OEM's Readiness

2020 not just has cost the lives of many, but it has also put down data and cyber security at risk. With its unwanted entry, many organisations have made their employees to Work from Home (WFH) or Work from Anywhere (WFA), in other words let's term it a remote working.

Since WFA or WFH are not very regular in India or a few countries, many organizations due to its security vulnerability had to undergo cyber and data security failure.

Cybercriminals saw remote working as an icing on the cake to play their cards that saw multiple number of ransomware attacks, data breaches in the previous year. Due to which cyber security, till date was not much spoken about, became a talking topic of every discussion table. Be it the Government, policy makers, tech enthusiasts, start-ups, pioneers, security experts, VARs and other great minds all share their knowledge and thoughts on how to improve cybersecurity.

VARINDIA got a chance to give an ear to a few names in cyber and data security vendors on their voice words about security challenges.

"COMMVAULT HAS IMPLEMENTED A CONTROL MECHANISM TO COMBAT INTERNAL THREATS"

RAMESH MAMGAIN
Country Manager, Commvault (India & SAARC)

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

Threats are not always externally sourced; it can also result from compromised credentials or deliberate acts of rogue actors. To combat such internal threats, Commvault has implemented a control mechanism to ensure administrative tasks that could threaten data are approved by two or more administrators from a selected privilege group, applying the four-eyes principle to data security.

We have earned a strong reputation as a dedicated and trusted partner to our customers, who will testify to our responsiveness, innovation, and rapid execution in the high pressure, high impact world that is vulnerable to multiple threats.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

At Commvault, the safety and health of our workforce is our utmost priority and keeping that in mind, we announced Work from Home for all our employees till June 2021 in the last year itself. In regions where pandemic situation is more controlled, we have started discussions regarding the reopening of facilities in a phased approach .To empower our employees working from home, we're constantly running virtual instructor led Learning sessions in the areas of Managing Remotely, Prioritization, Building Resilience, Building Trust with Clients and many more. Our ultimate goal is to ensure our employees feel safe, engaged and have all the skills and support to thrive even in adverse times like today.

ROLE OF CISOs:

Cybersecurity leaders, especially CISOs, have found themselves playing more strategic roles within their businesses and their role is only going to get more crucial with time. As the threat landscape evolves and becomes more sophisticated, CISOs will also need to be savvy strategic partners who can contribute to business solutions aimed at solving increasingly complex issues. As touted by Gartner, CISO will ultimately become 'key enablers of digital businesses and will be accountable for helping enterprises balance the associated risks and benefits by measuring, prioritizing, and improving an organization's security posture.

FORCE POINT'S CLOUD SECURITY GATEWAY SOLUTION HELPS TO MONITOR REMOTE WORKING EMPLOYEES

SURENDRA SINGH
Senior Director and Country Manager, Forcepoint

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

Forcepoint in addition to market-leading threat protection (the baseline required for data security), aims to help organisations secure their data and protect themselves against potential breaches using an inside-out approach. A key part of this is the deployment of Data Loss Prevention (DLP) systems integrated with machine learning, data analytics, and automation. We recommend newer, more unified platforms which can deliver visibility across hybrid, private and public cloud infrastructure while automating security policies based on changing conditions.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

Forcepoint employees who operate from office premises are secured with our corporate network. For employees who work from home, there are some best practices that we have adopted and also recommend to our customers. Force point's cloud security Gateway solution helps to monitor employees who are working remotely because it provides full visibility across all Web and cloud-based applications that employee use. These include applications that are unsanctioned or sanctioned, lesser known, internal to the organization or hosted in the organization's private cloud. Cloud Security Gateway enables organisations to see which tools employees are choosing to use, so they can make better-informed decisions about what helps them be most productive.

ROLE OF CISOs:

Cybersecurity has become the enabling engine which permits businesses to accelerate their pivot to the cloud and take advantage of the speed, scale and resilience of digital transformation. Today, Chief Information Security Officers (CISOs) can no longer operate solely within the parameters of a security program. They have to expand their understanding of how businesses operate in order to protect them. At the board level, this transition has also had another impact: It's helping boards to see value in digital transformation efforts across multiple areas in an organization.

"ENSURE WORK DEVICES ARE USE FOR WORK PURPOSE, TO AVOID CYBER ATTACKS"

ROHAN VAIDYA
Regional Director of Sales, CyberArk (India)

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

The pandemic has altered nearly every aspect of how organizations around the world operate. Everything from the rapid shift to remote work to completely rethinking the nature of customer interactions has contributed to turning the business world on its head.

These changes have also caused a dramatic acceleration in digital initiatives across industries. Many drove what felt like five years of transformation in five months – as they quickly adopted technologies to help productivity and business continuity. Whether it was bringing on new collaboration tools or moving critical infrastructure and applications to the cloud, everything has become more distributed.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

With many people Working From Home, cybersecurity has become an even hotter topic than before. With remote working, each one of us is now a potential entry point into the organisation for attackers, so risks have now increased, and organizations have become more vulnerable to cyberattacks than ever.

Cybercriminals are playing on people's fears around Covid-19 to conduct social-engineering based attacks. Whilst using new-age technologies and applications can be unusual for some, cybersecurity also becomes a major concern

By practising some simple tips and tricks one can mitigate the risks.

With so many of us working remotely from our homes, corporate security can easily be an afterthought to maintaining productivity. Some advice for a more secure environment:

Be productive and secure from anywhere, add biometric, multi-factor authentication when connecting to company systems and data.

Ensure, if possible, that work devices are used for work purposes only, to reduce exposure to dodgy websites and malware, that patches are kept up-to-date and are backed up to a secure location.

ROLE OF CISOs:

It has been an eye-opener for many organisations that working from home is indeed possible, does not negatively impact productivity, and can increase the wellbeing of staff. But this model comes with a security caveat. CISOs have been thrust onto the front line of this shift because of the clear security risks that home working represents. They have become involved in the fundamental business of organisations worldwide, which has absolutely resulted in more senior interactions. Cyber is now part of the strategy, not something that needs to be solved after the strategy has been put in place.

CYBER RISK INCREASINGLY BECOMING A BOARD-LEVEL ISSUE

KARTIK SHAHANI
Country Manager, Tenable (India)

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

Many security programmes do not effectively prioritise critical risks. It is also important to have visibility of all assets in the attack surface. This includes traditional IT devices, cloud infrastructure, and increasingly operational technology (OT), such as smart connected controllers or manufacturing controls.

A strong data protection programme should be based on three core tenets:

Focus on what matters most: Avoid trying to address every vulnerability. This consumes valuable resources on risks that have a low likelihood of being exploited. Utilise prioritisation and risk-based analysis to focus aggressively on critical risks that really matter.

Effectively measure your exposure: Obtain a clear view of all assets and your cyber risk exposure. Benchmark internally and externally. Create quantifiable measurements of risk reduction effectiveness that help you focus on what controls are really effective.

Know "how secure or at risk are we?"

Focus on identifying and reducing critical vulnerabilities that have the greatest likelihood of being exploited by an attacker. And it should be based on insights into the critical risks and assets within the business.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

Security has moved from a focus on the network to the security of the endpoint. Since the Covid-19 pandemic, staff continues to work from their homes or begin the migration to a hybrid working model and this trend will continue.

Home networks are untrusted. Zero-trust network models are increasingly gaining popularity as a strategy to harden security. Authentication and authorisation of users, devices, and applications will become critical as organizations adapt to the remote work environment with unknown and untrusted connections.

ROLE OF CISOs:

Nearly every industry sector and business model in the world relies on technology. This reliance means cyber risk now equates to business risk. It also means that cyber risk is not a concern managed by the Chief Information Security Officer (CISO) alone but one that's increasingly becoming a board-level issue. It is for this reason that CISOs are increasingly called upon to keep business leaders and board directors informed of their organization's risk posture in a clear and understandable manner. By working together, CISOs and business leaders can narrow the cyber exposure gap and ultimately secure their organizations from increasing threats.

"OUR ABILITY TO PROTECT OUR CUSTOMERS AND PARTNERS IS UNCOMPROMISED"

SUNIL SHARMA
Managing Director- Sales Sophos (India & SAARC)

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

Sophos' aim is to protect people from cybercrime by developing powerful and intuitive products and services. We protect businesses by providing next - gen cybersecurity solutions that prevent threats and unwanted malwares from infecting networks and devices. We also provide insight into evolving threat landscape and adversary tactics and advice on best cybersecurity practices.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

Sophos has in place a robust set of technologies that enables the majority of our global employees to work from home. We are fully enabled to continue day-to-day business, including product development and other important efforts, remotely. All of our departments, including threat intelligence, protection, and response from SophosLabs, Managed Threat Response, and Global Support Services are operating as normal to provide 24×7 detection, protection, and technical support. Our ability to protect our customers and partners is uncompromised. Our solutions were designed to protect endpoints, data and infrastructure regardless of location.

ROLE OF CISOs:

A CISO is already a regular participant in the boardroom discussions. Today, security affects the entire business including the brand management and is considered everybody's business. The stakes are high in case of a data breach and businesses have understood the importance of a proactive cybersecurity posture.

MCAFEE'S ROBUST SET OF SAAS APPLICATIONS HELP EMPLOYEES WORK AND COLLABORATE WITHOUT HASSLE

VENKAT KRISHNAPUR
Vice President of Engineering and Managing Director, McAfee India

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

We, at McAfee, provide security solutions to over 97 million enterprise endpoints, which include 75% of the world's Fortune 500 firms. For our customers, maintaining business continuity is vital, and we are well equipped to help keep their services up and running. Most of our critical teams, like engineering, R&D, customer support, operations were all equally or more productive, in our pursuit to keep our customers safe.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

We provide a seamless employee experience in the cloud. While our business involves securing cloud services for our customers, we also take pride in and providing the best digital experience to our employees. Employees across the world are growing accustomed to this 'work from anywhere' phenomenon and in my opinion, this is here to stay for the long term. At McAfee India, through various initiatives, we have ensured that our employees have been taken care of mentally and physically. For this, we actively and routinely arrange engagement sessions on mental wellbeing, nutrition, ergonomics, and parenting.

ROLE OF CISOS:

CISO has an important and expanded role in managing a company's 'security health'. With the prevalence of high-profile cyberattacks, putting finances and corporate reputation at stake, the top of the C-Suite is seeing the importance and realizing the value of cybersecurity. Today, the CEO/ Board would prefer to evaluate and make decisions related to Information Security themselves. Additionally, the elevated structure enables the CISO to be operationally more efficient and is now held accountable directly by the board/CEO. The role is not just operational anymore because it impacts the reputation and the business directly – and hence the elevation.

REMOTE WORKING HAS OPENED OPPORTUNITIES FOR THE THREAT ACTORS

HARPREET BHATIA
Director, Channels & Strategic Alliances, Palo Alto Networks (India & SAARC)

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

At Palo Alto Networks, we are walking the talk by fully leveraging our own cloud-delivered network security product, Prisma Access, to securely connect all employees to the applications they need. We have also transitioned our internal Security Operations Center (SOC) to a remote model in which all our analysts are working from home—the SOC is fully operational and continues to monitor for threats as our own user population shifts to remote work via Prisma Access. Our business continuity plans are consistent with industry best practices and include workarounds for possible disruptions to our people, facilities, applications, dependencies, and vendors. The all-hazards, multi-scenario approach is designed to ensure the continuity of not just ourselves, but the remote workforces of our all customers.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

Ensuring employees are inside the security bubble and vigilant about preventing cyberattacks requires investment in time, resources and equipment. The whole premise of being able to work from home to maintain business continuity falls apart if the employer and employee fail to maintain the same level of security and practices as at the usual workplace.

ROLE OF CISOs:

CISOs help to keep enterprises running without compromising security or compliance, while also ensuring that there is product security and service availability built into every step of the quality management process. To ensure security, the CISO must make all efforts to ensure the board and the CEO of a company understand the positive and negative repercussions of the risks involving an application, by mitigating it. While technology and network companies are moving rapidly to keep pace with the ever-evolving criminal elements, IT alone cannot be at the vanguard in the fight against the attackers. It is also the responsibility of everyone in the organisation with access to a computer or a smart device. The CISOs are responsible for making employees more aware of the security issues of the digital age, including malware and phishing, and encouraging them to take up the best practices. CISOs need to coordinate with the Chief Human Resources Officers to design and implement the information technology and security education of the workforce.