PHILIPPINE TELECOM GIANT TAKES A GLOBAL VIEW ON FIGHTING CYBER CRIME

CUSTOMER PROFILE

Globe Telecom — commonly referred to as Globe — operates one of the largest mobile, landline, and broadband networks in the Philippines. In addition to 3.5 million broadband customers, its 6,200 employees provide services to 50 million mobile subscribers, and almost a million landline users.

> "Our partnership with FireEye covers the entire threat lifecycle."
>
> — **Anton Bonifacio,** CISO, Globe Telecom

As the appointed protector of Globe Telecom's subscriber data – and nearly 1.05 million retailers, distributors, suppliers and business partners — CISO Anton Bonifacio, takes his role very seriously. "We don't have people's messages but we know who they called, who their friends are and where they've been," he explained. "We have the details of people's lives and it's imperative to do everything we can to protect it and to ensure their privacy."

To make sure that its data is secure, Globe has invested in a wide range of FireEye solutions and services. The company's pervasive network is protected against known and unknown advanced attacks by the FireEye® Network Security (NX) platform. The rapid detection and accuracy of alerts enables Globe to focus on events that pose a genuine threat.

"Our infrastructure is huge but we're only as strong as the weakest link: Each asset across the network is important and we need to ensure we secure every single element," described Bonifacio. To address the challenge of extending protection to each of its more than 10,000 endpoints, Globe deployed FireEye® Endpoint Security (HX series). HX assesses activities to identify exploits at onsite and remote locations, making it possible to immediately isolate compromised devices to stop attacks — all with a single click. Bonifacio continued. "Every endpoint counts and HX gives us the ability to instantly confine a threat and investigate the incident without risking further infection."

FireEye

"It is really about the whole industry experience that FireEye brings: I just can't do without it."

— **Anton Bonifacio,** CISO, Globe Telecom

The FireEye® Email Threat Prevention Cloud (ETP) secures what is typically one of the most vulnerable attack vectors: Email-based attacks, in particular spear phishing, remain one of the favored methods of launching advanced persistent threats (APTs) due to the complexity involved in detecting them. ETP is a SaaS solution that protects mailboxes against advanced email attacks and provides anti-spam and antivirus software capabilities. ETP seamlessly integrates with the FireEye NX platform to defend against blended attacks that attempt to exploit multiple threat vectors. Bonifacio noted, "ETP is a key component in our layered defense strategy and as it's specifically tailored for cloud-based environments it is the perfect fit with our Google email system."

Globe utilizes the FireEye® Central Management (CM) series to consolidate device and intelligence management, enabling the correlation of threat data across all of its FireEye components.

BEING REACTIVE AND PROACTIVE

Bonifacio is very confident in the effectiveness of the security solutions he has implemented but feels that this is only half of the challenge: "We have to protect everything across the entire environment; however attackers only have to find one tiny weakness. There is an inevitability that breaches will occur and I believe once you've done due diligence in securing your infrastructure, what's then most important is how you actually react when you are compromised.

"We have implemented world class defenses," he stated, "but if a breach does occur we don't try to hide it. We report every violation to our executive team. Being breached is most definitely not an indication that we failed; for me it's how we handle the incident — and what we learn from it — that determines success or failure."

Although placing an emphasis on prevention, to fully deliver on his strategy, Bonifacio has invested in additional services from FireEye's Mandiant team to complement his implementation of FireEye CM, NX, and ETP solutions.

CONSTANT VIGILANCE

"To ensure that Globe's defenses are always optimized to combat the latest threats, it schedules regular Mandiant Vulnerability Assessments to identify possible security weaknesses that could be exploited by attackers. Bonifacio noted, "Cyber criminals are relentless and very creative: It's imperative that we continually evaluate the ability of our security posture to defend against attacks. The Vulnerability Assessment distills the experience and expertise of the Mandiant consultants and equips us with the knowledge we need to constantly reduce risk and improve how we operate."

Bonifacio has further extended the capabilities and capacity of his in-house resources by subscribing to FireEye® as a Service (FaaS): "It's really reassuring to know there is a team monitoring our environment round the clock. FaaS gives me validation that a potential threat is actually real and immediately follows this by looking for signs of compromise. If things start to get really active, I now don't have to worry that we won't have the necessary bandwidth to effectively respond to incidents: If I need extra feet on the ground, I get them from FireEye."

To enhance its proficiency to handle possible breach situations, Globe invests in Mandiant Incident Response Services to investigate intrusions and targeted attacks. Using state-of-the-art proprietary technologies, Mandiant consultants identify the actions of the attacker, the scope of the breach and quantify possible data loss. Priority is given to eradicating the vulnerability and re-securing the infrastructure to prevent subsequent exploitation. "Nothing else matters if you

FireEye

cannot detect and respond to attacks in an expedient, effective manner. Doing this requires that you quickly quantify what you're dealing with: The Mandiant Incident Response team leaps into action as soon as a breach is suspected and equip me with what I need to know."

COLLECTIVE WISDOM

Bonifacio also utilizes Mandiant Cyber Defense Center Development (CDCD) to further refine and enhance the capabilities of his own team. He commented, "A defense in depth strategy is no longer just about prevention, it needs to be supported by world-class security operations utilizing tailored processes and procedures."

CDCD brings the collective intelligence and expertise of the global Mandiant team to focus on helping organizations create an adaptive defense strategy capable of minimizing risk and the impact of a breach.

"Cyber crime is a global threat: It is not enough to know about just one region; you have to learn from what is happening all over the world," reflected Bonifacio. "CDCD enables us to benefit from the best practices and proven techniques, collected from thousands of first-hand experiences from every corner of the world. The Mandiant team is fully familiar with our environment and helps ensure that all the individual elements work in harmony to achieve our overall security goals."

He concluded, "Our partnership with FireEye covers the entire threat lifecycle. I worked extensively with FireEye and Mandiant prior to coming to Globe and don't even look at the investment from a cost perspective: The capabilities complement and enhance my security operations. It is really about the whole industry experience that FireEye brings: I just can't do without it."

"The Mandiant team is fully familiar with our environment and helps ensure that all the individual elements work in harmony to achieve our overall security goals."

— **Anton Bonifacio,** CISO, Globe Telecom

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com