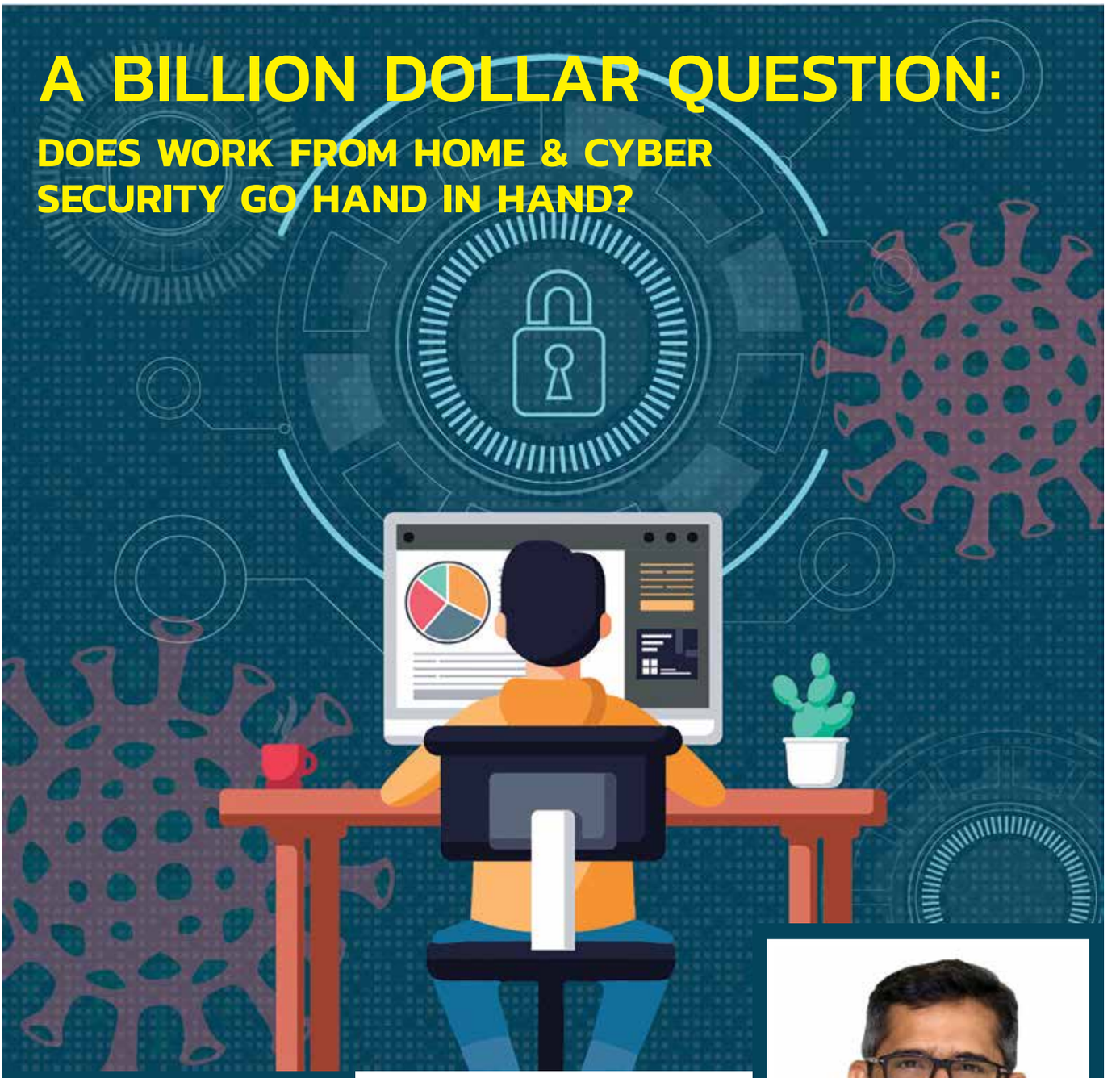
A BILLION DOLLAR QUESTION:

DOES WORK FROM HOME & CYBER SECURITY GO HAND IN HAND?



THE ONGOING PANDEMIC, COVID-19 HAS CHANGED THE LIFESTYLE AND WORK STYLE OF MILLIONS OF PEOPLE ACROSS THE WORLD. TO CURB THE SPREAD OF THIS PANDEMIC, PEOPLE ARE LOCKED DOWN IN THEIR HOUSE AT PRESENT AND ARE FORCED TO ADOPT THE 'NEW NORMAL' OF WORK FROM HOME. BUT AT THE SAME TIME, THIS IS ENDANGERING ENTERPRISE DATA AS THE SYSTEMS LACK STRINGENT SECURITY AS IN OFFICE SETUP. THESE DAYS WE ARE OBSERVING A LOT OF CYBER ATTACKS HAPPENING AROUND THE WORLD AND CYBER CRIMINALS ARE TARGETING PEOPLE WHO ARE PRESENTLY WORKING FROM HOME.

VARIndia managed to share a thought with a few managing heads of various companies about their strategy for WFH and Cyber Security. Each narrative has something to say. Here's straight from the horse's mouth:

While new threats are emerging all the time, there are three areas - Remote-work, Supply chains &IT and OT convergence; Tenable India is focusing in particular, says Diwakar Dayal.

According to Dayal, the sudden shift to a remote-work model means that new assets like employees' personal laptops and phones are being introduced into the enterprise IT environment. This influx of personal technology expands the attack surface and presents cybersecurity risks to organisations.

"We've already seen a number of phishing scams, misinformation and fraudulent work-from-home opportunities making their way around the internet. These could potentially put the wider corporate network at risk if accessed", said Dayal.

It is imperative to have a cyber-resilient supply chain to keep the critical infrastructure secure and operational. Many instances of cybercriminals trying to exploit the health crisis by targeting individuals and organisations to infect network, as such, any failure or interruption could impact this ability to operate.

As more organisations interconnect their OT and IT networks to create greater efficiency and efficacy, they also expand the cyberattack surface, enabling bad actors to easily move between the digital and physical worlds. Security teams overseeing IT and OT networks must, therefore,

DIWAKAR DAYAL
Managing Director
Tenable India

assess and prioritise vulnerabilities based on risk and likelihood of exploitation.

"Cyber hygiene practices such as maintaining systems, blocking malicious sites and IP addresses, enforcing multi-factor authentication and using encryption is a good place to start. It's most crucial during this time for security teams to understand their distributed attack surface" concluded Dayal while taking about avoiding cyber attacks.

Speaking about Cyber attacks and how would they provide protection, Surendra Singh's words were:

Forcepoint X-Labs, the custodian of threat and behavioral intelligence, in its latest reporton a three-month trend analysis of the web and email traffic reported a 358% jump in the number of malicious emails, in the week of March 23. The number of malicious emails is traditionally lesser than spam emails. Forcepoint Labs blocked over half a million spam emails every day mid-March onwards.

We encourage organizations to use modern data protection strategies that focus on protecting users and data everywhere. With data and applications moving beyond the traditional enterprise data centers and into the cloud, 'people' have now become the new perimeter from cybersecurity perspective.

In this 'new normal', organizations need to have an approach that protects critical data on-premises, data-in-motion and data in-the-cloud, as people access it from multiple devices (including BYOD) and from anywhere. For IT leaders, it's important to have visibility and control of their users' activity into the cloud. A clear understanding of the cloud applications people use and how they use them enables IT teams to mitigate risks and better protect sensitive data.

At an individual level, employees must focus on the following to keep themselves secure as they scale the work-from-home model:

- Use encrypted VPNs to keep themselves, and the company intellectual property, safe and secure.
- Be skeptical while clicking on any link or opening emails to avoid phishing attacks. Regular education by IT teams can help employees understand what to look for in a phishing attack.
- Use two-factor authentication for any company logins, be it internal applications or SaaS-delivered ones.
- Avoid the use of unknown USB thumb drives as there have been countless incidents from unknown USB drives infected with malware.

Parvinder Walia feels that, Since work from home began, an increase of cybercriminal activity is been seen. Due to anxious population and vulnerabilities resulting from the increase usage of remote access as well as home networks and devices, cyber crime is uprooting.

"We witnessed large scale password guessing attacks on Remote Desktop Protocol (RDP). Bad actors were apparently attracted by networks that are more open to incoming traffic due to remote working arrangement adopted by many businesses. Globally, there was a six-fold increase in RDP connection attempts in March compared to February"

"We also saw a surge in scam and malware campaigns using the pandemic as a lure, trying to capitalize on people's fears and hunger for information", said Walia.

Aside from the threat that is exploiting the pandemic, our researchers have also highlighted some of the top threats and malware in our Q1 2020 ESET Threat Report.

There are various things that people can do to stay safe at home, from the way that they work to securing their device. Remember to:

i) Avoid clicking on any links or downloading any attachments in unsolicited emails or texts from unknown sources, or even in trusted sources unless you are certain that the message is authentic.

ii) Ignore communications that ask for your personal information. If necessary, verify the content of the message with the apparent senderor the organization that they (seemingly) represent, and do so via a different medium than the received message.

iii) Be especially wary of emails that add to the sense of alarm and urge you to take immediate action or offer COVID-19 vaccines or cures.

iv) Control access to video conference by setting a password (do not embed it in the meeting link) and hold participants in a 'waiting room'. If file transfer is needed, then consider limiting the types of files that can be sent; for example, don't allow executable files (such as .exe files).

v) Use reputable multi-layered security software that includes protection against phishing.

Aside from that here are a few tips about how to secure your device as you work from home:

i. Enforce strong passwords to access the device, the domain and all services and applications. Set inactivity timeouts to log out when not in use.

ii. Implement full disk encryption to ensure that even if the device were to fall into the wrong hands, the company's data is inaccessible.

iii. Always use a VPN to connect to the organization's internal network to prevent man-in-the-middle attacks.

iv. Utilise Multi-Factor Authentication (MFA) to ensure that access, whether to cloud-based services or full network access, is by authorised users only.

v. Most importantly, do an audit of all home devices to ensure there are no vulnerabilities among connected devices and the network. Ensure that all firmware has been updated to the latest version and all passwords are updated and kept secure.

PARVINDER WALIA
ESET Sales & Marketing Director
for Asia Pacific & Japan

SURENDRA SINGH
Senior Director & Country
Manager, Forcepoint

J Kesavardhanan, believes, As COVID-19 continues to dominate headlines even in the world of cybersecurity, we still see standard phishing attacks that claim to be messages from the WHO or other credible sources, to mislead people into activating a malicious payload. But the efficacy of such attacks decreases as awareness increases, so we are now seeing cyber threats evolve to prey on people's financial anxiety and social isolation as lockdowns are extended.

A real threat is an SMS that claims to be from the Income Tax authorities and notifies the recipient of a refund, but actually steals banking credentials and installs OTP stealing malware.

Finally, we have also noticed an increase in attacks on Tier-2 and Tier-3 cities. Employees working from home create a lucrative opportunity for cybercriminals as they access critical business data and networks, but do not have adequate cybersecurity at home for protection.

OUR ADVICE TO AVOID CYBERATTACKS IS:

a) Install all patches and updates from hardware and software vendors

b) Install a good cybersecurity product and ensure it is updated

c) Practise good cyber hygiene, such as using unique and tough passwords, and

d) Exercise caution and scepticism when viewing messages or websites and think twice

KESAVARDHANAN JAYARAMAN
Founder and CEO
K7 Computing

before opening an attachment, clicking a link, or installing an application.

While speaking on new normal- Work From Home Govind Ramamurthy noted, "With the latest WFH trending these days, cyber attacks are heard much. Benign looking emails with malicious links are being used as a medium to conduct a phishing attack where the user or organizations data through the user could be compromised."

Users are worried about cyber attacks during the time of global crises, and cyber criminals are using this fear to execute various Covid-19 related scams for their own benefit.

Awareness about cyber attacks has always been the key towards constructing a safer work environment, whether in office or away.

Security teams in tandem with the internal communications and the Human resources department can conduct a weekly security training session to educate their employees on the various threats that the digital world is exposed to. On the other hand, users can observe basic hygiene, when it comes to the digital world.

SOME TIPS FOR THEM ARE AS FOLLOWS –

- Be very vigilant and avoid clicking on any unknown links or downloading documents from untrusted sources.
- Instead of clicking on unverified links for information, always bank on trusted sources and find them by with the use of a trusted search engine.
- Do not fall for advertising baits that seem too good to be true, or which offer information that requires a user to click on a link to know more.
- Organizations should have training campaigns on how to reduce the click-through rate.
- Do not share any personal information over the site that looks untrustworthy.

Adding to the discussion Shrikant Shitole, further says, Given that COVID-19 is the undoubtedly the overwhelming concern of governments worldwide for the time being, we anticipated targeting of government, healthcare, biotech, and other sectors by cyber espionage actors. Spear phishing messages were sent by the actor to China's Ministry of Emergency Management as well as the government of Wuhan province, where COVID-19 was first identified.

HEALTHCARE OPERATIONS, RELATED MANUFACTURING, LOGISTICS, AND ADMINISTRATION ORGANIZATIONS, AS WELL AS GOVERNMENT OFFICES INVOLVED IN RESPONDING TO THE CRISIS ARE INCREASINGLY CRITICAL AND VULNERABLE TO DISRUPTIVE ATTACKS SUCH AS RANSOMWARE.

The sudden and unanticipated shift of many workers to work from home status will represent an opportunity for threat actors. Organizations will be challenged to move quickly to ensure sufficient capacity, as well as that security controls and policies are in place.

In order to adapt to a remote and distributed workforce, organizations need to focus on protecting identities and applications regardless of whether they are in the corporate network or the cloud. The below mentioned tips offer a step in the right direction to keeping operations both secured and productive.

- Organizations must implement MFA on all external corporate resources to reduce the ability of network and application access through credential spraying, password stuffing and phishing attacks.
- Many organizations lose visibility into malicious activity targeting remote workers. Organizations should deploy a multi-layer endpoint agent on all employee endpoints.
- Cloud services are an important resource for remote workers and can contain sensitive corporate data. Ensure that teams are receiving logs from cloud providers and regularly reviewing them for unauthorized access and data exfiltration.
- Implement corporate alternatives, organizations can ensure that corporate data is protected and monitored by corporate security controls. For example instead of cloud use third-party solutions for note taking, file storage and document management.
- Provide security awareness training for remote workers. In addition to computing hygiene topics such as phishing and password guidance, train employees on physical security topics such using a privacy screen, limiting work on confidential material in public spaces and securing physical computing assets.
- Restrict off-network communications from virtual desktops to limit exposure. If some external network access is required, maintain a whitelist inclusive of only necessary, approved resources.
- Users should be provided the necessary equipment and trained on privacy best practices, including privacy screens, device locks and endpoint hardening.
- Organizations should consider the potential for laptops to be lost or stolen.

WFH shall sooner or later become the new norm, as a few companies are allowing their

GOVIND RAMMURTHY
Managing Director and CEO
eScan

employees to stay at home and work. But with this, it is necessary to look upon measures to protect the customers and educate them about Cyber security. Companies are taking preventive measures to protect their customers from Cyber criminals.

According to Dayal, "At Tenable, our customers are central to everything we do so we've developed thoughtful procedures that enable us to respond to emergencies and maintain high business standards."

Tenable is not just available to our customers 24 x 7, but our research team is working around the clock to publish the latest research on cyberattacks, phishing attempts and other opportunistic behaviours so that our customers can stay informed, said Dayal.

Forcepoint offers Dynamic Edge Protection (DEP), a new cloud-native platform, to deliver advanced web, network, and application access security as a service from the cloud. It implements the SASE model, weaving together advanced capabilities such as firewalling, intrusion prevention, web content inspection, malware scanning, URL filtering, application access, and more. This converged approach eliminates gaps and redundancies to stop attackers consistently, no matter where your people are working.

Organizations today are trying to navigate through what is arguably unchartered business territory as their global workforces have shifted to a large-scale remote work model seemingly overnight. At Forcepoint, we have pivoted to a virtual strategy and already kicked off various marketing programs such as virtual events, digital roundtables, digital workshops and webinars, etc. to support our customers come out on the other side stronger and more secure than before, concludes Sureinder Singh

In ESET, "Digital transformation creates additional considerations for cybersecurity. Globally, businesses have adapted by embracing technology to provide connectivity to networks, video conferencing, collaboration tools and cloud services. The company foresees that the way that they currently work will form the basis of the new normal.

Throughout this entire transition period, ESET has been continually monitoring and

identifying areas in which we can support businesses. One such way that we have done so is by extending the free trial duration of our consumer, SMB and enterprise solutions. Through this initiative we hope that businesses and employees will benefit from increased security and awareness during this period of work from home", said Walia.

Looking ahead, we will continue to develop new solutions that aim to meet the evolving consumer and business needs, as well as address the evolving threat landscape. In addition, we hope to place more emphasis on cybersecurity education to ensure that businesses and consumers are better informed of the current threats and how to deal with them.

Walia further added that ESET is currently offering free online cybersecurity training at www.eset.com/in/business/cybersecurity-training/ which is designed to educate employees on how to stay secure while they work from home. In addition to that, we have also put together a comprehensive package containing useful guides and checklists for IT administrators to set up and ensure safe remote workforce arrangement.

As a global cybersecurity solutions provider, ESET is also constantly monitoring and researching the threat landscape at a global scale, for any new developments.

Moving forward, we will continue to educate our customers by regularly updating our blog with new content as well as being available for any service-related queries that they may have in the future, confirms Walia.

The K7 Labs analyse hundreds of thousands of malware samples a day and we distribute frequent threat definition updates to ensure that our products are updated, and our customers are always protected from the latest cyberattacks.

We have also published a COVID-19 Cyber Threat Report that dives deep into pandemic-themed cyber threats and countermeasures to spread awareness on what the 'new normal' cyber threat landscape looks like, says J Kesavardhanan.

We are conducting many webinars to accelerate the spread of cybersecurity knowledge targeting both the consumer and enterprise markets. We have created industry-specific webinars for enterprise customers to address the diversity in the enterprise cybersecurity space. We also regularly publish blogs to keep users updated on the evolution of cyber threats and how they can protect themselves against cunning cybercriminals.

K7 has always been prepared to take on any cyber threats irrespective of the scenario that we have been presented. We have various technologies that can aid users and organizations to secure their data even in the current work from home scenarios. We have a very adept marketing team that works round the clock. We take on a multi-pronged approach when it comes to educating our customers and spreading awareness about digital threats.

We get in touch with our partners through various mediums and educate them and they in turn pass on the knowledge to our loyal customers first hand. In such a situation even if the customer has any queries regarding cybersecurity, with the help of our partners we get in touch with the customer and resolve their query.

SHRIKANT SHITOLE
Senior Director and Country Head for India, FireEye

WE WRITE A LOT OF INFORMATION ABOUT DIFFERENT SUBJECTS AND TOPICS ON THE CYBERSECURITY DOMAIN AND POST IN ON OUR BLOG, WHICH CAN BE ACCESSED THROUGH OUR COMPANY'S OFFICIAL WEBSITE. WE ALSO ENGAGE IN DIRECT COMMUNICATION WITH OUR CUSTOMERS THROUGH OUR SOCIAL MEDIA CHANNELS AND WE TRY AND SOLVE THEIR QUERIES. WE USE THE SAME MEDIUMS TO EDUCATE A WIDER AUDIENCE INTO KNOWING WHAT THREAT COULD DO WHAT KIND OF HARM TO THEIR DIGITAL EXISTENCE AND TIPS ON HOW TO SECURE THEMSELVES.

As we said, awareness goes a long way in avoiding digital threats and we take every possible step.

With the rapid escalation of COVID-19, organizations have to rapidly adapt to limit contact and person-to-person contamination, said Shrikant Shitole.

Over the past several weeks, organizations around the world have instituted remote, work-from-home policies. Business units and functions that have never been done remotely are now required to operate in a fully remote mode. During these rapid changes, security experts are rightly pondering what new risks may be introduced.

We at FireEye, are taking steps to ensure the safety of our clients. We have launched multiple reports and acquired additional solutions that aid to the resources we currently have to offer to our clients. We are also going the extra mile to keep a watch on how the threat actors are evolving in the current scenario. One of these steps is the acquisition of Cloudvisory in January 2020, as a means of combining cloud visibility with unrivaled insights into the threat landscape. Fully integrated into the broader FireEye cloud security portfolio, Cloudvisory now offers customers instant deployment across their cloud infrastructures, and further capabilities in security analytics through FireEye Helix and advanced threat detection through FireEye Detection On Demand.

Building upon the FireEye cloud solutions portfolio, Cloudvisory is a cloud-native security solution that gives security team's unified control over cloud sprawl and infrastructure misconfiguration. Unlike legacy and one-off security tools that introduce deployment complexity and fail to scale in the cloud without greater investments in talent, the Cloudvisory solution is designed to:

- Provide central single-pane visibility into assets, workloads and associated security controls and events across an organization's cloud infrastructure
- Remediate compliance failures, without any need for extra deployment components such as agents, appliances and functions
- Block and quarantine attacks using cloud-native micro segmentation

At FireEye, we understand the importance of an effective cyber security solution and believe in constant testing to validate the solutions deployed by our clients. In light of this, last year we made strategic investments to build new capabilities in our solution portfolio including security validation to help the customers to get more from their security investments. The Mandiant Security Validation (formerly known as Verodin), helps organizations demonstrate the value received from security through a data-driven, evidence-based approach. It enables customers to continuously validate their cybersecurity controls, identify and mitigate configuration issues, and optimize their people, processes, and technology.

As the cloud grows, FireEye is growing with our customers to ensure that emerging technologies are not an attacker's playground. To do this, our products and services protect traditional on-premise workloads from being leveraged for cloud attacks, and natively integrate with cloud providers to add protection, detection, and visibility for existing cloud workloads. As environments and attackers change, FireEye continues to innovate to help our customers meet those new security challenges.

The age of remote work is upon us. Companies around the world are letting their employees work from home, with many making the shift in a matter of days and some announcing plans to keep the policy going for the rest of the year -- or even indefinitely.

Though Work From Home may seem a permanent option for many, there are a few precautions to be taken.

Experts say they have seen a surge in "phishing" attacks targeted at people working from home, where clicking on a link in an email or message could lead to installing malware on one's device. Precaution is the only cure at this point of time. As any longer, will make things slip out of hands. The end of global pandemic is unknown; VARIndia requests its employees and clients to Stay safe, work safer. ■