COMBATING THE RANSOMWARE ONSLAUGHT

By Ray Irving

Cyber insurance has emerged as a key bone of contention in the rapidly evolving cyberthreat space.

In the last few months, we have seen large-scale, high-profile ransomware attacks in the Asia-Pacific (APAC) region, including on large insurers and tech companies. These come on the heels of multiple ransomware attacks around the world, including on IT firm Kaseya as well as Colonial Pipeline and meat supplier JBS in the US. Ransomware is a growing threat due to the wide availability of ransomware kits (known as Ransomware-as-a-Service) that non-tech-savvy criminals can easily obtain, as well as the rise of cryptocurrencies as cross-border payment methods that are difficult to track.

While the rise in ransomware started in 2020, this year has seen an even bigger surge. Attacks rose 93% year-on-year, according to Check Point. While much of the activity centres on the US, Europe, and Latin America, APAC financial institutions must still be prepared as they too are in the crosshairs.

Ransomware criminals, knowing that many firms would rather their **INSURERS PAY QUICKLY AND QUIETLY TO AVOID OPERATIONAL DISRUPTION AND REPUTATIONAL DAMAGE**, have increased their demands substantially. Ransomware gangs such as Ryuk have publicly stated that they specifically target firms with cyber insurance.

According to Kaspersky, 635 (35%) out of 1,764 companies and individuals attacked in 2020 by REvil – a major Russian-based ransomware group – were from the APAC region.

CYBER INSURANCE: IN THE EYE OF THE STORM

Insurers are especially juicy targets for cybercriminals because of the possibility of also accessing customer data, including around limits for cyber insurance policies. Cyber insurance has been on the rise over the last several years, but the explosion of ransomware has meant that many firms turn to their policies to pay out ransoms rather than look for alternative methods of dealing with an attack. Ransomware criminals, knowing that many firms would rather their insurers pay quickly and quietly to avoid operational disruption and reputational damage, have increased their demands substantially. Ransomware gangs such as Ryuk have publicly stated that they specifically target firms with cyber insurance.

As more firms and institutions rely on cyber insurance to insulate themselves from cyber risk, opportunistic cybercriminals have quickly realised that cyber insurers are now attractive targets themselves. By hacking and accessing an insurance company's policy data, cybercriminals can curate a list of ransom demands according to each victim's policy and business profile. They can therefore multiply their return on investment for one attack by targeting both the insurer and their customers.

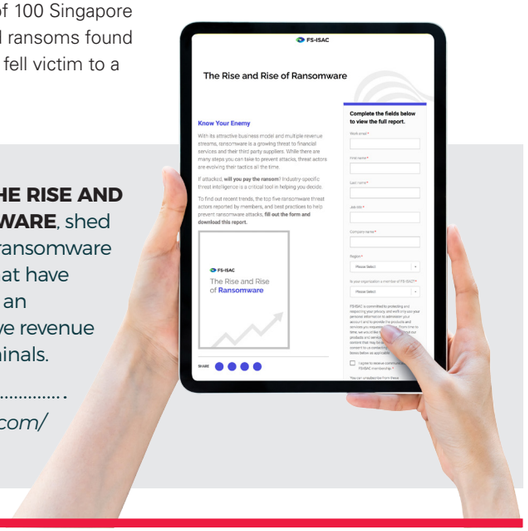
Cyber insurers have responded by increasing their premiums, tightening coverage terms, introducing ransomware payout limits, and adding clauses that remove liability for attacks by nation-states. Some insurers are ceasing cyber insurance completely, which could have a knock-on effect on victims' willingness to pay ransoms and, in turn, the revenue of ransomware groups. This has not gone unnoticed by cybercriminals. In fact, one large insurer was a victim of ransomware just days after announcing its cyber insurance policies would no longer cover ransomware payments.

Cyber insurers are now also scrutinising policyholders' cyber resilience strategies and systems more closely than ever and may deny cyber insurance to firms seen to have lax cybersecurity. As such, many firms are beginning to recognise that they must invest significantly in their cybersecurity and defence capabilities.

TO PAY OR NOT TO PAY

While law enforcement agencies across many jurisdictions strongly recommend against paying ransoms, firms may choose to pay to minimise disruption as well as monetary and reputational losses. However, they should bear in mind that paying ransoms reaffirm the viability of ransomware as a business model. Indeed, it may not pay to pay – a 2021 survey of 100 Singapore companies that had paid ransoms found that 25% of these firms fell victim to a second ransomware attack by the same threat actor group that perpetrated the first. Additionally, 28% of the surveyed firms reported that some or all of the recovered data had been corrupted. Paying the ransom can also lead to legal consequences for the victim organisation if the threat actor is a sanctioned entity, as can often be the case with ransomware attackers.

Our 2020 report, *The Rise and Rise of Ransomware*, shed light on emerging ransomware business models that have made ransomware an increasingly lucrative revenue driver for cybercriminals. In it, we stated that even the largest financial institutions equipped with the most robust cybersecurity systems are not impervious to ransomware attacks, especially on third-party vendors. That has been shown to be true in 2021, and we expect that ransomware attacks targeting the supply chain will continue. As many financial firms around the world use the same vendors, the industry faces an additional challenge of concentration risk, where an attack on a major supplier could impact multiple institutions.



Our 2020 report, **THE RISE AND RISE OF RANSOMWARE**, shed light on emerging ransomware business models that have made ransomware an increasingly lucrative revenue driver for cybercriminals.

https://www.fsisac.com/ransomware

BE PROACTIVE, BUT PREPARE FOR THE WORST

To avoid becoming a victim of ransomware, employ a multidimensional and pragmatic approach towards cyber risk. This means having protocols in place for worst-case scenarios, while simultaneously taking proactive measures aimed at prevention and risk minimisation. To this end, firms should:

+ Utilise a data vault: Savvy ransomware attackers are known to lock up and/or exfiltrate data backups before making ransom demands. Firms should invest in a data vault that is not connected to the main systems or backups. By safekeeping critical data offline, firms can not only ensure that disruption and losses are kept to a minimum, but also retain valuable leverage during ransom negotiations.

+ Share threat intelligence: As ransomware attackers often target victims on multiple continents, financial firms should participate in global intelligence sharing, as well as in smaller communities that focus on industry verticals and/or regions of operation. Intelligence sharing can not only help firms build pre-emptive defences against specific attacks but can also help victims understand the modus operandi of ransomware attackers, such as whether they are likely to decrypt data upon payment or post the data publicly.

+ Reinforce existing defences: This includes fortifying end points, focusing on email security, upskilling staff to minimise human error and securing networks. Firms must also ensure senior management and boards position cybersecurity as a top priority to secure sufficient investment.

+ Strengthen third-party risk management: Maximise cybersecurity on the firm's side of all interactions with third parties, minimising the chances that third-party vulnerabilities impact systems and data. Systematically review documentation, processes, security protocols, and personnel related to or used by suppliers. Consider employing external risk monitoring services to assist in evaluating the internet-facing risk posture of vendors.

Financial firms should participate in global intelligence sharing, as well as in smaller communities that focus on industry verticals and/or regions of operation. Intelligence sharing can not only help firms build **PRE-EMPTIVE DEFENCES AGAINST SPECIFIC ATTACKS** but can also help victims understand the modus operandi of ransomware attackers.

RANSOMWARE: HERE TO STAY AND CONSTANTLY EVOLVING

With ransomware accounting for an increasingly large proportion of cybercrime, ransomware is now a grave and immediate threat to financial institutions in the region. While firms must ensure that their defences are effective every second of the day, a cybercriminal group only must get lucky once. Firms should take immediate steps to safeguard themselves from ransomware, as it shows no signs of abating. ✱

■ *Ray Irving is the Managing Director, Global Business Services, at the Financial Services Information Sharing and Analysis Center (FS-ISAC), the only global cyber intelligence sharing community solely focused on financial services. He is responsible for expanding FS-ISAC's membership and service maturity around the world and leads the development of key strategic partnerships and member events. Serving financial institutions and in turn their customers, FS-ISAC leverages its intelligence platform, resiliency resources, and a trusted peer-to-peer network of experts to anticipate, mitigate and respond to cyber threats. Earlier in his career, Ray spent five years at UBS as head of security programmes where he managed the information security portfolio of over 30 IT security projects. During his 12 years in the financial services sector working for UBS, Citibank, and Lombard Odier, Ray has led projects and programmes covering all aspects of information security, including cyber threat management, data protection, security monitoring, and identity and vulnerability management.*