A GLIMPSE INTO WHAT CYBER SECURITY HAS IN STORE IN 2020

TODAY BREACHES ARE INCREASING AT A VERY RAPID PACE DESPITE RECORD LEVELS OF SECURITY SPENDING. IMPLEMENTING EFFECTIVE CYBERSECURITY MEASURES IS PARTICULARLY CHALLENGING TODAY BECAUSE THERE ARE MORE DEVICES THAN PEOPLE, AND ATTACKERS ARE BECOMING MORE INNOVATIVE. AND THIS IS PREDICTED TO CONTINUE IN 2020 AS WELL –

Securing the organizations and individuals have become essential in order to keep our society functioning. The threats encountered by the cyber world have increased three-fold. Security programs continue to evolve new defences as cyber-security professionals identify new threats and new ways to combat them.

There is a spending of $19 billion per year on cyber-security but still cyber-attacks continue to evolve at a rapid pace. To combat the proliferation of malicious attacks it is recommended continuous, real-time monitoring of all electronic resources. The recent examples of cyber attacks and cyber compromises have shown disturbing trends and the last couple of years have been rough on IT Security. The numbers of cyber attacks are only seem to be going up.

As we step into the year 2020, let us find out how the security majors are gearing up to combat these ever increasing cyber attacks.

SECURITY MARKET SHAPING UP IN INDIA

According to a PwC report, the cyber security market in India is expected to grow from USD 1.97 billion in 2019 to USD 3.05 billion by 2022, at a compound annual growth rate (CAGR) of 15.6%—almost one and a half times the global rate. Though many factors are contributing to this high growth rate, three factors are significantly driving the cyber security demand market in India —digital growth, increase in cyber attacks and stringent regulatory mandates. The study estimates that the market for cyber security products in India will grow at a higher rate than that for services.

According to IT Secretary, Ajay Prakash Sawhney, India has an estimated USD 1.9 billion (about Rs 13,500 crore) in cybersecurity service business, and USD 450 million (about Rs 3,200 crore) of cybersecurity products business. “There

AJAY PRAKASH SAWHNEY

IT Secretary

SANJAY MANOHAR

Managing Director, McAfee India

SEAN DUCA

VP and regional chief security officer, Asia Pacific & Japan - Palo Alto Networks

ROHAN VAIDYA

Regional Director of Sales - India, CyberArk

MURALI URS

Country Manager-India Barracuda Networks

JYOTI PRAKASH

Country Director – Enterprise Security Business, Micro Focus India

is also the presence of multinational and Indian entities which engage in R&D in cybersecurity, all of it currently amounts to USD 5 billion (about Rs 35,500 crore) worth cybersecurity ecosystem in India," he says.

Sanjay Manohar, Managing Director, McAfee India believes that much like the rest of the world, India is gearing up for an enhanced cybersecurity practice with a greater focus on personal data protection. "With sector after sector adopting digital technology to transform the nature of their business, their cyber risk profile changes just as intensely. Enterprise information security spending in India is on pace to total US$1.86 billion in 2019, an increase of 12.4% from 2018, according to the latest forecast from Gartner. The security industry is critical to ensuring India's prominence as a leading investment destination and the security of its major industries, and we anticipate a steady growth in this sector. Additionally, with disruptive and emerging technologies bringing in an influx of data, we believe the demand for advanced cyber security solutions will only increase," he observes.

Rohan Vaidya, Regional Director of Sales - India, CyberArk opines, "2020 will see a new (and unfounded) level of complacency around security driven by passwordless, behavioural and biometric authentication. With passwordless all the rage, organisations continuing to adopt biometric authentication for e.g. banking services and certain companies starting to add behavioral controls to assess whether a user is who they say they are as well, 2020 will be the time to remind ourselves that the most secure authentication is never the most user-friendly or the most cost-effective. We must see passwordless technology and the like for what it is – a great way of authenticating an individual but not a security panacea that will prevent mass data breaches."

Sean Duca, vice president and regional chief security officer, Asia Pacific & Japan, Palo Alto Networks contends that 72 percent of security decision-makers in large enterprises in India believe that security provided by cloud providers is sufficient to protect them from cloud-based threats. "Organisations need to recognise that cloud security is a shared responsibility. While cloud providers are responsible for the security of their infrastructure, the onus is on companies themselves to secure their data and applications stored in that infrastructure," he says.

With the various security services available to the end-users and corporate alike, it's evident that the cybersecurity market is shaping up well and is gaining importance since data protection is considered as the need of the hour by everyone. As per the latest PwC-DSCI report, the outlook for the Indian cybersecurity market is 1.5 times better than the global market. And this is due to the focus towards pioneering and enabling a 'Digital India.'

Murali Urs – Country Manager-India, Barracuda Networks says that Social Engineering Attacks such as spear phishing have quickly become one of the hottest and most dangerous cyber attacks around the world. "Cyber criminals will follow the money and pursue industries where the payout is the biggest. Trends in email security show that cybercriminals are finding new ways to make money that they did before, opting for account takeover and business email compromise attacks, which allow them to make money by tricking end-users into making payments rather than trying to seeing stolen information. The exception will be state-sponsored attacks, which will target industries with valuable intellectual property, such as aerospace, defense, technology, manufacturing and pharmaceuticals, and industries where they can cause disruption, such as utilities and transportation."

"As we accelerate in the fast-paced digital environment, we will witness a drastic rise in data volume. This will lead to a requirement for a strong cyber breach defense framework and cyber insurance will be critical here. Going forward, we will need to continue implementing a holistic security framework to identify, protect, detect, respond and recover from cybersecurity threats. Interestingly, focus on AI-based security and customized solutions will be on priority, which will help reduce millions of threat incidences into limited threat leads. Moreover, SOCs investment will go mainstream and DevSecOps will play a huge requirement in the coming year," says Jyoti Prakash, Country Director – Enterprise Security Business, Micro Focus India.

With many connected systems and ever-increasing use of smartphones giving rise to the risk of vulnerabilities, India with its proven prowess in software and services should now move aggressively in the area of cyber security. There is an increased cybersecurity investment by both enterprises as well as government agencies, as they step-up their efforts to protect their IT infrastructure from growing cyber attacks and also comply with regional as well as global regulations like IT Act 2011 and GDPR, etc.

While the economic boom has spurred developments across the country, cyber security awareness amongst users and companies is still low. With statistics showing over 50,000 cyber-attacks happening every year, it is evident that India is now a soft target for hackers.

Diwakar Dayal, Managing Director at Tenable India believes that there will be a shift in the cybersecurity industry towards a risk-based approach to vulnerability management which uses machine learning analytics to correlate vulnerability severity, threat actor activity and asset criticality to identify and manage issues posing the greatest business risk. This innovative approach will help Indian organizations focus on the vulnerabilities that matter most and address true business risk instead of focusing on flaws that have a low likelihood of being exploited.

Whereas Venugopal N, Director of Security Engineering, India, Check Point Software Technologies feels that today we find ourselves in the midst of the fifth generation of cyber- attacks known as Gen V which are attacks that are large-scale and fast-moving and can easily bypass the conventional, static detection-based defenses. "Organizations are still trying to protect their IT environment from the threats of today with older technology that only protects against viruses, application attacks, and payload delivery, and leaving their networks, virtualized data centers, cloud environments, and mobile devices exposed," he says.

Debasish Mukherjee, VP Regional Sales APAC at SonicWall observes a slight decline in malware in India, which is roughly in line with what is seen globally. "However, given that cybercriminals have become increasingly more sophisticated, we have observed a change in strategy with the ransomware subset of malware. Whereas hackers were previously casting a wide net with ransomware attacks, we now see focused efforts directed at fewer, higher value targets than before. This has resulted in a relatively large decrease in

DIWAKAR DAYAL

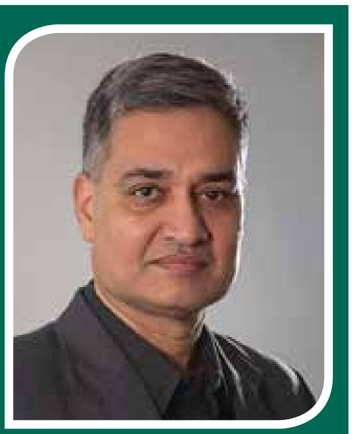
Managing Director
Tenable India

VENUGOPAL N

Director of Security Engineering, India, Check Point Software Technologies

DEBASISH MUKHERJEE

VP Regional Sales
APAC - SonicWall



RAKESH KHARWAL

Managing Director
Cyberbit

ransomware in India, as compared to both the global ransomware trend as well as overall malware. Where we have seen an increase in India is in intrusion attempts. In fact, India has one of the highest year-over-year increases in intrusion attempts globally. It's important to note that intrusion attempts could be related to a variety of factors – e.g., it could be accidental, due to misconfigured network equipment, or purposely, once potential hackers discover and exploit the vulnerability that misconfiguration has caused. This underscores why it's so important for VARs to leverage network security equipment that can quickly identify and protect against unauthorized traffic."

Rakesh Kharwal, Managing Director, Cyberbit says that a Cybersecurity Ventures report has indicated that the global economy will be losing $6 trillion annually by 2021. This is due to wide-ranging cyber attacks and cybercrimes. The staggering figure is about 2,000-times India's expected cybersecurity market size in 2022.

"However, looking at the bright side, India has the largest pool of youth, a budding startup ecosystem, and needs to create direct jobs. The nation has also envisioned making its economy worth $5 trillion by 2025. Secondly, a majority of businesses in India and the world across are focusing on enterprise-level EDR. However, the cyber attacks are getting more sophisticated than ever and can penetrate even the most sophisticated solutions. This presses on the need to move beyond enterprise-level cybersecurity frameworks to military-grade solutions.

NILESH JAIN

Vice President, Southeast Asia and India, Trend Micro

Lastly, the Smart City projects in India are being driven with full steam. Such projects involve the integration of IT and OT security. This leaves considerable voids amongst critical infrastructures, which can be penetrated by cyber attackers. So, the nation and relevant market players must adopt relevant ICS (Industrial Control System) and SCADA security solutions," he foresees.

The cybersecurity market in India will be defined by three key sectors according to Nilesh Jain, Vice President, Southeast Asia and India, Trend Micro - —banking and financial services industry (BFSI), information technology (IT) and information technology enabled services (ITeS), and government. "Although the demand from these sectors for strong security mechanisms is still catching up, they hold a promising future for cybersecurity in India. Adoption of emerging technologies such as cloud, chatbots, RPA, blockchain would result in organisations spending more on security consulting," he says. ■

THREATS TO COMBAT IN THE NEW DECADE

The year ahead will test many businesses, IT organizations, and data protection vendors as threats to business data become increasingly pervasive. As we head into a new decade, there's no doubt that attackers will try to use innovation against us but determining where they will focus will always be a challenge.

Though exciting advances occur in artificial intelligence (AI), autonomous vehicles, 5G networks cloud computing, mobile devices and the Internet of Things (IoT), these same developments seem to cause negative disruptions that make daily news headings.

What are the threats for the coming year? What solutions will be most imperative? What data breaches or ransomware attacks or other threats will cause the most dent? Some of the common prediction themes across vendors include -

RAJNISH GUPTA

Regional Director – India, RSA Security

"At RSA Security, we help customers manage their digital risks as they transform towards the digital era to shape the future of their business. On the business front, the accountability for cyber risk will move up the organizational chart, with businesses appointing board members with experience in risk management and information security. On the technology front, businesses will look to reduce dependency on talent via security orchestration and automation software, risk-based prioritization and comprehensive threat analytics."

SAMIR MODY

Vice President, Cyber Threat Labs - K7 Computing

"Data is the new gold, and we expect the trend of cyber threats that target data to continue, accelerate and diversify in 2020. We anticipate that cyber adversaries will respond to cyber defences by spreading their net beyond their typical targets. We expect them to more aggressively seek out weaknesses, such as poorly configured enterprise production servers, to sneak into corporate networks to inflict major cyber damage.

The explosion in mobile devices and the rapid increase in IoT devices present an attractive attack surface for cyber criminals in the nascent Industry 4.0 era. We predict growth in threats that target these devices via sophisticated malware exploiting loopholes, and their users through social engineering. We strongly urge organisations and individuals to steadfastly follow security best practices as a first, and essential, step in staying cybersafe in 2020."

JOHAN PAULSSON

CTO - Axis Communications

"Dedicated and optimized hardware and software – designed for the specific application – is essential with the move towards greater levels of edge computing. Connected devices will need increased computing power, and be designed for purpose from the silicon up, which is why Axis continues to invest in its own chip. This allows us to design an integrated circuit – or 'system-on-chip' – specifically for the video surveillance needs of today and the future and which, as with the latest iteration, ARTPEC-7, is designed with a security-first mindset. The concept of embedded AI in the form of machine and deep learning computation will also be more prevalent moving forwards. For those working with it, AI – or more accurately machine learning and deep learning – has now passed beyond being simply a buzzword, and become an everyday reality. It will therefore attract less attention as an 'exciting' tech topic, which may lead some to feel that it has failed to reach its potential. In actual fact it will be being used more than most people will appreciate – it will just be invisible to them. Again, however, one aspect that will need to be addressed is to create new deep learning models that are 'lighter', demanding less memory and computational power."

JOE LEVY

CTO – Sophos

"Machine learning has become an essential part of most modern organizations' cybersecurity strategy, and cybercriminals are now aware that these tools are being used to thwart their attacks. In response, criminals will set their sights on trying to evade or undermine machine learning security systems.

As the cat-and-mouse game between attackers and defenders continues, we can expect both offensive and defensive machine learning tools of increasing sophistication and effectiveness to develop rapidly. Over the next year, we expect to see more incidents where cybercriminals attempt to trick machine learning detection and classification models, and even leverage machine learning to generate highly convincing fake content for social engineering attacks.

In addition to leveraging prevention and protection to stop attacks before they happen, businesses are advised to take a layered approach to security. By combining human threat hunters with the leading threat intelligence and technologies like deep learning, organizations can detect and contain even the most sophisticated attacks faster, minimizing their impacts and costs."

SANJAY MANOHAR

Managing Director, McAfee India

"McAfee Labs predicts that in 2020 threat actors will increase the complexity and volume of their attacks, and more often use the world's evolving technology against us. They are targeting corporate networks to exfiltrate corporate information in two-stage ransomware campaigns. Only adding to this threat, deepfake videos or text will be weaponized to enhance information warfare. Bad actors will leverage AI and ML to extend their capabilities of producing convincing deepfake videos, in an attempt to manipulate individual and public opinion. AI-driven facial recognition, a growing security asset, will also be used to produce deepfake media capable of fooling humans and machines.

Every company in the world is on their journey to the cloud. However, keeping track of security incidents in the cloud has become increasingly difficult and the need for cloud security is greater than ever. In 2020, threat actors will find low-hanging fruit in the cloud - ransomware attacks will now target the cloud, while complex and potentially devastating cloud attacks will strike at an accelerated speed in 2020. McAfee also predicts that Application Programming Interfaces (API) will be exposed as the weakest link leading to cloud-native threats."

KIRAN ZACHARIAH
Vice President, IoT Business Solutions, Subex

“We expect 2020 to be a year of decisions. As the number of breaches increases and more state-backed and non-state actors enter the picture, we will have to scale up our cybersecurity game in the country. I see a significant increase in the budgets allocated for pro-active cybersecurity measures, staff training, audits and in procuring and deploying cybersecurity solutions. We have to remember that in 2019, we saw a steep rise in the investments made by malware developers globally. In the second half of the year, we saw those investments translate into more sophisticated cyber attacks. This trend will continue in 2020 and we need to be prepared for that.”

SURENDRA SINGH
Sr Director and Country Manager, Forcepoint, SAARC

“In 2020, organisations will turn their attention away from threat-centric to human-centric security focusing on two of its most important assets critical data and people. To this end, we see a marked increase in number of organisations enhancing their Indicator of Compromise (IoC) -based threat intelligence with the contextual insights of behavioral indicators. Additionally, expect a more mature approach by organisations to data/privacy protection legislation. Businesses are recognizing that maintaining an individual’s (customer’s) privacy and protecting their data can be a differentiator of a business’s service. This will invoke a move from a breach prevention approach to a more holistic principles-based approach. Lastly, more and more organizations, even government agencies, are moving to the Cloud as part of their digital transformation. Attackers will have a renewed focus on Public Cloud accessible systems and data in 2020 and beyond due to the richness of the prize and ease of accessing it. We expect to see more breaches both from external and internal parties as Cloud applications become more ubiquitous.”

MUSHTAQ AHMAD
SVP and CIO - CSS Corp.

“With the advent of digital transformation across sectors, being cognizant of cybersecurity challenges and safety is of utmost importance. The security landscape in 2020 will include optimal utilization of AI, with deep learning algorithms and mechanisms to combat malware and phishing attacks. As IoT, autonomous things and pervasive connectivity continue to drive digitalization, the possibility of cyber-attackers using more sophisticated AI-based threats looms large. Data threats and cloud security issues are pertinent ones that threaten the scope of cybersecurity now more than ever. Going forward, there will be an increased awareness of the need for a cybersecurity strategy. More cybersecurity products and services that leverage AI/ML and automation will be developed. We also expect cybersecurity to be deeply integrated into more tech products and pave the way for transformation across industries and organizations.”

OUSSAMA EL-HILALI
CTO - Arcserve

“Companies across all industries need to understand that ransomware is a "when" not "if" scenario, and better prepare for this continued onslaught of cybercrime. Instead of relying solely on security solutions, IT leaders must take a two-pronged approach to ransomware mitigation to avoid choosing between data loss or paying a ransom - and in many cases, both. This means not only making investments in more advanced threat detection and remediation software, but also ensuring that data backup and disaster recovery protocols have entered the modern era.

In 2020, more businesses will seek out vendors who offer an integrated approach to cybersecurity and disaster recovery with solutions that combine the two. In doing so, IT leaders will move away from segmenting threat prevention and data protection to assure mitigation from cyber attacks, no matter the level of sophistication or target. Further, IT teams will invest more time into making backup plans known to business leaders by more clearly documenting who is responsible for what if their organization were to fall victim to an attack.”

UDAY BHANU DAS
Co-Founder & CEO, Beyond Security Technologies Pvt Ltd

“A staggering 91% of cybercrime starts with email these incidents are “malware-less attacks” since they rely on tactics like impersonation to trick people into clicking dangerous links or providing sensitive info. The mobile users are at the greatest risk of falling for it because of the way many mobile email clients display only a sender’s name — making it especially easy to spoof messages and trick a person into thinking an email is from someone they know or trust.

In an era where we’re all constantly connecting to public Wi-Fi networks, that means our info often isn’t as secure as we might assume. Nearly a quarter of devices have connected to open and potentially insecure Wi-Fi networks network spoofing has increased “dramatically” as of late, and yet less than half of people exposed while traveling and relying on public networks.”

SECURITY TRENDS BELIEVED TO IMPACT BOTH BUSINESSES AND CONSUMERS IN 2020

- 5G and the IoT could make us all more vulnerable to cyber attack. 5G offers unprecedented data theft speeds
- Businesses will start to rethink their approach to the cloud
- Drones Open up New Pathway for Intelligence Gathering
- The rise of artificial intelligence (AI) based threats looms large so also AI will help prevent subscription services fraud
- Bad actors will turn to blockchain platforms for their transactions in the underground.
- Deep fake technology will be used for identity theft
- Ransomware Tactics Evolving
- ID Mules
- Attackers Will Find New Vulnerabilities in 5G / LiFi networks will be targeted by hackers
- Phishing attacks go beyond email
- Chatbot and voice assistance payment fraud will rise
- FinTech companies will be fraudsters' next big target
- Selfie biometric data will be the new dark web money maker
- Mobile malware attacks step up
- The Growth of "Passwordless" Authentication
- Email and internet-facing applications will continue to be the top threat vectors

MICHAEL SENTONAS

VP of Technology Strategy - CrowdStrike

"The old adage in cybersecurity, 'old vulnerabilities cause big damage' will ring true in 2020. Attackers will look to increase development of exploits that take advantage of the vulnerability in Microsoft's Server Message Block (SMB) protocol and they will do it with great success. Ransomware such as Ryuk allows an attack on a single infected device to quickly spread throughout an organization.

Whether you are dealing with nation-state attackers, eCrime actors or hacktivists, ultimately your best defense is to make sure your organization is deploying true next-generation solutions, such as the CrowdStrike Falcon platform that offers endpoint detection and response (EDR), managed threat hunting, next-gen AV with behavioral analytics and machine learning, and automated threat intelligence. These tools are key to gaining the visibility and context you need to meet these critical, outcome-driven metrics, and win the race against even the most sophisticated adversaries."

MOUNIR HAHAD

Head of Juniper Threat Labs

"In 2020, the number of IoT devices plugged into the internet will reach a threshold that will present an attractive target for cyber criminals. We will probably start seeing the first ransomware attacks on a large-scale targeting IoT devices running on low power microprocessors and using the Android or Linux operating system."

RAJEEV SAMANTA

General Manager of Sales, APAC Region, Tyco Security Products

"Virtually every segment in the country is beaming demand for electronic security today, from small households to small enterprises, large private enterprises and large government enterprises. There is growing demand from the government / private enterprises towards providing security infrastructure to serve the need of their establishments. I can observe a visible change in the mind-set of people responsible for maintaining security in their premises or by the law enforcement agencies towards the citizens they serve. Their needs are not only evolving, they are continuously challenging the norm and demanding better and relevant innovations, despite knowing that the same may come at a premium. I think this very point indicates that the respect towards the subject of security has increased immensely. From a "good to have" it has slowly become a "must have" over the last 5-7 years."