
The entire globe has undergone a 360 degree change with the sudden outbreak of COVID-19 pandemic. It has not only changed the way people lived their lives but also the way they used to work. The pandemic has forced people to work from home or anywhere and it is not at all a protected environment in terms of IT security. This has put the data of any organization not only in a vulnerable state and also exposed to cyberthreats.

As per a report by Check Point Software Technologies, the sudden push to provide remote working facilities to employees during the lockdown has made India vulnerable to ransomware attacks in the third quarter of current year. The study also reveals that after the US, India comes second among the top five countries most affected by ransomware attacks in the third quarter. Apart from ransomware, different kinds of attacks are also coming to the surface.

This happened as the organizations were in a rush to facilitate remote access and many companies allowed connectivity from unmanaged home personal computers that often lacked basic cyber hygiene such as updated software patches, anti-malware, among others. Even personal mobile devices were allowed access to networks.

Now, the enterprises are adopting latest technologies to secure their endpoints. At the same time in 2021, the cyber criminals will continue to target the remote workers as their easy targets. On this backdrop, we have gathered insight from the CIOs/ CISOs, vendors and partners on how they are mitigating threats, measures they have adopted to combat threats, how they are safeguarding their employees and customers. Let's take a look at it.

# INDIAN CIO's ARE PREPARED FOR A DATA BREACH

## VPN AND PRIVILEGED ACCESS MANAGEMENT : THE KEY TECHNOLOGIES

**SANDEEP SENGUPTA**
MD, ISOAH Data Securities

### EDUCATING CUSTOMERS & EMPLOYEES

Over the last 10 years, our "Indian School of Anti Hacking" has conducted several in-house training at top companies like Deshaw, Mjunction, CESC, National Power Grid, Banks; where our ethical hackers have shown LIVE demos of Hacking. This is the new form of training where you not only read and hear, but see practical demonstrations of the consequences of cyber security mistakes. This gives the best awareness. What you see is what you believe.

### MITIGATING THREAT SITUATION

Organisations have always invested in perimeter security as the endpoint was supposed to be in the trusted zone. Now with employees working from anywhere and everywhere, companies will invest a lot on endpoint security, as well as the authentication and authorisation tools and techniques. VPN, privileged access management, etc. will be the key technology. Cloud adoption which was mostly for the servers, now will also be used to put desktops on cloud, so that employees log into virtual offices in the cloud and all data is still in control with the organisation.

### SAFEGUARDING CUSTOMERS & EMPLOYEES

People have always been the weakest link whether they are working from home or office or client site. Providing them awareness is the key solution. The awareness should be in a language which they can relate to their day to day operations. Coupled with real life case studies related to their work, and focussing on the consequences proved by some LIVE demo, can open up their eyes. Usually companies make mistakes of making content which appears to be preaching without giving much insight. Organisations must think of people behaviour and award people who not only help to embed security in the company culture, but also bring innovation into the rapidly dynamic cyber security in today's world.

## TRAINING – THE ONLY MANTRA OF SUCCESS IN CYBERSECURITY

**DR. CHITRANJAN KESARI**
CIO & IT Head, Ahuja Hive Ltd. (Fosun Group)

### MEASURES ADOPTED FOR COMBATTING THREAT

Technology is playing great roles to safeguard our network. But when work from home is coming, all technology installations in corporate premises are not helpful to safeguard our users. A little contribution of user training for cyber security for basic things helps us in the long run.

### EDUCATING CUSTOMERS & EMPLOYEES

Education about cyber security plays an important role in our company and on customer sites also. My continuous training about basic cyber security helps our users.

### MITIGATING THREAT SITUATION

In our industry of construction, engineering and real estate, customer data and design are very important. As we are using ransomware protected information security solutions and backup on the great platform with reliable DNS protection solutions help us in protecting our data.

### UPCOMING THREAT

Plenty of problems happen and deepfake is one of the same as we as well as the government is also facing the same issues. Lots of people are facing the problem and losing lots of money due to this. I only tell that the fake has always been fake. Take your decision wisely by dealing with any person or call, or online links.

### SAFEGUARDING CUSTOMERS & EMPLOYEES

This is very challenging these days as users are using work from home environments to work and this is going to stay for safety and companies are saving lots by using work from home environments. But security is one of the concerns and regular interaction and training of our users help us for protection. Cyber security training for users plays important roles. Training, Training and Training is my mantra for success in cyber security.

---

## "DEEPFAKE THREATS ARE GROWING POTENTIALLY ALONG WITH SIGNIFICANT GROWTH IN AI/ML TECHNOLOGIES"

**DR. SAYED PEERZADE**
Group Chief Information Officer, Reliance Big Entertainment, Reliance Group

### MEASURES ADOPTED FOR COMBATTING THREAT

We are a digitally matured organisation, well ahead in curve on implementing the new age technologies, experimenting and bringing the things stability. Being in the worldwide operations and headquartered in Mumbai, most of remote connectivity essentials like Uniform Threat protection, Firewalls, and VPN's, AV protection, DLP's were in place. Only change in this pandemic is even regular office employees need to be shifted to home and for us it is just extending these services to everyone. We are the fastest of the lot in industry who moved to WFH and did not face single downtime on any of users because of cyber risk issues.

### MITIGATING THREAT SITUATION

We have mitigated all attacks effectively. In my point of view Network design and Data centralization are a major enemy of cyber threats like ransomware and that most of regulatory efforts increasingly push against this. From a CIO point of view or DPO's perspective, opting for decentralized, interconnected data sources is not only a more agile and efficient way to access only the data you need but actually mitigates machine learning risk. Due to faulty network design individual attacks can spread to other devices within no time. User awareness also plays a very important role here. We have the following processes inside organisations below enterprise wide for IT teams and endpoints, apart from decentralised network and data design. Decentralised networks will help in isolating the attack quickly before it spreads to all of the network.

### UPCOMING THREAT

As technology moves ahead, there is a parallel industry working on exploiting the new techs. Deepfake is one of them. Cybersecurity as a large has to act on every single threat and deepfake is no exception. Deepfake threats are growing potentially along with significant growth in AI/ML technologies. In the engine, deepfakes is not enchantment, it is pure mathematics. The application utilizes deep learning application, which implies it depends on neural networks to play out its functions. Neural networks are programming structures generally planned after the human brain. When you give a neural network numerous examples of a particular kind of data, state photos of an individual, it will figure out how to perform functions, for example, recognizing that individual's face in photographs, or on account of deepfakes, replace another person's face with it. However, as deepfake innovation improves, the tech business will probably play a smart game to try to remain one stride ahead that does not imply that staying aware of deepfakes is outlandish. New AI-based tools that identify frauds will probably help significantly, as will automated tools that can compare digital artefacts that have been filed by various companies and track changes in them after some time.

### SAFEGUARDING CUSTOMERS & EMPLOYEES

It is a wide topic to discuss. However, we can always summarise the four important aspects - Thought, Security, Culture & team. What is that 'thought' process needed to bring digital innovations, what is the 'security' role in these transformations, how to bring 'culture' of innovations, how to build an effective innovative 'team', and sustain innovative approach in the organisation for both business growth and security.

With security regaining priority in digital strategies, CISOs are definitely dispersing security responsibility throughout the organization and working to transform the IT culture.

My thought process of digital transformations and security combines, which I always put forward during all of my discussions

Transformations should be aligned to organisational business goals

Bring the transformations throughout organisation

Information Security should be a part of the Digital design, be it product or platform.

## AN INFORMED CITIZEN IS THE BEST DEFENCE AGAINST DEEPFAKE

**DR. RAJEEV PAPNEJA**
Chief Growth Officer, ESDS Software Solution

### MEASURES ADOPTED FOR COMBATTING THREAT

Work-from-anywhere is not something new for IT companies such as ours. Our employees have been used to this but for many of our customers this has brought in a paradigm shift in their way of working. The first and most important thing is to be vary of the fact that no matter where we work from, systems are vulnerable as soon as they are connected to the network. Layered defence mechanism works best for any kind of security, be it physical or virtual. It is important to identify the attack points in the landscape.

For example, if someone is using a SaaS application, the attack points besides the endpoint would be the data in motion over the Internet, data at rest, data during processing, the virtual machine itself that can be compromised, and the SaaS application which could be vulnerable. Every attack point has different ways of making them secure.

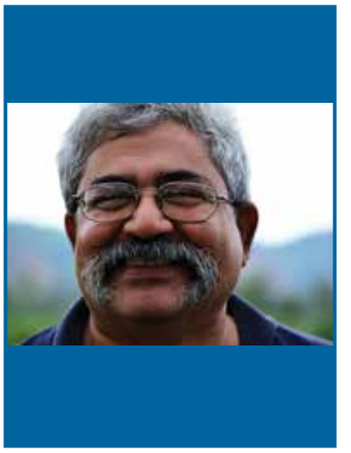
We should make sure that the basics are not neglected as part of the security framework, something as simple as having updated antivirus running on systems. Use of trusted and encrypted WiFi connection, https for secure connection over Internet or use of Web VPN etc. should be part of the defence mechanism. While technology can help us, the most important thing is to educate the customers and employees about the types of threats such as email phishing, link jacking, unsecured WiFi connections etc., and common safety measures for keeping their work safe. It would also make sense to promote mandatory backups and frequent password recycling which are real basics and mostly overlooked.

### UPCOMING THREAT

Deepfake is, and will be one of the most damaging threats in coming times. It has the power to bring down nations, forget an organization, by creating communal violence for example, by simply creating few doctored videos. We see a lot of doctored videos today floating on the internet and WhatsApp, and these videos can sometimes cause unrepairable damages.

As AI/ML technology is maturing, supported by the advances in neural networks and deep learning, it would not be surprising if the original video looked fake against the fake one. With the technology available in every common person's fingertips, we are sitting on a potential time bomb. With all the nuclear weapons and military on one side, and few Deepfake images/ videos on another side, it would be difficult to gauge which side can cause more harm to a nation. As mentioned before, technology can be used to mitigate the risks, but till then it goes back to the basics of educating the people of the possibilities and increase awareness. An informed citizen is the best defence against such threats.

## "THE 'DEEP FAKE' CAN BE WELL COUNTERED WITH THE 'DEEP TRUST'"



**JAIDEEP KHANDUJA**
Chief Technology Officer, AccioMango Pvt Ltd

### EDUCATING CUSTOMERS & EMPLOYEES

Pandemic has transformed the whole concept of automation, digitalization, and IT security in a very different manner. Gone are the days of virtualization and digitalization of an organization within the boundaries of its physical existence. The same goes true for boardroom to boardroom virtualization and digitalization. The organizational perimeters have expanded to the homes of its employees. Each employee's home has become his or her workplace.

Hence, that each endpoint having different geography was supposed to be strong in terms of security as an endpoint within the organizational boundaries. The immediate role of the organization was to make each individual accessing the servers and databases from 'anywhere' be more cautious and aware about it. IT training had a complete paradigm shift to build a new kind of strong security culture.

### MITIGATING THREAT SITUATION

I do not think threats and vulnerabilities have increased or this new situation will open more gates for attacks provided appropriate measures, checks and controls, and real time audits are there as a new layer of security to handle work from home or work from anywhere kind of situation. 'No Trust' is the best way to handle it. Hardware, be it a smartphone or a laptop at home, needs to be scanned thoroughly every time it connects to the business applications.

### UPCOMING THREAT

Deepfakes are the next threat on which cybersecurity has to act on. Rather, it has already started. But in my opinion, besides technology, HR and organization has a highly demanding role in this to build each workforce as a fully trusted warrior of the organization. The 'deep fake' can be well countered with the 'deep trust'. So, basically 'No Trust' and 'Deep Trust' will go hand in hand provided the organizations know what it means.

### SAFEGUARDING CUSTOMERS & EMPLOYEES

I think banking is the best example of this. Even before pandemic we all were (and are) doing mobile banking or online banking. For banks, every customer and every transaction is crucial. It is now required for every organization's business applications to be well equipped with stronger security layers (software & hardware) as well as appropriate checks and controls.

## "ESTABLISHING A CULTURE OF AWARENESS AROUND CYBER-SECURITY IS CRUCIAL TO THE ONGOING INFORMATION SECURITY"

**KAPIL MADAAN**
CISO, Minda Corporation

### MEASURES ADOPTED FOR COMBATTING THREAT

Since the COVID-19 pandemic started approximately one year ago, the world has changed in many ways. The biggest, most damaging and most widespread threat that all businesses are facing is phishing attacks. They have grown approximately 65% over the last year, and they account in billions in business losses.

A Cyber security leader strategy is needed, as the attack surface grows, and we rely more on digital technologies in all areas of business and industry. Cybersecurity challenges are increasing and cyber resilience can help organizations prevent, detect, respond, and recover.

The functions—Identify, Protect, Detect, Respond, and Recover remind us of how important it is to balance proactive safeguards while preparing for worst-case scenarios. This balance is especially important in all the business settings where a worst-case incident could drastically affect the solvency of a business

### UPCOMING THREAT

Deepfake is going to be the biggest threat. Deepfake, a combination of the words 'deep learning' and 'fake'. I will suggest preparing strategy against such incidents.

Social engineering attempts & Email based phishing – Make Employee training and awareness mandatory. By offering adequate training and creating awareness employees can be turned into an additional line of defence.

Plan, Act & Response Strategy – Ensure that your organization is ready to adequately respond to such incidents.

Further So many Security service providers are working on an AI-powered deepfake detection software for this purpose. The tool can automatically analyse videos and photos to provide a confidence score that the media has been manipulated.

### SAFEGUARDING CUSTOMERS & EMPLOYEES

Remote workers are typically the first to face security threats. They are often the source of network security incidents that can wave quickly through the rest of the organization. Even if we do not have remote employees, mobile devices like smartphones and laptops pose security risks.

Now the Cybersecurity leader role comes in picture to prepare strategy. We have to think from a broader perspective like Application Security, Network Security, Endpoint security, Email Security, IoT Security and so many based on the environment.

From support to strategy and set the culture, while most companies recognise the pressing need for technical security measures, without a culture of security in the workplace, the risk of threat can remain high. Human error can very quickly and easily undo even the most stringent digital protection, so establishing a culture of awareness around cyber-security is crucial to the ongoing information security.

---

## STRENGTHENING REMOTE PROTOCOLS WITH MULTIPLE INTERFACES AND SET UP OF STRONG LOCAL SECURITY POLICIES WITHIN LAPTOPS CAN MITIGATE RISK

**DR. HARSHA E THENNARASU**
Chief IT & Cyber Security Advisor, HKIT Security Solutions

### MEASURES ADOPTED FOR COMBATTING THREAT

Customers must ensure, are there any vulnerabilities that are residing in their laptops, those are major challenges for customers. Their laptops might consist of hidden BOTs and malware, spyware, etc., employee safety depends on the customers, IT and security guys to ensure patches and updates, etc.

### EDUCATING CUSTOMERS & EMPLOYEES

Regular webinars and video conferences are being used to bring continuous awareness. Increased the frequency of training from quarterly to monthly and bimonthly. Also we have designed an online survey type assessment which can evaluate the understanding of the employees.

### MITIGATING THREAT SITUATION

We have a solution like MDR with a proactive approach and instant response on the incidents reported, not being allowed to reach to employees. Even if there is any new variant of ransomware, employees are well educated to understand malicious files received and links over email. Even we have customized rules to block file less Ransomware.

### UPCOMING THREAT

There is an increase of traditional malware/viruses/spyware with new methodologies, where industry is overlooking these vulnerabilities. More raise on file less ransomware is expected, those are targeted through simple text codes which are compiled by local svchost.exe file and compile ransomware internally by passing all security mechanisms built around.

### SAFEGUARDING CUSTOMERS & EMPLOYEES

By strengthening remote protocols with multiple interfaces and set up of strong local security policies within their laptops, can mitigate the risk. Which is the only solution to prevent security breaches on remote workers. Definitely cybercriminal will have less mileage.

# OEM's are reinventing their security strategies

**The 2020 ongoing pandemic is still alive and remote working for many companies too. Ransomware attacks, cyber threats, cyber-crime is still going on, with this now a new cyber fear- Deepfake has cropped its head and is making its way to the cyber fear world.**

**A few Cyber gurus have shared their information with VARIndia to fight against the ongoing CyberWar.**

**Here's what each has to say:**

## AKAMAI- ANOTHER NAME FOR BEST EDGE SECURITY SOLUTIONS

### Prasad Mandava
### MD India & VP of Engineering at Akamai Technologies

**Measures adopted:** Remote working has caused new opportunities for cyber criminals to take advantage of the security trade-offs by individuals for ease of use and access to engage in credential stuffing attacks. The most common security threat seen during the pandemic is primarily based on phishing scams. As work from home continues, multiple measures are needed to be followed by the enterprises to protect the data.

Securing Enterprise Assets became of major importance as more enterprise servers, applications, and services become accessible to remote users.

**Protect and Secure Remotely Connected Devices:** As working from home will become a norm, and more devices will be connecting with the enterprise asset, it will become even more important for an enterprise to enhance the security aspect to cut down moderation.

**Reducing the Attack Surface from Threat Actors:** The Zero Trust approach, if enabled, will reduce the malicious and threat actors attacking major company devices, putting all data and security under direct risk.

**Mitigating threat situation:** Akamai's API security is mission-critical for organizations to develop partnerships, create connections for employees, and enable modern application architectures. For security teams who are looking for more comprehensive protection. Akamai offers some of the best edge security which gives one full control over security implementation with the following solutions:

**API Gateway -** It takes care of the business management and governance of your API traffic.

**Kona Site Defender –** It provides the same automated rule set plus a positive security model that can be further enhanced with client reputation to provide a reputation score on suspicious IP client behavior.

**Bot Manager Premier –**This enables security teams to manage exponentially growing good and bad bot traffic.

In the spirit of remote working and rapid innovation, secure API solutions can protect your system from DDoS attacks and protect your infrastructure improving your security controls and services.

## "SECURITY IS THE BEDROCK OF WHAT CITRIX HAS DONE FOR MANY YEARS"

### Ravindra Kelkar
### Area Vice President, Indian Subcontinent, Citrix

**Measures adopted:** Innumerable organizations across the globe are tackling cyber security threats and data breaches at any given time. With applications being modernized for web-based access and deployed in multi-cloud environments, the traditional VPN model does not adequately meet the needs of the evolving use cases and falls short on end-user experience and security. By implementing Zero Trust approach or a VPN-less access business can eliminate the need to maintain VPN servers and limit access to specific IP addresses.

Bad actors are targeting web and cloud applications via the local internet connections that remote workers use. Secure access service edge technology (SASE) delivers security services like web filtering, data loss prevention, and next-generation firewalls to protect these workers across a network.

Way to tackle this is Fast Identity Online (FIDO2) authentication which enables users to prove their identity using biometrics, mobile devices, or specialized security tokens.

**Mitigating threat situation:** Security is the bedrock of what Citrix has done for many years — securing apps, access, networks, data, and endpoints. Our solutions let employees work securely, the way they want. As mentioned earlier, SD-WAN networking solution can help the IT teams improve monitoring, and overall security. Our virtualization and container-based solutions help organizations isolate environments.

Password-less multi-factor authentication (MFA) also helps add an additional layer of security to users, devices, and resource authentication, authorization, and access.

All these combined, can help organizations become more robust and resilient to any huge, unprecedented wave of disruption in the future without compromising the security and privacy of the organization.

**Upcoming threat:** Deepfakes are becoming more and more sophisticated with time. The algorithms associated with it are also evolving rapidly. These factors combined have made it increasingly challenging to combat the threats and their adverse consequences. Additionally, with the increasing amount of work and content being accessed and shared online due to the pandemic, the use of deepfake video and audio technologies is expected to evolve into a major cyber threat to businesses within the next few years.

# CYBERARK ADOPTED TOOLS AND PROCESSES ENABLE EMPLOYEES TO SHIFT TO REMOTE WORK SEAMLESSLY

**Rohan Vaidya**
**Managing Director – India, CyberArk**

**Measures adopted:** As remote work strategy is being implemented for the long term, distributed IT environments are only going to continue to expand. Adoption of public cloud services, SaaS applications and remote access have dissolved the traditional network perimeter, so authentication and authorisation of all identities become paramount in order to stop the organisation's critical data and assets being potentially accessible in many more ways than previously possible. Identity becomes the key line of defence for most organisations and the de facto 'new perimeter.'

**Mitigating threat situation:** Ransomware is a type of malware designed to infect machines, encrypt files and hold the needed decryption key for ransom until the victim submits the required payment. Ransomware attacks on enterprises and government entities – cities, police stations, hospitals and schools – are on the rise, costing organisations millions as some pay off the attackers to untangle themselves and restore vital systems.

Research by CyberArk Labs has evaluated what mitigation strategies are most effective against ransomware. One of the key findings is that when local administrator rights were removed and application control policies were in place with a solution like CyberArk Endpoint Privilege Manager, 100 percent of ransomware samples were prevented from encrypting files. We also use application grey listing to proactively defend against previously unknown ransomware variants. With a greylisting approach, you can restrict read, write and modify permissions for unknown applications to prevent ransomware from encrypting data. You can also use greylisting to block access to network drives to prevent ransomware attacks from propagating across the enterprise.

**Upcoming threat:** Video and recordings of executives and business leaders are readily available across marketing collaterals, social media channels, and more. Attackers could coordinate deepfakes from these properties as a strategic follow-on to phishing attempts (which will also move away from email to other platforms like chat and collaboration apps) to make manipulated communications feel even more authentic.

For example, phishing emails spoofing IT asking for passwords are common. Attackers could also use manipulated videos of executive leaders on social channels to entice customers, employees, partners and more to click on malicious links – creating broader new attack avenues for malicious actors.

**Safeguarding customers & employees:** We at CyberArk have adopted various tools and processes which allow employees to shift from working in designated office spaces to remote work seamlessly. We collaborate with our colleagues across the globe in different time zones and different physical locations to ensure that the best talent is available to work with our customers using various workspace collaboration tools, from Slack to Teams to Webex. Our end devices are secured using combinations of security tools, including Endpoint Privilege Manager (EPM) which allows our employee to work effectively from any location around the globe. Our helpdesk team works round the clock to support our global employees.

# "F5 ENABLES ORGANIZATIONS TO SECURE AND DELIVER SUPERIOR DIGITAL EXPERIENCES"

**Santosh Matam**
**Security Manager, F5 Networks**

**Measures adopted:** Traditional perimeter security depended on firewalls, VPNs, and web gateways that separate trusted from untrusted users are blurred. Protection is now needed where applications and data, and users and devices, are located. As work from home continues, implementing a Zero Trust approach should be the priority for CISOs, their security teams, and users. We are fortunate that there are devices accessible today to shift to remote work seamlessly. With a robust application security portfolio and ability to secure the new control points in a Zero Trust environment, F5 provides the building blocks necessary to address a "Never trust, always verify" approach to securing today's applications, and also adds a third principle to Zero Trust, "Continuously monitor".

**Mitigating threat situation:** Ransomware continues to be the prevailing form of malware used by attackers for illicit gain and to cause disruption. According to the F5 Labs recent Phishing and Fraud Report 2020, phishing continues to be a popular enabler of ransomware and nearly 72% of phishing links send victims to HTTPS encrypted websites. A common security hole—and one that is easy to close—is weak authentication on Internet-linked logins. Locking down Internet-linked logins with better authentication is the first step organizations should take to protect against ransomware, ideally using multi-factor authentication. If you can't manage that, then at least make sure default passwords and known leaked credentials are changed.

Another common entry point for ransomware is a drive-by download, where attackers will trap websites with browser exploits that inject their ransomware. This means a user surfing a site and viewing a weaponized banner ad can unwittingly land ransomware on their network. These attacks typically leverage one of the much vulnerability in web browsers, web scripting languages, and web animation tools.

**Safeguarding customers & employees:** Phishing is a growing problem as an unprecedented number of unaware and unprotected users and devices are connected. The 2020 Phishing and Fraud Report found a 15% annual increase in phishing attacks in 2020 as well as an increase in phishing domains using HTTPS and sophisticated URLs.

An organization may have employees working from around the globe. Because of this, old access security measures are no longer enough and must be replaced with safeguards that allow employees and other verified users safe and secure access from anywhere, on any device, at any time. F5 enables organizations to secure and deliver superior digital experiences. For organizations adopting Zero Trust architecture, F5 BIG-IP APM delivers the industry's most scalable access management solution, APM consolidates remote access, web access management, and Identity Aware Proxy (which helps drive Zero Trust Application Access), enabling organizations to enable the formation of a secure application access that their organization and users require.

# MANAGEENGINE BE ABREAST OF LATEST SECURITY ATTACKS AND MITIGATION STRATEGIES

**Ananthakrishnan Vaidyanathan**
**Product Manager, ManageEngine**

**Measures adopted:** For employees, it is imperative they provide full visibility into their work-from-home setup for easier implementation of adequate safety measures to ensure corporate data is always accessed through authorized devices on secure networks.

For customers, the best option is to be alert. If there's even an inkling of doubt about the legitimacy of files or links, it is always safe to refrain from clicking or opening them to prevent falling victim to phishing attacks. Another option is to ensure you update enterprise software only from the product website to avoid installing malicious updates.

**Educating customers & employees:** As a company dealing with cybersecurity products, we, at ManageEngine, organize regular training webinars and online meetups to ensure all our customers understand the current security environment and how to best utilize the products at hand to ensure optimal security. We also regularly share checklists and questionnaires for customers to periodically check on their setup and be abreast of the latest security attacks and mitigation strategies.

**Mitigating threat situation:** ManageEngine's dedicated suite of endpoint security and management products lets you manage different servers, workstations, smartphones, and other types of endpoints running different OSes, all from a centralized console. It lets you authorize entities such as endpoints, apps, peripheral devices or even the employees themselves before accessing enterprise data thereby protecting enterprise data at rest, in use, and in transit.

**Safeguarding customers & employees:** We, at ManageEngine, have been constantly striving to come up with products that cater to the advancing security needs of enterprise, and 2021 will represent yet another step in that direction just like the last year. In 2020, we launched a suite of products that provide UEBA capabilities for threat analytics, enforce the principle of least privileges (POLP) as well as products that grant just-in-time privilege elevation to ensure a secure Zero-Trust setup. One of our core commitments this year is to bring in AI and ML into our entire suite of solutions to build security models that proactively identify attacks and recognize underlying user actions before mitigating them.

# "CYBERSECURITY AWARENESS FOR OUR CUSTOMERS AND PARTNERS IS ONE OF THE KEY FOCUS AREAS FOR SOPHOS"

**Sunil Sharma**
**Managing Director Sales, Sophos India & SAARC**

**Measures adopted:** As many companies are adopting WFH as a permanent company policy or even the adoption of hybrid working solutions, this shift has certainly caused some critical challenges for businesses in terms of cybersecurity. Some of the protective measures we recommend are:

Ensure devices and systems are fully protected and security solutions are up to date with the latest patches and versions. All too often malware breaches an organisation's defenses via an unpatched or unprotected device.

Create a secure connection back to the office using a Virtual Private Network (VPN) ensures that all the data transferred between the home user and the office network is encrypted and protected in transit.

Scan and secure email and establish healthy practice

Home working has led to a big increase in email as people can no longer speak to colleagues in person. The crooks are wise to this and are already using phishing emails to entice users to click on malicious links. Ensure email protection is up-to-date and raise awareness of phishing.

**Enable web filtering**

Applying web filtering rules on devices will ensure that users can only access content appropriate for 'work' while protecting them from malicious websites.

Make sure people have a way to report security issues

With home working people can't walk over to the IT team if they have an issue. Give people a quick and easy way to report security issues.

**Educating customers & employees:** We have a dedicated tool-Sophos Phish Threat that provides phishing attack simulation and training for end users. It helps our customers to nurture a culture of positive security awareness. Effective security training is also a part of Sophos Phish Threat, available through Sophos Central, which is a cloud-based management platform. Additionally, our customers can take advantage of more than 30 security awareness training modules, covering both security and compliance topics. Sophos Phish Threat integrates testing and training into simple, easy-to-use campaigns that provide automated on-the-spot training to employees as necessary.

**Upcoming threat:** Sophos Intercept X combines ransomware protection, deep learning malware detection, exploit prevention, End Point Detection and Response (EDR) - all in a single solution. Sophos' synchronized security strategy enables multiple security products to work together seamlessly with simpler management and better security. It allows Sophos endpoint (Intercept X) and firewall (XG firewall) to share threat intelligence, and provide faster comprehensive protection against advanced threats like ransomware.

**Safeguarding customers & employees:** Sophos has always been prepared for the reality of a remote workforce. Additionally, our Sophos partners can easily provide cybersecurity solutions and services to their customers, by using the many options from our portfolio that secure the current fluctuating protocols around remote working such as in Sophos' RED (Remote Ethernet Devices), VPNs (IPSEC and SSL), virtual firewalls, and synchronized security.

# MAINTAINING GOOD PASSWORDS AND PASSPHRASES IS MANTRA OF CYBER SAFETY

### Sandeep Bhargava
### Managing Director APJ, Rackspace Technology

**Measures adopted:** Threat actors can be disastrous to an individual or organization, and it is the job of security professionals to ensure that proper security measures are in place to protect against it. For example, it is a good idea to ensure that the business has backups of its critical data so that an attack does not immobilize the organization for an extended period.

**Things to be kept in mind to safeguard remote workforce:** Use firewall protection solutions: Firewall solutions can leverage a single-pass architecture designed to prevent network vulnerabilities, block the download of known malware, and prevent malicious encrypted content from circulating around your network.

Back up the data. Maintaining recent backups of your data is essential. Companies that follow this fundamental best practice can safely ignore ransom demands and revert to stored files with little data loss.

Keep up with patches and check your security software. Merely keeping up with the latest patches for Windows, Mac, and Linux operating systems and your third-party applications will go a long way to reducing your exposure to ransomware.

Be sure that the security software installed and that it's up-to-date. New malware surfaces every day, so keeping current with your anti-virus software helps keep your data safe.

Educate staff to spot scams. Employee awareness is crucial in avoiding a ransomware attack. Staff should be coached on how to spot scams and urged to take the time to pause and check emails that don't look right.

Take the "Security First" approach. Weave security awareness and practice into the process from beginning to end. DevSecOps is a concept that emphasizes the importance of integrating security into all parts of IT system development and operations, rather than leaving them disconnected. While perfect security is not possible, concepts like this bring it closer.

**Educating customers & employees:** At the onset of COVID-19 and the shift to Work from Home one of our key priorities was ensuring that an open line of communication was established between Rackspace Technology and our customers. In fact, we looked to over communicate in order to ensure customers knew how and who to reach out to during this time. Over this last year we've looked to educate and support our customers, including setting up roundtables on security with global experts available to answer questions and give advice, we've ensure customers know who to reach out to in our customer success team in order to guide innovation and secure infrastructure from possible attacks.

**Safeguarding the customers and employees:** One of the most important ways to safeguard customers and employees is to put in place policies to guide staff to better help them understand their responsibilities and what is acceptable when they use or share data, emails, internet sites and additional computers and devices. It's important to make sure the staffs knows about the threats they can face and the role they play in keeping the business safe. All should know how to maintaining good passwords and passphrases, how to identify and avoid cyber threats, what to do when they encounter a cyber threat and, importantly, how to report a cyber threat.

# "MCAFEE WORKS TOWARDS PROTECTING EVERY ASPECT OF A CUSTOMERS' DIGITAL EXPERIENCE"

### Vamsi Ponnekanti
### Head of Technical Sales, India & SAARC, McAfee

**Safeguarding customers & employees:** McAfee works towards protecting every aspect of a customers' digital experience - from device to the cloud. The company is responsible for protecting over 680 million+ total endpoints and provide security solutions to over 97 million enterprise endpoints, which include 75% of the world's Fortune 500 firms.

For employees, McAfee's robust set of SaaS applications provide a secure environment to work remotely and get work done with ease. Together, we are working on developing stronger defences to ensure that the 'future of work' is a secure one.

**Educating customers & employees:** Implementing a cloud-based secure web gateway so corporate devices can be protected against web- based threats without routing through VPN.

Allowing employees to connect to sanctioned cloud services from their corporate devices without using their VPN, protecting data with a cloud access security broker (CASB).

Setting policy in your CASB so that cloud services have device checks, data controls, and are protected against attackers who can access SaaS accounts over the internet.

Implementing multi-factor authentication for sanctioned cloud services where applicable to reduce the risk of stolen credentials being used to access accounts.

Letting employees use their personal devices to access corporate SaaS applications to maintain productivity, with conditional access to sensitive data in the cloud.

**Upcoming threat:** While deepfakes technology is at a relatively nascent stage in India, considering its quick proliferation, it is essential to develop guidelines and regulations to curbits rampant misuse. Effective monitoring and punishable laws for such offences will be crucial in controlling this menace before it causes irreversible damage. Until then, it is up us as consumers to remain resilient, cautious to defend ourselves from the dark world of deepfakes.

## "RISK-BASED VULNERABILITY MANAGEMENT (RBVM)- THE PROCESS OF REDUCING VULNERABILITIES ACROSS AN ORGANIZATION'S ATTACK SURFACE"

**Kartik Shahani**
**Country Manager, Tenable India**

**Educating customers & employees:** Employee awareness regarding the importance of multifactor authentication, software updates including patches, and awareness of phishing and other tactics used by bad actors to access networks is foundational and should not be underestimated.

However, the onus of ensuring the security of a business lies with the organization. With employees working from home and using personal and work devices - each device, each asset in the infrastructure needs to be considered as potentially becoming rogue. Therefore security teams need to continue to minimize privileges where necessary and the attack surface to which they have access.

A lot of the issues organizations are facing are simple foundational things that they're not doing well such as patching. By and large, the MO for most cybercriminals — whether they be rogue actors or state-sponsored — is the path of least resistance: they're getting in through known but unpatched vulnerabilities. Security teams within organizations need to get the basics right, address vulnerability patching diligently and implement the right security controls.

**Mitigating threat situation:** To avoid falling victim to ransomware, organizations need to implement security awareness training and a risk-based vulnerability management program. Security awareness training can help thwart the threats posed by malicious spam and phishing attacks. When it comes to vulnerabilities, it is crucial to observe that with the number of vulnerability disclosures constantly climbing, keeping on top of them can seem insurmountable.

Risk-based vulnerability management (RBVM) is the process of reducing vulnerabilities across an organization's attack surface by prioritizing remediation efforts based on risk. Put simple, RBVM is about understanding vulnerability risk in the context of threat and business impact. By focusing on the vulnerabilities that are both dangerous and likely to be exploited, organizations can make the best use of their resources and increase the return on their risk management investments.

**Safeguarding customers & employees:** Most remote workers have a variety of connected devices such as smart television sets, doorbells, baby monitors and more in their homes in addition to their laptops and tablets. This means that every time a remote employee logs into their laptop, each of those devices becomes part of the enterprise attack surface. Since security teams won't be able to run network vulnerability scans of personal devices, installing local vulnerability detection agents to provide off-network visibility is beneficial. Risk can also be mitigated by adding IT systems management onto laptops so that the security team can control software updates and patching. This is a simple, but effective strategy.

# VARs ARE GEARED UP TO TAKE CYBER SECURITY AS AN OPPORTUNITY

**After the unprecedented time of lockdown and the beginning of the new normal, businesses all over the world are facing newer challenges. The year 2020 has seen a surge in crimes and growing in 2021 as well. One of these is the danger of the Deep Fake technology, which can be used to make users believe something is real when it is not. This poses a major threat to businesses across the globe as it can be used to deceive people online. Deepfakes will also likely increase extortion attempts against influential business leaders. It also has significant potential to enhance market manipulation attacks in addition to scams and direct impersonation. On this backdrop, industry leaders have shared their views.**

### "TO HAVE STRONG FIRST LINE OF DEFENCE, EMPLOYEES AND ASSOCIATES NEEDED TO EDUCATE"

**VIBHORE SHRIVASTAVA**
MD, VIBS Infosol

**To keep customers safe:** We realise, apparently, customers have started discussing of security at first. Our enterprise customers were earlier more concerned about perimeter security and basic endpoint management solutions, however, with the sudden rise in cyber threats and different attack patterns, they are now looking for endpoint threat management suite, including anti-malware, anti-Ransomware, EDR, MDR, APT, encryption, anti-phishing, APT, Email Security and many more.

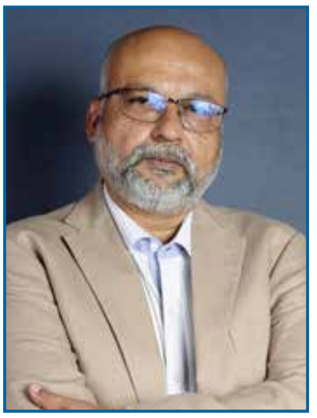
Thanks to all our customers who engaged us at the initial phase and treated VIBS as their trusted advisor in difficult times. Our solid inputs are real value to them to manage major cyber threats and malicious acts during work from home / work from anywhere.

**On educating customers:** We all have great expectations from 2021 since last year was full of struggle for most of the businesses. However, this year, with hope there are more serious threats associated. There are multiple ways to address and build a strong secured environment. Most importantly, out of all, is to manage and control our internal threats. Report claims, major setback happens due to lack of awareness and negligence by internal team. To have a strong first line of defence, we need to educate our team, employees and associates.

**Safeguarding the customers and employees:** In 2021, Cyber security trends flow majorly towards Endpoint management suite, Network optimisation, Email protection and secured cloud practices. We were the early technology adapters & Solution partner to bring immediate protection for unknown threats to our large enterprise customers. We had arranged many interactive knowledge sharing sessions with customers & our own employees to enhance their learning curves and to ensure the ability to serve in critical times for unknown threats.

## 'STRAIGHTFORWARD METHODOLOGY CAN HELP TO PREPARE FOR THE IMPACT OF MALICIOUS ATTACKS'

**PRASHANT JAIN**
CEO, JNR Management Resources



**The upcoming threat:** To help define an adequate response to the growing deep fake threat, we in our organization have brought together our security experts and team. By doing this we have designed a straightforward methodology that you can implement to help prepare for the impact of malicious deep fake attacks. This methodology is based on three pillars:

- **Employee training & awareness:** By offering proper training to the employees and increasing awareness employees can be turned into an additional line of defense.
- **Detection:** Detecting the fraudulent media beforehand can minimize the risk to the organization.
- **Response strategy:** We are making our organization ready to adequately respond to the deep fakes.

**Safeguarding the Customers and Employees:** As most employees work remotely, we educate our employees on key cyber risks and arrange training sessions so that they can learn how to spot threats and be an effective line of defense for their organization.

With advancements in technologies like Cryptography HSM, SSL Certificate, Encryption, & Digital Signature we can be assured that we are keeping our data and our clients/users' data safe & secured.

**To keep customers safe:** With advancements in technologies like Cryptography HSM, SSL Certificate, Encryption, & Digital Signature we can be assured that we are keeping our clients/users' data safe & secured.

## 'EVERY ORGANIZATIONAL EMPLOYEE SHOULD BE MADE AWARE OF THE EMERGING THREATS VECTORS'

**V.ANAND**
CEO, Raksha Technologies

**To keep customers safe:** The current situation has increased the number of teleworkers to multifold than what organizations have factored for. We have also seen a rise in the number of security breaches. Organizations must relook into their infrastructure, invest in tools of new age that ensure secure connectivity to access public & organization resources and manage every endpoint connecting the organization. Organization should ensure visibility into the security incidents which can be prioritized & remediated. Customers should also conduct periodic training to all employees on security awareness as end user ignorance on cyber hygiene is the major contributor to security breaches.

**The upcoming threat:** An emerging threat in cybersecurity space, Deepfake that uses the artificial intelligence to recreate fake data. Though it is said to be still emerging, the estimate of the impact looks high. Every organizational employee should be made aware of the emerging threats vectors, enforce a data policy to make sure data is available to the right people only & detection mechanisms are fine tuned to detect and prevent any data exfiltration.

**Safeguarding the customers and employees:** Being a trusted security partner, we keep our customers aware of the market trends, best practices, threat information, tools that customers could leverage to detect, contain, remediate & reinforce security of their infrastructure & sensitive data. We also extend our wide range of consulting, implementation, managed services that helps customers to bridge the skill gaps. We ensure the best of our services are delivered at all times.

## "OUR ENDEAVOUR IS TO SAFEGUARD IT SYSTEMS FROM CYBER-ATTACK AND TAKE IMPERATIVE STEPS"

**VIPUL DATTA**
CEO, FutureSoft Solutions

**To keep customers safe:** FSPL has always been customer centric and proactive in educating and keeping our customers informed about various checks adherence whilst moving from work from home to work from anywhere.

We are in regular touch with our customers and man-oeuvre our discussion on investing in solid technical infrastructure that will support their legacy and modern applications, their investments into identity and access management, in the cloud, in modernizing their network architectures and maintaining Security standards and solutions for more secure remote work in the longer term on connections and devices, operations and access and while co-ordinating internally and externally.

**Safeguarding the customers and employees:** As our customers and employees work remotely, our endeavour is to safeguard their IT systems from cyber attack and take imperative steps to protect them against cyber risks namely;

1. Assess core IT infrastructure regularly
2. Secure applications and devices
3. Embed cybersecurity into business continuity plans
4. Update access and security measures in short intervals

**The upcoming threat:** Deep fake is a combo of Deep learning and AI based technology, "Fake" which is used to alter images, audio, video etc.

With the world more connected by digital media and the costs for creating deep fakes slumping dramatically, this emerging technology can pose a serious risk. As workplaces have become virtual, due to Covid19, video conferencing and other digital tools pose a threat and an opportunity to be deceived.

At FSPL, we explore the benefits and risks of new technologies by applying a multi-disciplinary lens. We focus on preparing, protecting, detecting, responding and recovering all points of the security lifecycle and define a response in line to the threat. We are also prompt in preparing employee training and awareness, detecting false media at an early stage can mitigate the risk and adequately respond to such issues proactively.

## "IT IS ENSURED A SUITABLE ENDPOINT SECURITY IS INSTALLED AND MONITORED FOR TIMELY UPDATES"

VIJAYAKUMAR V
COO, Symmetrix
Computer Systems

**To keep customers safe:** Depending on the affordability, sensitivity of data and to have good control over the computing devices, it is highly recommended to connect thro VPN. Wherever the affordability is an issue, we ensured a suitable endpoint security is installed and monitored for timely updates are happening. Data backup schedule are implemented to synchronize the data on the cloud. In a nutshell, safeguard each computing device with suitable endpoint security, use VPN for safer connectivity and practice regular backup processes.

**On educating customers:** We regularly meet our customers, explaining to them the risk of an un-secured IT environment at home, specifically due to the pandemic situation. The organizations are understanding the importance of Data & network Security and most of them have implemented the required data & network security.

**Safeguarding the customers and employees:** We handle data & network security in two angles: Protecting the data / network with required security practices implemented and reliable data backup solution. Choose & use suitable DLP software, monitor the activities and timely action for any issue is noticed. Human errors continue to exist and cyber criminals will look for the opportunities to take the advantage of the situation. There are plenty of data protection / backup solutions available in the market. Proper data backup process will ensure timely recovery of the system and to put the user back in action with minimum loss of time.

## 'GOOD GOVERNANCE IS ESSENTIAL FOR MANAGING CYBERSECURITY ISSUES'

MANOJ KANODIA
CEO, Inspira Enterprise

**To keep customers safe:** The WFH has increased the threat vector for the hackers and made it a bit easier for them to penetrate into an organisation's network as we are aware that the employees are one of the weak links in the chain.

The key mitigation strategy is not technology alone. With whatever technology investment an organisation plans and invests in, it will not be successful until the organisation has a strong foundation of cybersecurity aware employees.

**On educating customers:** Building resilience and mitigating risk are critical in the current climate. Considering the future of work involves making informed decisions about safety, legal liabilities, and potential threats to both capital and employees.

**Some practices that we have been focusing on, not just for our clients, but even internally are:**

**The upcoming threat:** Deep-fake technology can create such realistic-looking content that represents an unprecedented development in the ecosystem of disinformation. The content produced by deep fakes seems so real that the viewers are induced to trust it and share it on social networks thus hastening the spread of disinformation. This can tarnish a company's reputation.

Deepfakes will provide an unprecedented means of impersonating individuals, contributing to fraud that will target individuals in traditionally 'secure' contexts, such as phone calls and video conferences. This could see the creation of highly realistic synthetic voice audio of a CEO requesting the transfer of certain assets, or the synthetic impersonation of a client over Skype, asking for sensitive details on a project.

## "TO SET UP TWO-FACTOR AUTHENTICATION IS ONE OF THE BEST PRACTICES SUGGESTED TO CLIENTS"

DHIRENDRA KHANDELWAL
MD, E Square System & Technologies

**To keep customers safe:** Technology is the great enabler allowing large numbers of people to work from home during the coronavirus pandemic and also in the coming future it is enabling a work-from-anywhere environment. Although working from home permits a business to keep working, it brings huge security risks, setting a more prominent need to keep up compliance with significant data security necessities.

Organizations need to guarantee that their information is protected and resilient outside the security of the work environment. We always suggest our customers maintain the security of company data, as it is the responsibility of both the organization and their employees to maintain appropriate security. The best practices we suggest to our clients is to set up two-factor authentication, preconfigure work-from-home arrangements, regularly back up data, control access to VPNs, if possible, use of company laptop for remote work, and educating the organization on phishing scams.

**On educating customers:** Remote working today has become a norm for enterprises to manage remote teams and for individuals to work as a full-time remote employee. The foremost task we recommend to our customers is planning with each functional team through collaboration tools and solving any issues they face. With efficient communication, clients can support their team's productivity, creativity, and build better security practices. We act as security advisors for our customers guiding strategy, processes, and technologies to better protect the organization.

Moving ahead we help building guidelines on how to handle private data, clarifying their accountability, and full transparency on how the data is handled. By collaboration with vendors and OEMs, we are ensuring that all devices implemented with the client are secured by design, which doesn't compromise personal privacy and security.

**Safeguarding the customers and employees:** In the current business environment, the cumulative depth and volume of private and corporate data has made it a rewarding target for cyber crooks and sabotages. The increase in remote work demands improvement in the cybersecurity infrastructure and assesses what people will need to work safely and be able to securely sign-in to corporate systems.

After evaluating the data security scenario in 2021 for data security, we identified initiatives across these security verticals are essential such as security operations, cyber risk & cyber intelligence, data loss & fraud prevention, security architecture, identity & access management, program management, investigations, and Governance policies. We have taken instant steps in curbing these vulnerabilities and to evaluate & rethink how to oversee the business and protect the assets and data both for our organization and clients.

## ‘ONE HAS TO BE ALERT AS CYBER SCAMSTERS ARE ALWAYS A STEP AHEAD’

JITEN MEHTA
Director, Magnamious Systems

**On educating customers:** We have started educating the customer rather this has been by their business division only and now the security demands are coming from business and not from IT. This is a major shift.

**Robust product and solutions:** There is no solution which is robust. You need to keep monitoring and fine tune the products and keep adding the new features or develop the same. Most important is the end-users need to be alert and get them trained to keep the system robust.

**Safeguarding the customers and employees:** A; Educating the users/Business heads/IT Team. Also suggest proactive approach like MTR, a managed threat response so that threats can be managed at beforehand only.