CYFIRMA

Delving into the Secrets of the Deep, Dark Web

Over the years, organizations have employed cybersecurity solutions in appliances, software, and all different layers of security controls—perimeter, endpoint, data security, and the overarching governance related process security control. Security controls operate in a traditional ABCD approach while hackers and perpetrators are masterminding novel ways of invading organizations. This calls for protection measures to be smarter and reach a stage where organizations can monitor, detect, or prevent upcoming events that they have never encountered before. The only way to achieve that is by integrating a good cyber intelligence capability that accomplishes all tasks in one place. The emerging field of cyber intelligence is often regarded by most as the heart of cybersecurity. Equipped with the capability to do just that and more is Singapore/Tokyo based CYFIRMA, a cybersecurity company that uses a proprietary artificial intelligence-enabled analytics platform to help organizations gear up for cyber attacks and manage related risks before they occur.

In this interview, Kumar Ritesh, Chairman and CEO of CYFIRMA, shares some insights about the organization's cyber threat visibility and intelligence products and services, their unique value proposition, and roadmap for the future.

Kumar Ritesh, Chairman & CEO

What are the challenges you have faced in your journey as a cybersecurity provider and how do you tackle them?

What is very interesting to see hackers doing lot of research about target, environment and Assets before launching an attack "Age of Random attack are going away, time is upon us to face planned cyber-attacks". Today, hackers and perpetrators are sponsored to launch innovative and gruesome cyber-attacks against a target while we as organizations have limited resources. To tackle the cyber incidents and breaches, we adopt a reactive approach hoping that the walls of security controls we have created will prevent hackers and perpetrators from breaching. The reality is that these hackers have since become more innovative in their attacks method, approach and plan of attack.

The issue in the market is that we are not applying the hacker's viewpoint, into our current cyber postures. At CYFIRMA, clients get to see the hacker's perspective of their organization, interests, and background. We try to understand their prime motivation and readiness to attack as well as their arsenal of potential attack methods.

We strive to drive awareness in the market that cyber intelligence is not just applying intelligence into the security controls; it is also about applying intelligence into an organization's business drivers, strategy, management control and people.

There is a clear need in the market for CYFIRMA's application of contextual threat intelligence to cybersecurity. How ready do you think the market is right now?

The market has been ready for the last three years. The issue is that nobody has figured out how to apply intelligence to all strategic, management, and operational layers of an organization. Just keeping technological controls up to date won't stop the hackers as they are always one step

ahead constantly figuring out new ways. You need to have an intelligence driven approach in place which enriches process, governance model, compliance framework, and an Agile strategy. The strategy has to be agile because in cyberspace, the hackers, their profile, and the type of methods that they use, keep changing.

> **Just keeping technological controls up to date won't stop the hackers as they are always one step ahead constantly figuring out new ways**

How do you help companies to use your services in all three strategic, management, and operational layers?

Our cloud-based cyber intelligence analytics platform collects data from thousands of sources: open and close channels, blogs, security forums, peer to peer, social and commercial forums. At the core of our technology offering is our ability to embed our solution into the dark web where the hackers and perpetrators operate and plan their targets and potential attack tactics. There, hackers communicate by disseminating their conversations into hundreds of different forums to thwart anyone from monitoring them.

We are the whistle-blower of cybersecurity. Our sophisticated predictive intelligence engine embeds virtual drones into deep web forums to silently monitor while waiting for any of our clients' names, industry, or geolocation to pop up. As soon as that happens, we capture and bring that information to our cyber intelligence analytics platform. The platform applies five layers of AI and ML engines that filter through the data to provide an organization a view as to understand who the hackers are, their potential targets, drivers of interest, estimated time ofthe attack, and more. We deliver the five key drivers of who, what, when, why, and how, in three different segments within our daily intelligence report to our clients.

The first segment of our report is strategic intelligence, which enlightens the readers on those hackers that have shown interest in their organizations. We look into the history of the cybercriminals, correlate information from public forums to gauge their intention, find out about the type of attacks that they can potentially launch based on these hackers' backgrounds, as well as their maturity on certain areas regarding coding and creating new malware and ransomware.

In the management intelligence segment, if we find that our clients' first-line of defense isn't enough, we inform them to augment their second-line of defense. Our clients evaluate their incident response, compliance and patch management process and our insights help them to strengthen their management layer, tighten their compliance posture, as well as their governance model.

To enrich security controls—firewalls, anti-virus solution, data loss protection control, proxies—our operational intelligence provides organizations with daily indicators of compromise, which pertain to the active threats.

Can you elaborate more on your product and service offerings, more importantly, your 360-degree cybersecurity services?

Our 360-degree services come as a subscription model under which there is a base package, which our customers subscribe for. It includes the daily threat visibility, an intelligence report, and a weekly update for our subscribers on what is changing from a tech and regulatory perspective and cyber incidents analytics we analyse malicious emails/ files using property sandbox and correlate automatically with threat intelligence to present affiliations to any threat actors, details of campaign and attribution.

Among other services, we provide brand and executive monitoring, cyber scoring, vulnerability analytics, and cyber education—all components being intelligence driven. To prevent hackers from attacking brands or causing reputational damage, we monitor infringements around the brand, check for lookalike domains or email spoofing while also monitoring the key individuals of a brand who can drive the market sentiment. Because when brand impersonations don't work, hackers and perpetrators move on to target the C-level executives of a company. As for insurance companies that face big lags, with the time period for risk assessment being three to six months, we perform real-time, intelligence-driven cyber risk scoring to help them sell cyber insurance efficiently.

Our partners today include top Japanese manufacturing, technology, product and solution, retail, BPO, and services companies. In the U.S., we are currently working with large financial institutions and product and engineering services companies. With predictive cyber threat intelligence, we are committed to helping organizations and institutions decipher the next move of potential cyber-attackers and undertake proactive measures in advance. CA