# Cyber: Taking cover


**Celso De Azevedo, 36 Commercial, reports on the latest trends in cyber insurance post-COVID-19**

IN BRIEF

- Cyber security in 2020: the worst year to date?
- Cyber insurance industry: challenged to its limits.
- Regulatory developments.

In April 2020, the Federal Bureau of Investigation commented that daily cyber security complaints to its Internet Crime Complaint Center had increased by 400% since the onset of the coronavirus (COVID-19) pandemic (*zd.net/3kJqKlC*).

Such an unprecedented increase in cyber losses is reflected in the findings of Hiscox's recent Cyber Readiness Report. The insurer surveyed over 5,500 private and public sector organisations located internationally, between December 2019 and February 2020, and found a six-fold increase in the median value, and a 50% increase in the total amount, of cyber losses in the early months of 2020. In addition, more than 6% of the companies surveyed had paid a ransom in this period ('Hiscox Cyber Readiness Report 2020': *bit.ly/3nz2swt*). Another survey—'The Beazley Breach Insight Report 2020'—noted a 25% increase in incidents involving ransomware in Q1 of 2020 as compared with Q4 of 2019 (*bit.ly/3pJ511c*).

Meanwhile cyber security experts have reported that the average ransom payment in Q3 of 2020 is US$233,817, which is an increase of 31% from Q2 ('The Coveware Quarterly Ransomware Report Q3 of 2020': *bit.ly/36QyxJL*). Further, almost half of ransomware attacks have threatened to release exfiltrated data in addition to encrypting the victim's data. Email phishing remained the most significant attack vector for larger organisations, but for smaller companies of less than 1,000 employees, over 55% of ransomware cases resulted from the exploitation of improperly secured Remote Desktop Protocol (RDP) services.

During the COVID-19 crisis, RDP attacks, followed closely by phishing attacks, have become the most frequent attack vectors used by cyber criminals to install ransomware on IT systems worldwide. RDP attack attempts are reported to have increased by 140% in Q3 of 2020 as compared with Q2 ('ESET Threat Report Q3 2020': *bit.ly/36Jnsdq*). Brute-force RDP attacks have greatly increased in frequency during 2020. Criminals use port-scanning software tools to survey the entirety of the internet in order to identify exposed RDP ports. Thereafter, brute-force software is systematically deployed to log in to these ports to gain administrator access to the system and deploy malware.

However, RDP compromise has risen not only due to improperly secured credentials but, more critically, also from Common Vulnerabilities and Exposures (CVEs). The most exploited CVEs between 2016-2019 and during 2020 are well-known and have been published by the US-CERT (the 'United States Computer Emergency Readiness Team') together with a detailed list of 'Mitigations for Vulnerabilities Exploited in 2020' (*bit.ly/3feEa8m*).

Keeping up with such ever-growing lists of vulnerabilities in widely used software products, as well as constantly installing suggested security patches (mitigations), have become onerous and complex tasks for most SMEs. There is a dawning realisation that SMEs are involved in a losing battle against cyber-attacks in the remote working environment.

A recent report from cyber security firm Bitdefender has concluded that 2020 could be the worst year in cyber security history (*bit.ly/3pI9u3V*). Cyber security experts are concerned that the typical attack vectors which have been observed during the COVID-19 crisis are so severe and difficult to mitigate for most SMEs that ransomware payments will continue to grow in 2021.

The cyber security industry has yet to rise to the challenge and offer businesses more effective cyber security solutions against well-known cyber threats. As a result, class action litigation in the US (and similarly in the UK) against software manufacturers who offer products with known cyber security vulnerabilities may also increase in the future.

## Cyber insurance

As a result of the increase in cyber-attacks in 2020, the cyber insurance industry will be challenged to its limits to continue to provide the same extent of insurance coverage in the coming months and years.

At present, cyber insurance coverage broadly encompasses:

- First Party Coverage: (a) data recovery and software repair; (b) privacy breach management; (c) regulatory investigation; and (d) business interruption.
- Third Party Coverage: (a) data privacy liability; (b) network security liability; and (c) media liability.
- Cyber Crime Coverage: (a) cyber extortion; (b) fraudulent transfer of funds; (c) social engineering; and (d) corporate identity theft.

Beyond 2020, the big question will be whether the COVID-19 crisis will result in a further increase in sales of cyber insurance or whether the opposite may occur.

Cyber insurance growth may stall due to the expected premium increase for cyber insurance policies. As a reaction to the current cyber security predicament, premium increases for cyber insurance are becoming more common. It has been reported that cyber insurers may increase their premium rates by 10%-15% in the future (*bit.ly/3lHtrWp*).

Broader exclusions and lower sub-limits are also being imposed by many cyber insurers. Nevertheless, this gloomy picture of the future of the cyber insurance industry is by no means certain. The same increase in cyber-attacks has been reported to have generated a 340% increase in the sales of cyber policies in April 2020 as compared with the same period last year (*bit.ly/3pGYN1y*).

However, as known security weaknesses are increasingly exploited by criminals, some insurers have been restricting coverage on the basis of exclusions relating to failures to keep security software updated regularly or to obtain adequate cyber security software.

Exclusions relating to negligent acts of senior officers are also being used by some insurers to target alleged failures to adopt adequate cyber security measures by corporate policyholders.

Some of these exclusions are controversial as they deal with the very essence of the type of cyber insurance coverage being sold by underwriters.

Exclusions and sub-limits are also becoming more common in relation to coverage for social engineering attacks that

result in data privacy claims or fraudulent transfer of funds losses. Some cyber policies require that coverage for social engineering attacks must be conditional on a network failure.

The preparatory declaration, application forms or placement questionnaires that must be completed by policyholders in order to obtain insurance have also become more detailed in terms of the information required about the cyber security systems and other security measures that businesses have put in place. In a hardening market, the answers provided by policyholders may be used by insurers to deny claims based on non-disclosure or misrepresentation relating to the policyholders' duty under the UK's Insurance Act 2015 to make a fair presentation of the risk to the insurer.

In a different jurisdictional context, but exemplifying this problem, in the US case of *Columbia Casualty Co v Cottage Health System* (No. 2:15-cv-03432 (CD Cal) (filed 7 May 2015)), the insurer denied coverage under its cyber insurance policy, 'NetProtect360', in respect of a claim for payment of defence costs and settlement of a data breach class action lawsuit in the US against Cottage, the insured.

The underlying data breach lawsuit against Cottage arose out of a disclosure to the public, via the internet, of confidential medical records of approximately 32,500 hospital patients that were stored on Cottage's servers.

The insurer denied coverage on the ground that Cottage had triggered a policy exclusion relating to 'Failure to Follow Minimum Required Practices' involving 'procedures and risk controls identified in the Insured's application' to 'regularly check and maintain security patches on its systems' and to 'enhance risk controls'.

The insurer alleged that Cottage had failed to change the default settings of its File Transfer Protocol so that its web servers would not permit access to patient records via Google's search engine.

Relying on these alleged failures to mitigate risk, the insurer also argued that the insured's application form relating to the insurance policy contained a misrepresentation that materially affected the acceptance of the risk and, therefore, rendered the policy 'null and void'.

Although in this case the judge dismissed the claim on the ground that the ADR provision in the policy had not been followed by the insurer, the case is a timely reminder that insurers are willing to deny coverage by relying on policy terms (and preparatory declarations by the policyholder) that impose a duty on the policyholder to continuously update its cyber security systems.

There have been no reported cases in the English Courts relating to cyber insurance coverage disputes, but this is not surprising in view of the low policy limits being offered to SMEs and the low penetration rate of 12.7% among SMEs based in the UK in 2020 ('GlobalData's 2020 UK SME Insurance Survey': *bit.ly/36M4W3R*).

However, the UK's Financial Ombudsman Service, which deals with complaints against insurers, is likely to see an increase in complaints from individual customers and some small businesses arising from non-payment by cyber insurers based on allegations that policyholders have failed to update cyber security measures.

In these disputes, underwriters may struggle to succeed in arguing that a policyholder has failed to take adequate cyber security measures where the cyber security software contains inherent vulnerabilities that are unknown to the policyholder or too complex to be effectively patched.

## Regulatory developments

Due to the increase in the number of ransomware incidents affecting businesses, cyber security operators and the cyber insurance industry as a whole, the US regulatory authorities have decided to intervene.

On 1 October 2020, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN) issued separate 'advisories' to provide guidance to 'U.S. individuals and businesses in efforts to combat ransomware scams and attacks'.

OFAC's advisory warns that any ransomware payment is illegal if it is made to a sanctioned entity under its Specially Designated Nationals list, which includes ransomware operators. OFAC also refers to its Sanctions Enforcement Guidelines for financial institutions and companies, which include those involved in providing cyber insurance, digital forensics and incident response, as well as financial services. These guidelines require that such service providers must also adopt a risk-based compliance programme to mitigate exposure to sanctions-related risks.

Similarly, FinCEN's advisory warns that ransomware payments in any convertible virtual currency (CVC) may violate anti-money laundering legislation. The advisory reiterates that financial institutions must file a Suspicious Activity Report (SAR) in relation to any ransom payments made through them. The SAR must include and take account of broad 'red flags' such as:

- when the customer discloses the relationship of the payment to a ransomware incident; or
- where the CVC exchange trader is associated with ransomware activities according to public or government sources.

As a result, financial institutions (and other regulated entities) may have to file SARs in relation to most transactions involving CVC exchange traders so as to comply with these latest guidelines. The next few months will indicate whether these stricter guidelines will result in a reduction in ransomware payments in the US and whether other countries will follow the US government's example to tackle the problem.

In the UK, where there is any knowledge or suspicion of money laundering and terrorism financing, a SAR must be filed with the National Crime Agency pursuant to Pt 7 of the Proceeds of Crime Act 2002 and Pt 3 of the Terrorism Act 2000 (respectively). Moreover, under the UK's Terrorism Act 2000, any ransom payment is unlawful if the payer knew or 'had reasonable cause to suspect' that the funds may be used for the purposes of terrorism. Even partial financing for the purposes of terrorism, defined as any 'political, religious or ideological purpose', would suffice for a ransomware payment to be unlawful.

It is problematic for anyone who may wish to make a ransomware payment to avoid criminal liability. In the UK there are currently 76 proscribed organisations listed under the Terrorism Act, and another 14 under previous legislation (*bit.ly/3nETUnN*). There are also other, constantly updated, lists of designated persons who are subject to sanctions for 'believed involvement in terrorist activity' (*bit.ly/3nASTNL*).

Separate terrorism and sanctions lists are also issued by the EU and other countries. Since the UK's Terrorism Act is not restricted to suspected terrorist organisations listed only by the UK government, any other international list may also be taken into account. In addition, the latest anti-money laundering regulations in force in the UK are the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017), which implemented the EU's 4th Directive on Money Laundering.

The MLR 2017 provide that, in determining the potential risk exposure to money laundering or terrorist financing, a 'relevant person' must prepare a written risk assessment report that takes into account a list of factors, including the nature, scale and complexity of its business; its customers; geographic areas of operation; its products or services; its transactions; and its delivery channels.

In view of the broad basis of the considerations imposed by the MLR 2017, it is likely that the recent US government's guidance advisories will have an impact on

UK businesses' SAR notification duties, even if such businesses do not operate in the US or are not subject to US regulations.

## Recovering ransomware payments

Reported in January 2020, the English High Court case *of AA v Persons Unknown and* others [2019] EWHC 3556 (Comm), [2020] 2 All ER (Comm) 704 signalled the upward trend in ransomware attacks. In this case, the hackers wanted to conceal their ransomware gains by receiving payment in Bitcoins from the victim, a Canadian insurance company, which was insured under a cyber insurance policy issued by an English insurer (AA).

In October 2019, the hackers installed malware, called BitPaymer, which infected over 1,000 computers and 20 servers of the Canadian company, and demanded payment of US$950,000 in Bitcoins to release a decryption tool to restore their victim's IT systems.

Cyber investigation specialists traced some 96 Bitcoins, worth around US$800,000, to a cryptocurrency exchange, Bitfinex, operated by two British Virgin Islands companies.

The significance of the decision of the High Court is that the English insurer company, having paid the ransom in Bitcoins on behalf of its Canadian insured, succeeded in obtaining a proprietary injunction over the cryptocurrency. By issuing the injunction, the English High Court held that cryptocurrencies were capable of being considered 'property' under English law. In its decision, the court adopted the analysis set out in the 'Legal statement on cryptoassets and smart contracts' published by the UK Jurisdiction Task Force.

More broadly, this case illustrates the novel issues that will need to be considered by the courts in relation to cryptocurrency payments for ransomware, which are likely to become more frequent in the coming years.

> *"The shift to remote working practices has exposed the limitations and inadequacies of benchmark cyber security protocols"*

## Comment

This past year has witnessed a dramatic rise in ransomware attacks due to the remote working practices imposed by the COVID-19 crisis. This has resulted in a huge transfer of economic activity to web based remote vehicles without adequate cyber security protocols to deal with the new challenges of such an enormous task.

This shift to remote working practices has evidently exposed the limitations and inadequacies of benchmark cyber security protocols that had been previously adopted by businesses worldwide.

However, at present, the steep learning curve for cyber security software developers, experts and the cyber insurance industry has not reached its peak. In the dynamic and changing world of remote working, there have been continuous and ever-increasing demands of all those who operate in this new environment. The coming year will see the next chapter in the remote working experiment, which affects us all, unfold. **NLJ**

**Celso De Azevedo** is an international re/insurance and commercial dispute resolution lawyer, 36 Commercial (*https://36group.co.uk/commercial*).