Announcements

New IBM Cybersecurity Hub to Help Asia Pacific Organizations Build Cyber Resiliency

- IBM Security Command Center in India represents significant investment in security incident response and training for organizations across APAC

- Asia was #1 most-targeted region for cyberattacks in 2021, according to IBM Security X-Force Threat Intelligence Index, released today

- New Security Operations Center (SOC) part of IBM global network for helping clients around the world respond to cyber-attacks

India, Bengaluru, February 23, 2022: IBM (NYSE: IBM) today announced a multi-million dollar investment in its resources to help businesses prepare for and manage the growing threat of cyberattacks to organizations across the Asia Pacific (APAC) region. The centerpiece of this investment is the new IBM Security Command Center, the first of its kind in the region, for training cybersecurity response techniques through highly realistic, simulated cyberattack – designed to prepare everyone from C-Suite through technical staff. The investment also includes a new Security Operation Center (SOC) which is part of IBM's vast network of existing global SOCs - providing 24X7 security response services to clients around the world.

According to new IBM global analysis released today, Asia is now the #1 most targeted region for cyberattacks – representing 26% of attacks analysed in 2021[1]. The data reveals a significant regional shift compared to the past decade of the report, where North America and Europe have historically ranked as most-targeted. This trend signals a growing need for security investments amongst Asian organizations, particularly those in financial services and manufacturing, which were the most-targeted industries in the region. The new IBM cybersecurity centers will help address the most pressing need of the hour for organizations of all types, to accelerate their security strategies and align business priorities with a security-first approach.

Located at IBM offices at Embassy Golf Links in Bengaluru, India, the new facilities represent a strategic hub for IBM cybersecurity activities in the region, which also include IBM Managed Security Services, access to IBM's team of incident response experts, as well as IBM Consulting, IBM Research, IBM India Software Labs, and IBM Garage, a collaborative approach designed to fast-track innovation and drive meaningful, lasting transformation for clients.

The new facilities were inaugurated in presence of Shri. Rajeev Chandrasekhar, Hon'ble Union Minister of State for Electronics and Information Technology and Union Minister of State for Skill Development and Entrepreneurship.

Speaking at the virtual launch, Shri. Rajeev Chandrasekhar, Hon’ble Union Minister of State for Electronics and Information Technology and Union Minister of State for Skill Development and Entrepreneurship said, "As India becomes the largest connected democracy in the world, our PM’s vision is that cyberspace will not just become a place for innovation, growth and opportunity, it will also become a place where the future standards and future technologies for securing the cyberspace evolve, mature and proliferate. I believe the Cybersecurity Hub launched by IBM today will go a long way in creating an ecosystem of not just awareness but also capabilities and talent in creating a safe cyberspace. I congratulate team IBM and look forward to a stronger partnership between the Government of India, our agencies, and IBM going forward with a common objective of realizing the Digital India mission and making sure that the Indian cyberspace becomes and remains safe and trusted."

Commenting on the launch, Sandip Patel, Managing Director, IBM India said, "One of the biggest challenges impacting the success of the exponentially growing digital economy and that of countries across the world is cybersecurity. Cybersecurity is a global challenge threatening enterprises more vigorously than ever before. We have an opportunity to respond and act now. We need cutting-edge technology and coming together of the entire ecosystem to address this threat and the launch of the IBM Cybersecurity Hub is, in fact, a response to this challenge. It will empower clients to respond to incidents with greater speed, effectiveness, and transparency."

"Preparing for a cyberattack is like fire-drill training. Everyone from executives through to contractors need to understand their own role in an emergency and reinforce the crucial response steps through practice,” said Chris Hockings, IBM Security CTO for Asia Pacific. “The new IBM Security Command Center is the first in Asia Pacific enabled to train the entire business in the art of response to a cyberattack event, further enhanced by the real-time experience of our security experts based in the adjoining global Security Operations Center. With Asia Pacific's enormous growth, diversity, and role in global supply chain, these capabilities can be a real game changer for helping customers face growing threats in the region."

Capabilities of the IBM Security Command Center

The highly realistic, immersive training simulations offered in the new IBM Security Command Center in Bengaluru leverage industry-leading audio and visual effects as well as live malware, ransomware and other real-world hacker tools. IBM designed the simulations after emergency and disaster response training models, in consultation with dozens of experts from different industries including emergency medical responders, active duty military officers and its incident response experts. The IBM Security Command Center in Bengaluru can deliver customized experiences and workshops - including virtually - that are tailored to organizations’ unique security requirements and objectives, leveraging the IBM Cyber Range Design consulting team.

Some examples of the types of trainings available include:

- **Ox Response Challenge**: Designed for the executive team to immerse a wide variety of stakeholders in a realistic "fusion team" environment in which players must figure out how to respond to a cyberattack as a team, across dimensions such as technical, legal and public relations.
- **Operation Red Escape**: Giving participants the opportunity to flip roles, it puts them in the ‘seat’ of a real-world attacker as an elite member of a growing adversarial group and develop a cloud-based attack on a major corporation. This non-technical interactive scenario allows business leaders to see first-hand how adversaries carry-out common cyberattacks on organizations with real adversarial tools and techniques.
- **Cyber Wargame**: In this hands-on scenario, participants uncover a cyber-attack lead by a cybercrime gang targeting a fictitious corporation. The Cyber Wargame tests the organization’s incident response process, communication and problem solving by positioning technical and business teams in the middle of a cyber security incident to see how they would work together to resolve it.

Expanding IBM’s Global Security Operation Center (SOC) Network

Adjacent to the new cyber range facility, IBM’s new Security Operations Center (SOC) will provide Managed Security Services (MSS) to clients across the globe. With capacity for 600 security response operators, it is the second IBM SOC in Bengaluru, with the other SOC continuing to specifically serve regional Indian clients. The new SOC is part of IBM’s vast global network of SOCs, which serve more than 2,000 clients around the world - managing more than 2 million endpoints and 150 billion potential security events per day. IBM’s global SOC network now includes 9 locations such as Atlanta (U.S.,) Australia, Costa Rica, Japan, Poland, Saudi Arabia and more. It offers MSS investigation experts to assist with on-the-ground response, dedicated security experts with strong vertical expertise, personalized advisory services combined with a holistic approach to secure hybrid cloud environments. IBM’s SOC model leverages AI, machine learning and automation, bringing together human expertise and advanced technologies to help respond with speed, efficiency and transparency.

2022 IBM Security X-Force Threat Intelligence Index Highlights

The 2022 IBM Security X-Force Threat Intelligence Index announced today unveiled the following insights regarding the threat landscape in Asia:

- **Financial services** and **manufacturing** were the top attacked industries in Asia, representing

nearly 60% of attacks studied.

- **Japan, Australia** and **India** were the most-attacked countries in the region.
- **Top Attack Types:** Server access attacks (20%) and ransomware (11%), Data theft (10%) were the top attack types observed in Asia.
- **Initial Infection Methods:** Vulnerability exploitation and phishing tied for the top infection vector at Asian organizations in 2021, each representing 43% of attacks observed in the region.
- **Ransomware groups:** REvil made up 33% of ransomware attacks analyzed, and Bitlocker, Nefilim, MedusaLocker and RagnarLocker were significant players as well

To view the full results, visit: http://ibm.biz/xforcethreatindex

---

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM Security X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 150 billion+ security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide. For more information, please check www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

---

[1] *For purposes of this report, IBM considers Asia to include Australia, East and Southeast Asia, India, and the Pacific islands.*

For further information: Vinay Krishnan | IBM India Communications | vinay.krishnan@in.ibm.com

---

Additional assets available online: Photos (