2021: RINGS THE PREPARATION BELL FOR CYBER & DATA CHALLENGES

The unprecedented pandemic has created ripples in the digital world and has actually accelerated the digital journey of many organizations. The pandemic has speed up the digital transformation by a few years. Digital transformation has become the key element of business strategy. Though the pandemic has created havoc across the globe from a human health perspective but at the same time it can be considered as a booster in the IT industry boosting the organizations with digital power.

We have witnessed organizations adopting digital transformation on war footing but they have missed out on the agile data privacy and security infrastructure. With the digital power comes the threat of cyberattack. According to Kaspersky Security Network (KSN) report, India saw a 37 % increase in cyberattacks in the first quarter (Q1) of 2020, as compared to the fourth quarter (Q4) of 2019.

The pandemic has forced almost the entire globe to adopt the new normal of working from home which has left data in a vulnerable position. The increased use of connected devices, apps and web services at homes make the remote workers more susceptible to cyberattacks. This threat is compounded by many individuals continuing to work from home, meaning this threat not only impacts the consumer and their families, but enterprises as well.

Consequently, as organizations will adopt digital transformation in future, it will become critical for them to protect and manage data by deploying robust data protection solutions. It will become a necessity for CTOs and CIOs to protect customer data. With this the role of Chief Information Security Officer (CISO) will become even more prominent within the managerial hierarchy.

Let's take a look at industry experts' view on how they have armed themselves to face challenges in data security, best practices adopted and the growing importance of CISOs. We have considered insights from the CIO community and also from the vendors and partners.

"BARISTA GEARED UP WITH SAP AS BACKEND AND POS AS FRONTEND APPLICATION TO FULFILL ALL THE COMPANY REQUIREMENTS"

YOGENDRA SINGH
Head – IT, SAP, Barista Coffee Company

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

The biggest security challenge that large organizations are facing is that they're not acting quickly enough towards a risk-based view of their environment. Multiple application and multiple network access are major challenges to protect data. We should understand business requirements to gear up with single or minimum and effective solution. Do not follow the trends without understanding the business requirement. Barista geared up with SAP as backend and POS as frontend application to fulfill all the company requirements. We are following best practices and using minimum customization.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

For WFH Users we integrated VPN Connectivity with MAC binding so that employees can use applications only on official Laptops/tabs and also using MPLS for Stores connectivity. In office we are using firewalls, antivirus to protect and filter in and out traffic to protect from outside threats. We are following best practices in policy segments.

ROLE OF CISOs:

The role of CISO is more critical while every organization allowing to work from home. Employees are using unsecured connectivity to access organizational data and application and this situation is increasing chances to generate loopholes in cyber security.

AHUJA HIVE BELIEVES IN SYNCHRONIZED SECURITY TO PROTECT NETWORK

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

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

My experience with cybersecurity is immense to protect my company. My personal experience is to focus on basic and improve the protection awareness of users in our company and follow the best practices. We believe in synchronized security to protect my network either SAP on AWS, Salesforce and other critical application on premises.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

Secure network tunnel created for end users from company provided devices to AWS, regular updates of patches our users' computers, awareness about updates, help us to protect. Also replying emails give users awareness about cybersecurity help us to protect in the current situation.

ROLE OF CISOs:

Depends on company to company and industry to industry, this is required. But in my opinion, if we focus on basic than we protect our self always. I have seen many organizations, lots of investment done for the CISO and their team, but still frauds are going to happen, because they are focused on man power not on basic things, a small bean can spoil your cyber security policy driven approach.

"OUR ORGANISATION HAS BEEN ACTIVELY INVOLVED IN CAPACITY BUILDING ACTIVITIES"

DR. KARNIKA SETH
Cyberlaw expert & Founding Partner, Seth Associates

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

Our organisation has been actively involved in capacity building activities -on creating awareness on cybersecurity, both within and outside the organization. Thrust is on deploying latest tools and techniques to safeguard data and address privacy concerns. During Covid pandemic our organisation delivered more than 50 webinar sessions for chambers of commerce such as NASSCOM, CII, FICCI amongst other bodies to empower people at large.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

Extensive cybersecurity training was imparted to employees and usage of reliable VPN, conference and collaborative work platforms was encouraged. Flexible timings were allowed and mostly work and projects were monitored digitally and daily work reports were created and shared through collaborative platforms.

ROLE OF CISOs:

As most businesses shifted from brick and mortar model to digital medium, cybersecurity assumed greater significance in Covid and post Covid times! This shift will require greater mobilisation of resources, both in terms of equipment, infrastructure and manpower training to deal with new technological demands of changing business models.

ESDS - AN EARLY ADOPTER OF AI/ML BASED SECURITY PRODUCTS AND FULLY AUTOMATED SOLUTIONS AS PART OF ITS SOC

DR. RAJEEV PAPNEJA
Chief Growth Officer, ESDS Software Solution

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

ESDS is into providing Managed Datacenter and Cloud enabled services with its Tier 3 Datacenters. One of the core offerings from ESDS is its SOC services. So the question really becomes all the more important for us because we are taking responsibility of securing data of hundreds of organizations. And add to it that our biggest clientele base is from Government and BFSI sector. The threat landscape keeps on increasing with each passing day. The speed of cloud adoption, use of IoT in smart cities, BYOD, and sudden shift to remote working has undoubtedly created an unprecedented opportunity for the attackers.

With the above context, as a Datacenter we have to, and have always been ahead of time in case of technology adoption. ESDS had already started using AI/ML based security products and fully automated solutions as part of its SOC few years back. These solutions not only analyse operational security data and detect cyber threats/vulnerabilities, but also respond to security incident threats in real-time. Through the combination of Dynamic Threat Models, Machine Learning (ML) and Artificial Intelligence (AI) with contextual and situational awareness, proactively surface threats that matter, and automatically contain and eliminate them in real time. While we had certified security resources in SOC, we made sure that all senior people in the organization have adequate cyber awareness. ESDS has its indigenous security products & solutions such as Web application Firewall, Web VPN, Vulnerability scanner etc. We have built our own SOAR stack using various tools and technologies.

On the server and storage front, while data at rest and data in motion was good enough till now, attacks have started surfacing up during processing, and to mitigate them we are embracing confidential computing. We have deployed a zero trust architecture for utmost control and of course the traditional stack comprising of the perimeter firewalls, IPS/IDS, Virtual firewalls, SIEM, use of appropriate encryptions, DLP etc. all the way to robust processes and role based access for people have always been in place, backed by regular audits. Automation is the mantra for surviving in near future and we are banking on it.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

Being an IT organization, work from home was not something new for the employees at ESDS, more or less we were set to work from anywhere. We had our own security solutions that enabled the staff without much hassle to work from home. We were already using collaboration platforms in our daily work lives, so that was also nothing new for us. As part of best practices, our HR was mainly focused on making sure that people try to maintain work life balance by being reasonably productive.

ROLE OF CISOs:

CISOs have become as powerful as the CFOs. A thin crack in the security framework, and the organization can crumble down because reputation in digital world is equally important as finance. Sudden change in the way world will be operating going forward has opened up ways for plethora of attacks, and vulnerabilities that were never thought of were exposed. The CISO role shall now be mainstream and not simply technical as it used to be wherein traditionally CISOs were more responsible for figuring out the tools to maintain the security posture and take care of incidents or create a security architecture. Going forward they shall have the leadership seat in business arena and the most important skill would be to explain the risks in business terms to the board, in a language that is non-technical.

SDG SOFTWARE IMPLEMENTED COMPLIANCE & SECURITY PROGRAM WITH DEFINED SET OF CONTROLS AROUND DATA SECURITY

MEETALI SHARMA
Head - Risk, Compliance & Information Security, SDG Software

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

With the increased remote working, data security has become of paramount importance for the organization. Protection of PII and confidential information is critical for meeting the business objectives. At SDG, we have implemented a robust and comprehensive compliance & security program which has defined a set of controls around data security. These controls have been determined after conducting a thorough risk assessment of the threat landscape of the organization.

Employees are made aware of their responsibilities as custodians of critical information and appropriate training has been provided to them. Tools around data security such as DLP, EDR, URL filtering, no admin access on endpoints, multi-factor authentication, Single sign on, monitoring etc have been implemented to ensure we are resilient.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

We have made a lot of efforts to ensure smooth remote working for employees without any business disruption. BCP plans have been updated for remote working scenarios and employees are being given continuous training around security aspects for remote working. Help desk and facilities teams are available 24 * 7 to support the employees.

Adequate arrangements have been made to follow COVID guidelines once employees start coming to office. For now, employees are advised to continue working from home unless it is critical for them to come to the organization.

ROLE OF CISOs:

The role of CISO will definitely be of much more importance going forward as he/she will have more of an advisory role to the board of directors on strategic initiatives related to cybersecurity. CISO needs to develop strategies and build capabilities within their organization around data security, business continuity and remote working.

"WITH SIGNIFICANT HELP FROM OUR INFRASTRUCTURE, CLOUD SOLUTIONS, PROCESS AND SECURITY GROUPS, OUR EMPLOYEES QUICKLY PIVOTED TO WORKING FROM HOME"

RAVINDER ARORA
CISO, Infogain

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

At Infogain, we have adopted cybersecurity strategies to take a smarter, more adaptive approach to protect critical databases, files, and more with a comprehensive data security platform. Due to the surge in cyberattacks in 2020, companies increasingly realize that they need to build application security into the entire lifecycle from development to runtime, which leads to development teams adopting DevSecOps practices at a pace.

As 2021 progresses, more application teams will take full responsibility for their security, with appropriate security team support. In addition, as responsibility and budgets shift, application teams will increasingly adopt a DevSecOps process, fully leveraging automation to maximize velocity and develop a culture of continuous improvement. This is the year when security teams in large and small organizations will break down walls and change the security culture at scale by applying DevSecOps with intelligence-based code solutions to automatically build secure infrastructure, replacing manual attempts to fix vulnerabilities.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

The COVID-19 pandemic is a serious concern for all of us and helping our employees and their communities stay safe is our highest priority. With significant help from our infrastructure, cloud solutions, process and security groups, our employees across the globe quickly and successfully pivoted to working from home. After a week of testing, 95% of our India-wide organization moved to work from home (WFH) with stellar results, including rapid VDI technology adoption, high productivity, and continued collaboration and communication with our clients. Our work continues uninterrupted, with high productivity and continued business growth. Our ISS group and our Admin teams were instrumental in facilitating the transition to WFH. We allocated hundreds of laptops, hosted hundreds of engineering support calls, and maintained 24x7 support for VPN configuration. We delivered relevant equipment to employees' residences and provided a 24x7 quick response mechanism for admin services. We also rolled out WFH guidelines for our employees, managers, and teams to help them acclimate to the new approach. A key component of our work from home model is ensuring our delivery team members work securely. To ensure security for our clients. We defined and implemented a Microsoft Windows Virtual Desktop-based approach, including a secured comprehensive desktop and app virtualization service running in the Azure cloud. This virtual desktop infrastructure (VDI) solution gives us simplified management, multi-session Windows 10, optimizations for Office 365 ProPlus, and support for Remote Desktop Services (RDS) environments. Since we already provide Microsoft Azure Expert MSP level services to our clients, we were able to quickly leverage the relevant technologies to secure remote work practices among our internal delivery teams. I am proud of the way our teams innovatively leveraged technology in an intense, rapid-turnaround situation.

ROLE OF CISOs:

The CIO and CISO have vital roles in ensuring the organization can function as pandemic containment measures are implemented. At Infogain, we believe that tech integration will be a major factor in organizations' day-to-day operations, especially with remote working being here to stay. We need to ensure that businesses can work remotely and flexibly and that employees are confident in doing so. This may require us to revisit decisions on access rights, entitlements, and risk posture. In these unprecedented times, the role and activities of the CISO are directly relevant to companies' CEOs and boards.

"THE POLICY DEFINES THE EXPECTATIONS, RESPONSIBILITIES, ELIGIBILITY OF COMPANIES TO HAVE A REGULAR OPTION OF REMOTE WORKING"

DINESH KAUSHIK
CIO, Sharda Motor Industries

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

1. Take Security Analysis Seriously
2. Recognize Sensitive Data:
3. Change your Perspective:
4. Network Security
5. Internet Security
6. Online data Security

Protecting organizations from hackers is difficult, especially when they are machines. Thus, you should turn to extreme automation when it comes to data security- this is the time when security analytics comes into play. Security analytics helps in understanding what is going on within the company. It also handles complex data landscapes, especially for organizations that have large data centers, several employees that use their own devices, and valuable customers and employees that use vulnerable connected devices. With security analytics, you can quickly gain not only data but also analytics needed to protect your IT resources.

The Chief Security Officer is not responsible for security analysis but for anything related to data.

Protection with Proper implementation tools like firewall, Fortinet sandbox for gateway level security is required.

THE BEST PRACTICES FOR REMOTE WORKING:

Work from home is a growing trend in today's work environment, in which employees can easily plug-in from just anywhere they are. The policy defines the expectations, responsibilities, the eligibility of companies to have a regular option of remote working, and others took it up during emergencies. Coronavirus has sparked a revolution in the work from home scenario, many employers have already considered the work from home set up quite seriously, to avoid reduced productivity.

ROLE OF CISOs:

A CISO is responsible for establishing security strategy and ensuring data assets are protected.

The CISO's role is 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. Compliance is a key element of the role, as is understanding risk management.

CISOs are expected to help with regulatory compliance, you should know about PCI, HIPAA, NIST, GLBA and SOX compliance assessments as well. CISOs will understand how the cybersecurity threat landscape is evolving and how that could affect the security risks facing their particular organisation.

"ISOLATE SERVERS AND DEVICES THAT CONTAIN VITAL DATA FROM COMMON NETWORK"

D V SESHU KUMAR
Asst Vice President – IT Head, Orient Cement

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

Data security seems to gain more attention with each passing year. Data security is the number one priority, and concern, of IT departments. This is because, over recent years, companies have begun using multiple external applications to carry out company processes. This has greatly increased the security challenges of a company and the risk data breaches. This includes the integration of mobile devices into the business world. Everyone, from business owners to entry level employees, bring their personal mobile devices to work.

At some point, they have all connected with the company's infrastructure, whether it was intended or not. Even if we follow network security tips. All it takes is plugging a phone into a terminal, PC, or laptop to charge the phone and that system is potentially at risk.

Isolate servers and devices that contain vital data from a common network. By removing these systems from the common network, it eliminates the possibility of remote access, thus increasing the security.

It is important to emphasize application security instead of device security. Most applications are cloud-based. Cloud-based systems run non-stop and give users uninterrupted access to the systems, including hackers.

By using both a proactive and reactive protection method, then it's actively hunting out weaknesses in the system. It gives a company more control over its network. Real-time Intrusion detection software is a great way to monitor when data is being accessed, by whom, from where and when. It gives the ability to immediately identify any odd network behaviours as it happens. This helps in catching the problem before it gets out of hand.

THE BEST PRACTICES FOR REMOTE WORKING:

Remote work presents a unique challenge for information security because remote work environments do not usually have the same safeguards as in the office. When an employee is at the office, they are working behind layers of preventive security controls.

Some of the important parameters when working from home are avoiding public Wi-Fi, using personal hotspots, VPN to use for remote access applications, VPNs provide a flexible connection to connect to different services (web pages, email etc.) and can protect traffic. Also set up encrypted remote connections into a remote desktop or other individual server. Many of these connection types (RDP, HTTPS, SSH) include encryption. Very important thing is to keep work on work computers and not on personal computers. Never leave your devices or laptop in the car etc., car is not any safer place to keep. It is a best practice to keep it with you work laptops and devices.

ROLE OF CISOs:

Things are rapidly changing for today's CISOs. In its State of Cybersecurity, reports say that organizations might be starting to move away from the traditional reporting model for CISOs because of the desire to avoid conflicts of interest. The CIO is chiefly concerned with implementing new technology projects to support the organization, whereas the CISO is interested in minimizing the organization's risk level.

CISOs need to draw upon other skills so that they can effectively explain security risks facing the organization to the board and direct their strategy's implementation across the entire organization. It is important that CISOs moving through the different departments will be able to both understand and approach digital security as a holistic problem.

WHIRPOOL CORPORATION FOCUSING ON DATA PRIVACY, PROTECTION AND LOSS PREVENTION

DAREN K FAIRFIELD
CISO, Whirpool Corporation

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

To face the near challenges in data security, our organization is focusing on data privacy, protection, and loss prevention. These challenges have driven a change in how we view data privacy more holistically across the globe given the surge in government regulations on privacy and the consumer's expectations.

We have deployed a global network of privacy champions, capabilities, and training to promote strong data privacy practices. In addition, we have addressed stronger data access protections and recrafted our least privilege model to drive access to data by those who truly need it to do their jobs.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

From a technical standpoint, this includes multi-factor authentication for system access, enforcing security tools are current and running on all employee computers, and stronger asset, vulnerability and patch management. From a human standpoint, we have adopted many health protocols for those coming into the office including limiting who can enter company buildings, social distancing and mask wearing guidelines in workspaces, and daily health checks.

We have also provided some additional equipment support for those working from home to ensure their productivity and ergonomic situations are supported. Our employees also receive extensive phishing training and are engaged in our simulated phishing program to raise cybersecurity awareness.

ROLE OF CISOs:

Our take on the CISO role is that it will continue to evolve and broaden its reach into other areas of risk management, communications, and privacy. With the takeup of greater digital capabilities across global organizations and building these digital capabilities into consumer products, the CISO's boundaries are becoming less defined as risk needs to be considered beyond the company's four walls. This includes supplier risk, consumer risk, and product risk.

The CISO must now be more than just an IT person. For example, the CISO must now perform roles such as an educator, a risk manager, an auditor, and a corporate communicator. This need requires more diversity in the skill set for the future role of the CISO and a much greater understanding of the business as all functions are embracing new digital capabilities without traditional IT involvement.

NEC DESIGNED AND DEVELOPED SECURITY FRAMEWORK AND CONTINUOUSLY REVIEWING AND IMPROVISING SECURITY POSTURE OF THE ORGANIZATION

PREETI KANWAR
IT Head - Chief Information Security Officer, NEC Corporation India

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

In order to ensure data security, we have adopted new technologies, have established the required guidelines for users and customers and are ensuring the adherence of industry standards. Of course there are cybersecurity experts who are working round the clock to ensure all aspects of cyber security are covered at the organization level but generating awareness and sensitivity amongst the workforce is also an integral part of our way of working. Top management's focus and seriousness is playing a very big role in managing the data security at NEC.

To protect information assets, NEC has designed and developed the security framework and is continuously reviewing and improvising the security posture of the organization. We have our internal SOC, to keep a close eye on the on-going cyber-attacks and issues. We understand how important it is to ensure quick actions in case of even the smallest issue.

We have positioned information security management, information security infrastructure, and information security personnel as the three pillars of the information security governance framework within the NEC Group. We invest significantly in this domain and have a dedicated team who work tirelessly to handle security aspects of the organization. We thereby maintain and improve our comprehensive and multi-layered information security.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

In order to keep our daily operations running smoothly, we are ensuring that the following guidelines are met:

- Regular appropriate cybersecurity education and awareness training for all employees
- Implementation of required security software on laptop, desktop, official mobile phone, Tablets etc.
- Ensure coverage of all assets for regular patch updating and regular scanning
- 24/7/365 monitoring, detection, and response capabilities for our information systems
- Easy to follow Incident management workflow.
- IT performance dashboard contains the security key performance indicators as well which gets monitored and reviewed closely on regular basis.
- Awareness amongst users to take regular backups.
- Regular testing of DC backup and restore
- Implemented MFA of all critical services and data center access.
- Implemented Z-scaler and Z-app to control internet browsing.
- Regular updating of passwords with high complexity

ROLE OF CISOs:

Companies need to protect not just their own intellectual property, operations and strategies, but also customer data collected during different processes, as well as conform to applicable data privacy laws. As we move into the 'Next Normal', simply introducing cybersecurity measures is not enough. It is evident from several industry reports that security breaches increased to unimaginable heights. In order to cope with more sophisticated cyber-attacks, it is essential to strengthen security measures in a planned fashion continuously that helps ensure business continuity, which is one of the most important KRAs of the CEO. In addition to maintaining an organization's security through an effective combination of various security measures, leaders are supporting continuous efforts that reduce vulnerabilities for their stakeholders.

In my personal experience, we are increasingly focusing on keeping our data secure and risk-free. As more and more businesses recognize cyber-related risks and the immediate need to address these, CISOs will continue to get non-technical C-suite counterparts' backing. In the end, both CEOs and CISOs have similar goals demanding increased coordination and virtual facetime.

"WE PREFER BEST SECURITY SOLUTIONS ARE BUILT-IN NOT BOLTED ON"

AJAY YADAV
Head-IT, Arshiya Northern FTWZ

PREPAREDNESS TO FACE CHALLENGES OF DATA SECURITY:

We are ensuring all stakeholders have a good basic understanding of security and privacy i.e. data classifications data protections techniques by developing and communicating clear policy about trusted devices and regularly sharing information about the changing threat environment will help establish and reinforce a strong security culture even in a changing environment. We have implemented strong access barriers one would encounter through a web, mobile interface these barriers could include passwords, biometrics and MFA.

THE BEST PRACTICES ADOPTED FOR REMOTE WORKING:

We believe securing remote work is not solely the job of the IT Team, it also requires trust, the most effective way to build trust is to listen, learn and lead with empathy. We prefer best security solutions that are built-in, not bolted on. We have implemented DLP endpoint protection SOPHOS EDR, upgraded our firewalls to Fortinet 100F, SD WAN for remote sites, VPN connectivity, remote work force monitoring to all WFH Users.

ROLE OF CISOs:

A recent study shows that the number of data breaches in 2020 has almost doubled with 3,950 confirmed breaches against 2,103 recorded breaches in 2019, with the year far from the end. About 80 percent of the data breaches have occurred due to simple brute force attacks, which should raise serious concerns regarding data security Just one serious security incident or data breach could derail the growth and profitability of their companies because of impact to brand and the cost to remediate, fines and legal fees and customer loss. As a result, the role of the Chief Information Security Officer (CISO) is growing in importance.