Readiness of the VARs

The ongoing pandemic situation has created a deep impression on the cyber security enterprises, while employees opted for remote working. 'WFH' has increased the risk of data security as workforce was not properly educated about the security risks of remote working prior to the pandemic. BYOD means that employees are bypassing the policies and procedures required to protect corporate assets, making it significantly easier for hackers to access this information.

Determining how to ensure business continuity without allowing BYOD threats to increase will vary based on the individual organization. Digital transformation initiatives and disruptive technologies like AI and 5G deserve their place on the corporate agenda, but not at the cost of security. OEMs with the help of its Channel Partners are ensuring security for its customers. Industry leading Partners have delved deep into this situation and shared the thoughts.

MANASI SAHA
CEO, Macaws Infotech

MACAWS PROTECTS ORGANISATIONS WITH A CROSS-GENERATIONAL BLEND OF THREAT PROTECTION TECHNIQUES

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

Macaws Infotech's vision has always been to make the Customer safe for exchanging digital information, and protecting the critical Data. This requires multiple layered approaches to security – leveraging a range of techniques that all work together – sharing threat intelligence across the enterprise and speeding the time to respond.

With the help of world-renowned Cyber Security and Cloud Security Solutions, we protect the organisations with a cross-generational blend of threat protection techniques. Using the right technique at the right time gives the customers, the best protection against the broadest range of threats, with the most efficient performance.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

We are still having WFH for 90% of my employees, 10% are using their own vehicle, maintaining social distance, wearing mask, face shield and hand sanitizer, meeting the customer online only. "NO PHYSICAL VISIT, ONLY REMOTE". Mantra of Macaws is "NOT TO PLAY WITH THE FIRE, BE SAFE, KEEP YOUR FAMILY SAFE, TRY TO KEEP COMMUNITY SAFE"

ROLE OF CISOs:

With the increase in development of various SOC related development, incident response, compliance regulatory process implementation, technologies like EDR, XDR and multi-cloud, definitely comes under the jurisdiction of CISO only. The responsibility has increased in such a way that CISO as service has started taking shape a lot. This not only helps in commercial control but also helps smaller SMBs to also look for CISO as their requirements too. The above technologies are upcoming development that is going to happen in the coming future and off course CISO is going to be the most vital department and role too. This will not only help in maintaining proper cybersecurity & cloud security strategies but also will help in keeping the services up and maintaining productivity of any organization.

D K BAJAJ
Director, D M Systems

D M SYSTEMS NOT ONLY GEARED THEMSELVES TO WFH BUT PROVIDED THE SOLUTIONS TO THE CUSTOMERS ALSO

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

In this Covid situation, there were many challenges and one of the main reasons was to first gear ourself to adopt work from home for our own team and then to sell appropriate solutions to the customers, who were thinking to adopt the same. We not only geared ourselves to work from home but provided the solutions to the customers also to do the same. Some of the solutions we sold to the customers were Virtual Firewall, Virtual WAF, DLP, SSL-VPN solutions and employee monitoring solutions etc.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

We have given the choice to our employees to work from home or office without compromising on the operations and security. All the remote devices are secured with end-point solutions fully equipped to handle ransomware attack or in case of total wipe-out or data-loss situation etc.

ROLE OF CISOs:

Role of CISo is more important now as working in this new normal situation was also a challenge and how to migrate or adopt secure work from home solutions as to work 100 % from home was a challenge for them also. The other challenge to CISo is to make sure the data integrity as working from home gives exposure to a lot of threats like data pilferage and ransomware. In addition to the above they have to monitor the selective manpower in a positive way for the management. It has a lot of negative / positive side of this depending on the company product and services.

VIBHORE SHRIVASTAVA
MD, VIBS Infosol

INCREASING THREATS AND STRONG COMPLIANCE DYNAMICS ARE CRUCIAL FOR ALL ORGANISATIONS

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

VIBS Infosol is always committed to provide niche solution-based approach for all customers. We always encourage our team to grow their knowledge which helps the Organisation to offer innovative solutions for known / unknown threats and behaviour patterns at customer Infrastructure. We believe learning is the only way to understand current market flow and predict future threats and cyber-attacks.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

VIBS Infosol has PAN India presence and having multiple offices. We have closely observe the City pattern and post discussion with leaders, we have decided to reopen few locations and start working normally. Other locations are still supporting customers and following WFH policies. Our HR and leaders are proactively assuring that all team members are maintaining proper Hygiene and following protocols in Office and at customer place. Since we are more into services and consultancy, our few customers are expecting us to visit and consult them for ongoing threats and challenges.

ROLE OF CISOs:

CISO is one of the essential leaders in major organisation nowadays. Increasing threats and strong compliance dynamics are crucial for all organisations to address. BFSI, IT / ITES are the major verticals where CISO has a broad role to play and enhance security aspects for the organisation. Enabling major security postures and defining strategies to enhance defence protocol are major factors to address by CISO. There is a huge shift towards security as a business priority.

ANUJ GUPTA
MD, Hitachi Systems Micro Clinic

PRIORITIZING PRODUCTIVITY OVER SECURITY INDICATING A MORE EXPANSIVE ROLE OF CISOS

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

At Hitachi Systems Micro Clinic, we have undertaken some pre-emptive measures across organizations to prevent data thefts, implement enterprise security policies, and establishing a process to create and monitor applications. While implementing work from home solutions we have strengthened backup and archive, network security, endpoint security, and content and web filtering. Simultaneously, we ensure awareness and training of employees on cybersecurity best practices and policies to proactively safeguard data.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

The biggest differentiator we have made within our organization was changing the perception of employees towards new normal, where working is not associated with physically present in an office. However, a sudden transition did not come easy, we ensured the safety of our employees' paramount and continued our business-as-usual by shifting gears and adopting work-from-home practices all our employees. We also implemented multifactor authentication for all our remote users to mitigate the risk of unauthorized access.

ROLE OF CISOs:

There is a shift in the outlook of organizations from prioritizing productivity over security which is bound to change indicating a more expansive role of CISOs. This would include establishing a robust cybersecurity practice from meeting ever-increasing regulatory complexity, compliance, and risk management to create the security policies and architecture, processes, systems. Since cyber-security has become a key business priority there is no doubt, the role of CISO will become indispensable.

L ASHOK
Managing Director, Futurenet Technologies (India)

FUTURENET TECHNOLOGIES WORKING ON 24X7 SECURITY MONITORING AND RESPONSE CENTRE

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

We will be working closely with our OEM's to improve our information security. In specific we are working on 24x7 security monitoring and response centre. This will be logical extension to our Managed Services business.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

We have adopted Citrix as the default method to access all official networks. This has enabled our employees to work anywhere on any device.

ROLE OF CISOS:

More than importance they will have more money to spend. With emerging threats every organization has increased its IT budget for information security.

DHIRENDRA KHANDELWAL
MD, E Square System & Technologies

CISOS SERVE AS CYBERSECURITY AMBASSADORS ACROSS THE ENTERPRISE

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

We have taken steps to evaluate and rethink how to oversee the business and protect the assets and data by end-to-end encryption and encrypt stored data. The biggest hurdle is security as a priority and security awareness for the employees from top to bottom, especially those who collect the personal data of clients and individuals.

Guidelines have been provided organization-wide 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 devices are secured by design, which doesn't compromise personal privacy and security.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

Remote working today has become a norm for us to manage remote teams and for individuals to work as a full-time remote employee. The foremost task is planning all the deliverables with each functional team through collaboration tools and solving any issues they face. With efficient communication, we support our team's productivity, creativity, and sense of belonging. While managing a remote team, we provide our employees with cloud-based tools to work together to drive productivity in remote teams.

ROLE OF CISOS:

As the leader of cybersecurity for an enterprise, the Chief Information Security Officer (CISO) is swiftly becoming crucial to a business's survival. CISO can unify organization and security objectives and help navigate innovative and pending privacy guidelines.

CISOs serve as cybersecurity ambassadors across the enterprise; as strategic advisors guiding strategy, processes, and technologies to better protect the organization; and take dynamic actions to lead the current and upcoming generations of technical personnel in the organization and community.

VIPUL DATTA
CEO, FutureSoft Solutions

FSPL HAS ALWAYS INVESTED IN ONBOARDING INDISPENSABLE EXECUTIVE LEVEL SECURITY LEADERS

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

As organisations move towards the 'future of business', it becomes difficult to address threats using conventional approaches. Current era is fuelled by the mobile and cloud ecosystem, which is emerging as the primary driver for computing and users now access and share information across systems and cloud-based applications from outside the organisation.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

As the world goes back to the new normal, FSPL has drafted plans with the company's cyber security factor which is a very crucial factor. We have been very vigilant to prevent vulnerable machines getting connected to corporate networks.

1. We make sure that users reset / change their password before they login into their system.
2. Ensure all systems are updated antivirus signatures, patches, and software versions.
3. Health checks of Data Leakage Prevention tools and other technologies have been performed.

ROLE OF CISOs:

FSPL has always invested in onboarding indispensable Executive level security leaders, to be confident that security measures, adoptions and deliverables are maintained up-to the mark at all times. IT security infractions and compliance enforcement policies are adhered with no compromise.

JITEN MEHTA
Director, Magnamious Systems

CISO'S ROLE IS ALWAYS CRITICAL

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

We have internally deployed a DLP solution along with the classification of the Data to avoid the leakage through the team members and trained people on spoofed email through the phishing threat training with a strict firewall policy for all the employees including the Promoters. The same solutions we are promoting to our customer through different products like Smokescreen/Seclore/Sophos etc.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

Currently we have not started our offices and all are working from Home and all the Back office employees are working through the Citrix VDI on a central server and they cannot download anything on their local desktops. All the invoices are digitally signed through the ERP.

ROLE OF CISOs:

I believe that CiSO's Role was always critical as from the last couple of years security has become a prime importance and data has become more valuable than even money. Since now all will be accepting the Hybrid culture and working from Home CISO has to be more vigilant and alert for any info security breach.

J. PAUL VIJAYKUMAR
Director – Sales,
DigitalTrack Solutions

CISOS ROLE IS UNIQUELY POSITIONED TO HELP ORGANIZATIONS MANAGE DUALITIES

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

We DigitalTrack plays an active role in the digital transformation of industries to bring digital to every person, home, and organization. As digital transformation initiatives accelerate across the world, we have a clear responsibility to ensure that cyber security and privacy protection remains a top priority. Enforcing to customers and implementing an end-to-end global cyber security assurance and privacy protection system is one of our crucial strategies.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

In the hybrid workplace of the future, identity becomes the new perimeter—the first line of defence for any organisation. IT teams must look at scaling VPNs and multifactor authentication (MFA) to verify each user's identity before allowing them access to the network. As companies fast-track their move to the cloud, it's crucial to deploy secure access services edge architecture (SASE) to ensure protection for multi-cloud access.

ROLE OF CISOs:

As the guardians of information security, it's the CISO's role to create a strategy that deals with ever-increasing regulatory complexity, creating the policies, security architecture, processes and systems that help reduce cyber threats and keep data secure. CISOs will understand how the cybersecurity threat landscape is evolving and how that could affect the security risks facing their particular organisation. The chief information security officer (CISO) role is uniquely positioned to help organizations manage those dualities, but it requires a different set of leadership qualities for CISOs that goes well beyond their traditional role as guardians of all things technological.

VIJAYAKUMAR V
COO, Symmetrix
Computer Systems

CISOS MUST COME OUT WITH A SUITABLE SOLUTION TO BALANCE BETWEEN SECURITY & DATA

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

Securing the digital information is an ongoing challenge to any organisation and needs continuous monitoring and proactive action to secure the data. In the "New-Normal" situation, we quickly worked on the solutions to balance between the protection and availability of data – not only for our organization, but for our customers as well.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

In the new normal situation, getting timely support for any hardware support is a challenge. We identified a suitable Endpoint Diagnostic Tool, which analyses the hardware for various parameters and sends the alert to the administrator. This will help us to take proactive action to fix any issues, that include low-disk space to most of the hardware related problems. Thus, we can achieve high availability of the devices to the users, be more productive and minimize the possibilities of data loss due to hardware related problems.

ROLE OF CISOS:

The role of CISOs is always very important for any organization, where sensitive data is being handled. Due to the "New-Normal" situation, their role has become more important. Since many of the users are forced to work from home, the CISOs must come out with a suitable solution to balance between Security & high Availability of data and to minimize the impact of the business operations.

NITYANAND SHETTY
CEO, Essen Vision
Software

CISOS HAVE BECOME AN IMPORTANT ROLE UNDOUBTEDLY

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

The last year has been a year of unlearning a lot of our traditional ways of the data protection strategy. Covid-19 opened up a completely new normal and a new set of challenges organisations now face as compared to a year back. We had to add some different technologies and tools built on Zero trust in our arsenal to provide customers with the confidence that even in the current situation and what we face in the near future EssenVision can provide them with the right data security practises and keep them unharmed from the breaches and attacks we have seen in the recent times.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

We adopted the Cloud a long while ago for our emailing platform, however the usage of the entire platform of O365 with Teams, One drive & Sharepoint online was done very effectively by the entire team in the last 1 year for internal and external communications, internal data storage & client meetings. We believe as a company providing these platforms to our employees we are now fully geared to working remotely without teams in this New Normal.

ROLE OF CISOs:

Earlier the compliances that were followed within the 4 walls of an organisation premises could not be applicable for employees working from home. Apart from the infrastructural and logistical challenges, Security Issues were paramount for an organisation. The CISO definitely has become an important role and an important resource in the strategy of setting up an Infrastructure in the new working environment as his inputs in protecting and security organisation data was key and an important aspect of this new environment.

RAGHUVEER HR
Senior Director –
Sales, NTT Ltd. India

CISOS ENSURING THE SECURITY RISKS ARE PRIORITIZED

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

As we leverage technology to become a progressive, digitized society, security threats have become more serious and sophisticated, particularly cyber-attacks. Within this environment, we're responsible for the protection of data, ICT service infrastructure and customers' basic rights, freedoms, and information assets, as well as the provision of a sound foundation for the growth of the digital economy.

When we put together our new medium-term management strategies in 2020, it was our mission to contribute to the building and development of a free, open, and safe ICT platform that will support the infrastructure of the digital economy. We also made it our vision to realize the digital transformation of both customers and NTT itself, and for that reason, we will be chosen by customers.

ON THE ROLE OF CISOs:

The role of the CISO is highly relevant and very important already – with every new cybersecurity breach, the c-suite has become even more keen to hear from the CISO on the best security posture the organization must adopt. Now more than ever, CISOs are focused on ensuring that the security risks are prioritized, protocols and policies are followed, and cyber intelligence moves seamlessly throughout the organization. Businesses are looking to transform themselves and security is the first prerequisite to it. Developing a security program is imperative to being able to protect your business interests and your valuable assets, and CISO's are the ones to turn to for it.

MANOJ KANODIA
CEO, Inspira Enterprise

INSPIRA HAS BEEN PROACTIVE IN RECOMMENDING AND IMPLEMENTING TECHNOLOGIES

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

Inspira has been in the forefront of technology transformation for the organisations and we recommend the controls be adopted based on the risk profiling. This has also been a key aspect of our internal risk mitigation strategy. Our teams operate from multiple locations which enhances the surface attack area. For this we have ensured the relevant security controls in place for information security.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

Being a security services provider to clients across various verticals, we have been proactive in recommending and implementing technologies to pivot to the remote working mode at the advent of Covid19 outbreak and the subsequent lockdown. We have ensured our team members across various locations in India and overseas have access to the technology available to enhance their safety, efficiency and productivity. For the team members visiting the office, we have a combination of physical, logical and COVID-specific security controls in place. These controls are governed by our Information Security Policy.

ROLE OF CISOs:

With the continuous evolution along the digital continuum the CISOs are required to balance the need to protect the data and operations and also keep cyber risk at an acceptable level. The CISOs role is uniquely positioned to help organisations manage these dualities and gives them the strategic differentiations within their organisations. The ones who would stay longer in the same organisation will be those who are business focused, understand management expectations and are able to communicate with the stakeholders.

Today the management expects their CISO to have a strategic vision, being able to engage with stakeholders and inspire, as well as other capabilities that are becoming increasingly important to the CISO role.

SAIRAMAN MUDALIAR
Director, Pentagon
System and Services

CISOS WILL BE THE KEY AND STRATEGIC STAKEHOLDER

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

We are an IT solution provider and have been helping organisations manage their technology needs to run business. Security is one of the key services we help companies to achieve and have been following best practices for it on many platforms. Having said that, the security threat is as dynamic as the IT innovation is, so we are upgrading our skills and services at home as well as for our customer needs. Cybersecurity, data management practices and governance are the areas where we are focusing more for coming days.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

Endpoint data management is the most critical aspect when it comes to remote working or WFH. Its more than only data management, even employee awareness and empowerment for day-to-day operation is the key. We are helping them to practice automatic device locking, password management, encryption, regular backup and managing their local router for connectivity.

ROLE OF CISOS:

It always was and with evolving technology adaptation and ever-increasing threats, CISO will be the key and strategic stakeholder not only in security but in overall business operations as well.