Modernising Cyber Security Operations for a Collaborative Approach to Cyber Defence

An Industry White Paper published by CIO ACADEMYASIA

In partnership with IronNet

CIO Academy Asia organised a virtual panel discussion on the topic of "Modernising Cyber Security Operations for a Collaborative Approach to Cyber Defence", on 3rd December . The panel discussion included a facilitated round table in which many industry participants and digital leaders contributed and shared their thoughts.

This report is based on the insights shared by the main presenters and the participants during the virtual panel discussion.

All reports and surveys on the state of cyber security in Asia as well as globally underscore one major point: Cybersecurity threats are rising consistently-- from volume to methodologies deployed and to the level of sophistication of the attacks. Cyber attacks now range from conventional attacks to Advanced Persistent Threats (APTs) and Nation state level attacks.

The most frequent types of attacks are Social engineering (16%), Advanced Persistent Threats (APT) (15%), Ransomware (12%) and unpatched systems (12%), according to a report by Group-IB.

When the WannaCry ransomware attack affected more than 200,000 computers in 30,000 organizations across 150 countries in May this year, it exposed the soft underbelly of the organizations in the APAC region that were vulnerable to such attacks. According to a report by the Asia Pacific Risk Center (APRC), organizations in the APAC region are 80 percent more likely to be the target of a cyber attack.

Existing Cybersecurity Controls are Failing

As in other parts of the world, business and governmental organizations in the ASEAN region are also taking measures to combat and contain cyber attacks, said P. Ramakrishna, CEO, CIO Academy Asia in his opening remarks. Their response ranges from adopting a reactive and manual posture (people based following doctrine, doing their best to put out fires) to a more resilient posture ("Resilient Enterprise").

The former CISO, department of Defence, USA, defined a "Resilient Enterprise" as one which is predictive and focused, which isolates and contains damage, and applies rapid forensics to protect key enterprise resources to continue operations despite cyberattacks.

The agility and speed of action in this regard varies from organization to organization but unfortunately, most companies in the region fall between the two lower ends of the spectrum: they are struggling to defend themselves, choosing between manual and tools-based defence, and for most organizations, becoming a "Resilient Enterprise" remain the holy grail.

Another major of concern is that for most companies, existing cyber security controls are failing. Supply chain networks with third party involvement are growing, so is the attack surface as more employees work from home and 5G networks get operationalised. In this context, stopping attacks with focus on boundary protection is neither sufficient nor effective.

Need for more Resilience

As the CIO Academy Asia survey results shows, digital leaders in ASEAN agree that there is a need for more resilience and data security, info security and Government, risk and compliance (GRC) policy implementation are priorities for them. The measures they are taking for this include creating cybersecurity awareness among end users and technical training of IT staff, implementing end-point security, implementing SOC technologies and automation of threat management systems.

A Security Operation Center (SOC) refers to a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

While digital leaders agree that gaps in security operations need to be closed, there is a growing realisation that use of threat intelligence is crucial in defending their organizations with an organized and collective approach.

Role of Collective Cyber Defence

Speaking on the role of Cyber Defence, General (Ret) Keith Alexander, Founder, Chairman and Co-CEO, IronNet Cybersecurity, said that Nation State attacks are increasing globally, and he cited the role of Russian cyber attacks in Eastern Europe and the cyber attacks in the Middle East, involving Israel and Iran. These types of attacks are growing and collective cyber defence is the strategy required to thwart such attacks, he said.

He also gave the example of the Solarwinds attack. According to Identity Theft Resource Center (ITRC), "the rise in supply chain attacks (which often insert malicious capabilities into targets but don't immediately exploit them) increased the lag between when the initial compromise occurred and when related malicious activity started and the damage was discovered". For example, even though the SolarWinds breach occurred in March 2020, it was not discovered until more than eight months later. Surprisingly, in many cases, no damage has yet occurred. Although as many as 18,000 SolarWinds customers downloaded the compromised Orion software, the actual number and size of exposures across those customers remain largely unknown.

According to Ed Skoudis, SANS faculty fellow and director of SANS Cyber Ranges and Team- Based Training, SolarWinds is part of a large attack category called "undermining software integrity." He stated that many applications are actually compilations of several software packages or modules, many of which are open source. Skoudis cited a recent paper that documented 174 malicious packages available online that attackers had used to compromise applications in use at many companies.

Clearly, as the attacks grow in sophistication, CIOs also need updated security systems and the old signature-based threat intelligence systems don't cut the mustard anymore, Gen. Alexander said.

Signature-based malware detection can identify only "known" malware. Unfortunately, they fail to detect new versions of malicious code that keep coming relentlessly from cyber criminals. These newly released forms of malware can only be distinguished from benign files and activity by behavioural analysis. That's why there is a need for behavioural analytics, said Gen. Alexander.

Praising the role of Singapore, he said that Singapore is in a unique position as there is an abundance of technically trained staff in the country who could be roped in to put together a collective defence system.

Shift in Strategy

BG. Gaurav Keerthi, Deputy CEO, Cyber Security Agency of Singapore (CSA), highlighted a shift in CSA's strategy, an organization which is only about five years old.

He said that while the agency always had a razor sharp focus on protection and

incidence response related to Critical Information Infrastructure (CII)'s essential services of the country, but the nature of cyber incidents has caused them to rethink their overall approach.

According to BG. Keerthi, it is good that Cyber security laws and regulations are in place in Singapore but while big organizations are taking care of their cybersecurity needs, small organizations become targets of cyber attacks, especially in supply chain cyber attacks. In this respect, small organizations in the supply chain that don't have the resources or capacity to defend themselves become a means to get to the larger organizations. About 80 percent of companies in Singapore are SMEs, so they represent a large threat surface to cyber criminals. It is these smaller outfits that CSA is going to focus on now as a strategy to bolster the security posture of the country.

"We just can't collectively defend the crown jewels only," said Keerthi. "We have to protect the smaller companies too."

At the high level, Keerthi said that CSA treats security like drinking water: clean the water upstream a lot (with the telcos) so that downstream it is safe for citizens and businesses alike to consume them with the peace of mind that it's clean, that it has been treated (harmful elements have been removed from it) with the oversight of a responsible governmental agency.

Therefore, while protecting big and smaller businesses, the government has to strike a balance between "what the government can do and what private companies should do", said Keerthi.

Cybersecurity as a collaborative journey

Following the philosophy of cybersecurity as a collaborative journey, Keerthi mentioned two special measures that the Singapore government feels will help businesses become more secure. They are as follows:

The Data Protection Trustmark (DPTM): DPTM is a voluntary enterprise-wide certification for organisations to demonstrate accountable data protection practices. The DPTM will help businesses increase their competitive advantage and build trust with their customers and stakeholders.

Cybersecurity Labelling Scheme: CSA has launched the Cybersecurity Labelling

Scheme (CLS) for consumer smart devices, as part of efforts to improve Internet of Things (IoT) security, raise overall cyber hygiene levels and better secure Singapore's cyberspace. The CLS is the first of its kind in the Asia-Pacific region. Under the scheme, smart devices will be rated according to their levels of cybersecurity provisions. This will enable consumers to identify products with better cybersecurity provisions and make informed decisions. CLS recently bagged CIO Academy's Inspire Tech Award under the cybersecurity category.

Cyber security as an enabler

Speaking of a mental model, Keerthi emphasized positioning cybersecurity as a business enabler, something that evokes trust in the consumer as well as in the supply chain. He also suggested that companies should work with those vendors (including SMEs) that value security. This will ensure the cyber defence across all the businesses across the supply chain.

Cyber security as a value generator and differentiator

For any organization, big or small, cybersecurity is a cost and sometimes there are questions around the return on investment (ROI) aspect of cybersecurity. Not only should cybersecurity be seen as fire insurance (companies have to pay heavy fines to government agencies in case of security breaches), but it should be seen as a value generator and differentiator. Keerthi cited the example of Apple's iPhone, which is marketed as a secure device that champions the privacy of the consumer.

Work together, defend together

Achieving real-time collaboration with peers to respond as a team is a challenge, yet it is the way to go for real time discovery of threats based on behavioural analytics, threat correlation and insights from peer-SOCs and enhanced SOC prioritization, said Gaurav Chhiber, VP- Asia Pacific and Japan, IronNet Cybersecurity and IronNet Team. He was talking in terms of his company's philosophy which believes in collective defence.

Chibber presented an iron-dome view of Singapore organizations collaborating to fight attacks, that practice real-time attack intelligence sharing and real-time collaboration.

IronNet's Collective Defense platform – based around our IronDome and IronDefense products – enables organizations to share intelligence, hunt, identify, and collaboratively stop threats like never before. It delivers the industry's most advanced network detection and response capabilities, enhanced by analytics, threat intelligence, and a seamless ability to collaborate through Collective Defense.

Key observations by some panelists

Scott Lee, Information Security Specialist from said that SATS have been an early adopter of IronNet's collective defence solution. Lee said that he has extended it to the supply chain as a cyber defence strategy. He concurred with a lot of what other panelists suggested. He admitted that his organization has a global footprint but resources are limited. After deploying IronNet, he is able to use resources more efficiently, as there is a 50% saving in terms of time invested in monitoring and analysing incidents.

Going forward, he plans to bring in more subsidiaries into the security network, work together with them, with a single panel, and a centralised team, where everyone speaks the same language. Commenting on the role of government-driven awareness on matters of cyber security, he said that it helps them, even when the information is about a single phishing incident. He suggested that government agencies should facilitate in providing experience to companies like his what a nation state attack involves, so that they are better prepared when such attacks really take place.

"Today, we have a very informal collaborative environment," said a CIO practitioner from the healthcare sector. "A couple of years ago, in a major public sector event in Singapore, we immediately got an informal notification by various parties who were trying to give us a heads up on the ongoing security problem they were going through. That was a good wake-up call and helped everybody respond faster."

Commenting on the strategy of collective cyber defence, he said that the ability to come together to pool our resources and help each other out is critical. "We read about ransomware-as-a-service today. You can't beat that when you are on your own. It's impossible. I agree with what is being said about collective defence but what we need to figure out is how we can create a proper platform where we can then have a trusted environment where we can share threat information."

A senior practitioner from the telco industry said he has been conducting behaviour analytics for almost two years.

According to him, context is important when we do behaviour analytics. "When we went into Covid lockdown, our behaviour fundamentally changed and our logs went haywire," he said. "If 10,000 staff are suddenly working from home, imagine all the logs--from proxy logs to firewall and VPN logs--are totally different (from the pattern visible when they worked from office). People (monitoring the logs) could not grasp the logs. The lesson learnt was that while behavior analytics is good, the practitioners should understand the time and landscape as well.

"We have done cyber crisis training at the security or technical staff level but we need more training at the senior leadership level and involve them in the process," commented a CISO from the education sector. He said that senior leaders have very limited time and it would be a good idea to have exercises conducted for top level business leadership collectively as an industry.

For Enquiries, Please Contact:

David Chin
Deputy CEO
CIO Academy Asia
david@cioacademyasia.org