Businesses should beat cyber crime through intelligence sharing

FRI, MAY 29, 2020 - 5:50 AM

BRIAN HANSEN

AS FINANCIAL services evolve to deliver more convenient, faster and frictionless services to users, the attack surface of the industry grows exponentially - and with it, the risks of cyber crime. While cyber crime is a competitive business, attackers rarely work alone. We must learn from our adversaries - and share intelligence on them, the way they do on us.

The International Data Corporation (IDC) estimated in its Worldwide Security Forecast that global spending on security would reach US$151 billion by 2023. But with the paradigm shift of not only customers but also employees going virtual nearly overnight because of Covid-19, cyber criminals are taking advantage of new opportunities, so that spending may need to increase substantially.

Financial services around the globe are now primarily functioning with employees working outside of the traditional office to reduce the threat from Covid-19. This dispersed workforce provides cyber criminals increased opportunities to target staff and company data. Financial institutions, large and small, now have proprietary corporate data accessed from non-secure environments, which may not have the same level of firewall and security as the normal in-office setup.

In addition, the rapid change in working conditions and increased reliance on virtual communications is, in itself, another vulnerability. For example, in early April, one of our member institutions reported that Covid-19-related phishing against their Hong Kong staff alone increased 437 per cent in two weeks. These were not mass-produced or industrial phishing attempts, but tailored and very legitimate-looking emails.

Cyber criminals are taking advantage of customers too. From January to the first week of April, more than 98,000 high-risk domains were created with a Covid-19 theme since the outbreak started, reported DomainTools. FS-ISAC reviewed these and found more than 1,500 financially-themed domains, including domains pretending to be banks, offering coronavirus-related credit, loans, insurance and more. The bulk of the domains were created in March.

SEE ALSO
Cybersecurity firm Sygnia opens Asia-Pacific HQ in Singapore

By the second week of April, the numbers of new high-risk domains were down 92 per cent, following a crackdown by domain registrars. This shows how quickly the threats are evolving and changing, and the speed with which cyber criminals exploit a vulnerability and then change tactics once defences are built.

A NEW ERA OF CRIME

Of course, cyber threats unrelated to Covid-19 continue. Singapore experienced the highest percentage of ransomware detections in the Asean region last year, with ransomware making up 15 per cent of all attacks across all sectors. This year, such attacks will continue to grow in scale and evolve into different, more targeted variants. Threat actors will continue to improve their ability to craft socially-engineered attacks through open-source intelligence (Osint) gathering. There is also growing evidence that cyber criminals in the region are enhancing the obfuscation of malware, to improve the chances of it going undetected.

Even as ransomware grows more sophisticated, it is also being commoditised; any would-be cyber criminal can go onto the dark web and buy a ransomware service or a kit made by a professional. This professionalisation extends to the networks cyber criminals build to execute highly-complex operations, with diverse functions that resemble legitimate companies. Cyber-criminal networks often have organisational roles like chief executive officers, recruiters and even customer-service agents who guide victims through how to pay them to recover their stolen files and data. Many of the world's most complex hacks demonstrate tight co-ordination across multiple platforms and markets from players who have built trusted relationships.

Now, more than ever, the only way to stay ahead of these sophisticated criminal networks is for us to work together as well. In financial services, this is especially crucial, since large-scale attacks on multiple institutions could damage overall trust in the financial system and impact everyone, not just one or two firms.

This is where organisations like information-sharing and analysis centres (Isacs) come in. They enable communities, industries and sectors to overcome the challenges posed by intelligence sharing. Using a trust model such as the Traffic Light Protocol - a set of guidelines that dictate with whom information can be shared - as well as a set of operating rules, a secure member portal and small circles of trust created for specific communities within given sectors and regions, Isacs creates a trusted platform where organisations can freely share intelligence with their peers, without fear of leaks.

STRONGER TOGETHER

Of course, intelligence sharing, particularly among competitors, comes with its hurdles, and some firms may be hesitant to share critical information that can put them at risk. But the reality is that the faster the intelligence is shared, the more likely it is that other institutions will be able to put up defences to stop the same attack from hitting them. This makes cyber attacks much more expensive for the cyber criminals, since they must start again with each attack instead of using the same strategies and infrastructure on many victims.

FS-ISAC enables intelligence sharing across the global financial services industry. Since opening our office in Singapore in 2017, we have grown to serve financial institutions across the region. This enables sharing of locally relevant threat activity as well as best practices in the whole life cycle of cyber security, from design to technology to operations. We work together to build the muscle memory to stop new kinds of attacks through exercises, and we build trust through in-person and online meetings with peers and subject matter experts.

Since the advent of Covid-19, FS-ISAC has hosted several business resilience calls for thousands of members with information and intelligence about how they can protect themselves against Covid-19-related cyber threats.

Since cyber crime is constantly evolving around the world, the need for intelligence sharing will only increase over time. As we have seen with the cyber threats that have accompanied Covid-19 thus far, new attack vectors emerge quickly and without warning. Secure peer-to-peer intelligence sharing circles where institutions can learn from each other will be increasingly useful, since no institution can anticipate every threat all the time. Only by collaborating as they do can we beat cyber criminals at their own game.

- **The writer is executive director, Asia Pacific, Financial Services Information Sharing and Analysis Center (FS-ISAC)**

CYBERSECURITY CRIME

BREAKING NEWS

03:50 PM Seoul: Shares finish higher as economic hopes offset China-US worries

03:41 PM ARA-backed crowdfunding platform raises S$2.7m from maiden property investment product

03:30 PM Softbank-backed Coupang under scrutiny after South Korea warehouse virus outbreak

03:29 PM Former HK leader lashes out at HSBC over security law

03:17 PM 611 new Covid-19 cases in Singapore, including 3 Singaporeans and PRs