cases are similar to the fake president fraud and social engineering claims still seen today, although the modus operandi for BEC events is subtly different and more effective. Hence, they are often successful especially in the region.

### Mitigating BEC incidents

Essentially two mitigation steps can be implemented to combat BEC. First, greater investment in cyber insurance is needed in many businesses. Second, there

is need for a structured and targeted approach to training employees in cyber risk awareness, including how to identify rogue email.

For covered BEC and impersonation fraud claims, the cyber policy should provide for the cost of an IT forensic investigation to determine whether the insured’s system was compromised, the extent of the breach and what kind of data was compromised. The policy should also provide legal advice on reporting and notification obligations to data subjects and regulators. The cover for any direct financial loss (misappropriation of funds) due to criminal activity is often restricted.


### Targeted ransomware

Another prominent type of cyber breach in recent years is ransomware, which has become marginally less prevalent, falling from 18% in reported incidents in 2018 from 26% in 2017. Nevertheless, as predicted for 2019 and beyond, there are a number of instances that show ransomware and extortion type attacks becoming more targeted, with the attack on Norsk Hydro matter being 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, in turn, forced to revert 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 is typically determined by how well an organisation has backed up its data and of course, the potential BI that may ensue. We regularly witness poor procedures in place.

The ransom amounts have increased in size over the years. While the amounts demanded in respect of the ‘WannaCry’ ransomware attacks were in the region of \$300 to \$600, there have recently been cases where cyber criminals have demanded tens of thousands to millions of dollars. Meanwhile, the disruption and BI costs associated with such attacks have risen sharply. This trend is likely to continue in the next couple of years. It is worth noting that even after an insured pays a ransom to decrypt their files, there ensues a very laborious process of double checking that the decryption will work, and then isolating data to ensure re-infection does not occur and thereafter cleaning files before reinstalling everything. This process is very expensive and disruptive with potential legal/regulatory implications.

AIG anticipates an increase in cyber claims on both the global and regional levels. BI claims especially will continue to be significant, as ransomware and extortion attacks become more targeted. Considering the geopolitical make-up of the world today, it can be deduced that the rapid spread of malware or attack of critical service provider by state-sponsored actors could cause widespread BI losses and impact a wide range of industries, potentially also causing physical damage. 

Mr James Hebert is head of financial lines, MENA at AIG.