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 may increase their premiums, tightening measures aimed at prevention and risk minimisation. To this end, firms should:

- **Utilise a data vault:** Savvy ransomware attackers are known to look 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.

**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 FS-ISAC is 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.

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.