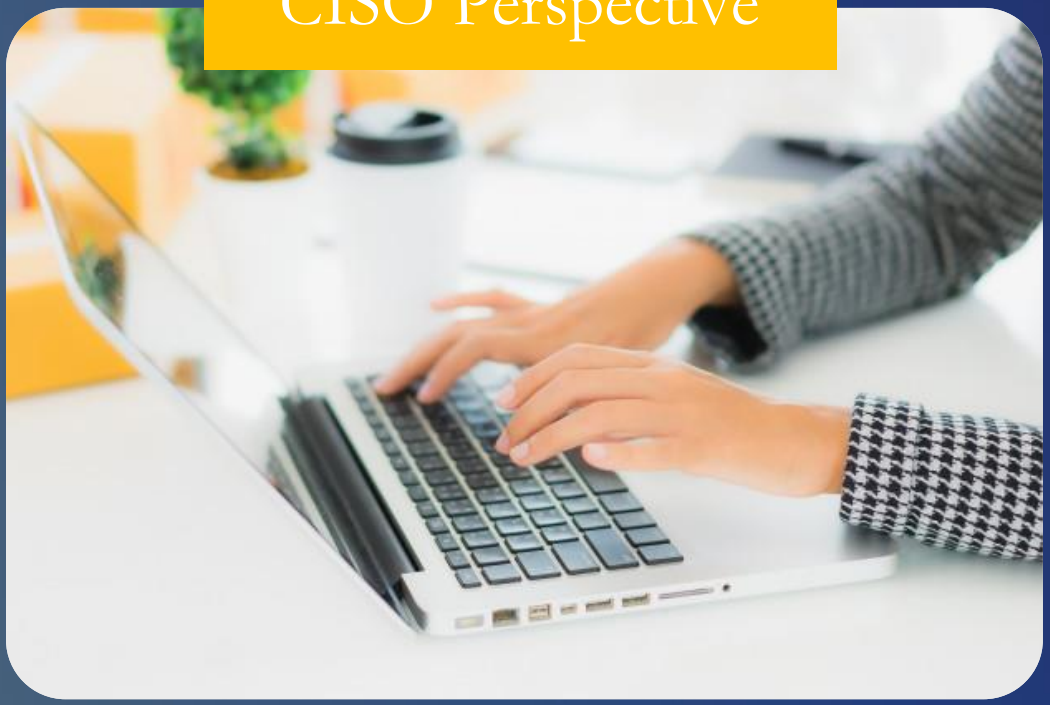
DSCI

PROMOTING DATA PROTECTION

A NASSCOM® Initiative

RESUMING WORK FROM OFFICE UNDER THE NEW NORMAL

CISO Perspective



MAY 2020

Introduction

The Government of India has announced its plan to extend the lockdown further. However, organizations have already begun to strategize the return of their workforce back to their respective offices when lockdown ends. The circumstances in offices will not be the same when employees return, and many CISOs imagine the return of full workforce to happen in phases, spread over next several months.

COVID-19 would require employees to stay cautious and adopt social distancing norms at all the time, be in seating area or in closed door meetings. Hand sanitizers and face masks have gained permanent place in procurement of office supplies. This phenomenon might stay for years to come.

Data Security Council of India (DSCI) has been organising special calls since mid of March 2020 and has recently concluded the series "CISO calls" after seven successful weekly discussions. The platform allowed CISOs from various sectors such as banking, public services, insurance, oil & gas, transport & tourism, and many more to come and discuss their strategies of dealing with the pandemic.

This paper focuses on the most pressing discussion of the hour - How should organizations roll-out their strategy for return to work from office under new circumstances? It presents the aggregated view from our weekly calls with the CISOs, and these views are equally applicable to large organisations as they are to the small and medium businesses, including start-ups.

No matter the level of scale and complexity of the organization and the sector it belongs to, the strategy for fighting such a humanitarian issue must include the basics of any organization – **People, Processes and Technologies.**

People – The most important element of any organization

Organizations will have to develop their own system to manage the workforce returning to the workplace. While doing so, they may consider their decisions ultimately falling under one of the two segments – **strategical and operational level**.

Just like organizations do risk assessment and data classification across business units, they will have to develop strategical assessment model to identify the critical resources who can deliver critical project deliveries. Some CISOs referred this approach as people classification approach. Developing resource capability matrix is the first step in this direction. Only once the BU heads have the exhaustive list of employees, mapped with the capabilities and business processes, they will be able to move to the next step, which is criticality assessment of business process.

> Risk classification or Data classification have always been critical in the first steps of cybersecurity, return to office under new normal should begin with **People classification**

Critical assessment of business process will involve assessing the overall impact on the business if the project deliveries are further delayed or hampered due to unavailability of the resources.

There are various approaches to people classification – some CISOs would like to classify employees based on the critical nature of their work, productivity while working from home. While some CISOs would classify their employees based on exposure of the individual with vendors and various other partners in the ecosystem. The second approach would then help CISOs to monitor the employees' health and interactions accordingly. Below tables shows two such approaches:

Approach 1 includes segregation criteria to be contracts, productivity or proximity to office
Phase 1 criteria to resume office: – Employees who live very close to the office – Employees who are bound to work from office under client contract, and hence couldn't perform tasks under lockdown situation
Phase 2 criteria to resume office: – Those who need access to the lab or critical resources – Those whose productivity has seen a dip by HR or BU head
Phase 3 criteria to resume office: – All the remaining employees

Table 1: Segregation criteria to help organization to think about phased return

Approach 2 includes segregation criteria to be interaction level with vendors and external parties
Red zone employees include those who need: – Public interaction – Banks, Post office, Security Guards, Service support staff, Hospitals, Malls, – Interaction with internal employees (e.g. Pantry, Café, Runners, Rest Room, Cleaners, Drivers)
Orange zone employees include: – Employees who need moderate public/ private interaction – Manufacturing employees in production line
Green zone employees include: – Those who are individual contributors, without any interaction with external parties – Typically include accounts department or senior leadership

Table 2: Segregation criteria for employees to improve monitoring

Duration of each phase may vary from multiple weeks to months, depending on regular evaluation done by leadership and HR.

Processes – "New normal" demands updated processes

COVID-19 is a unique situation that has tested organizations' agility and resiliency. The beginning of lockdown required organizations to adopt new processes that made at-scale work from home feasible. Similarly, once the lockdown ends, it will require organizations to re-visit these processes. Certainly, the processes that were applicable for work in the office under usual circumstances or pre-COVID-19 situation won't apply in post pandemic "new normal". To many CISOs, COVID-19 has been like a zero-day attack on our lives, and hence it requires us to rethink about the processes and implications of these new processes on the teams.

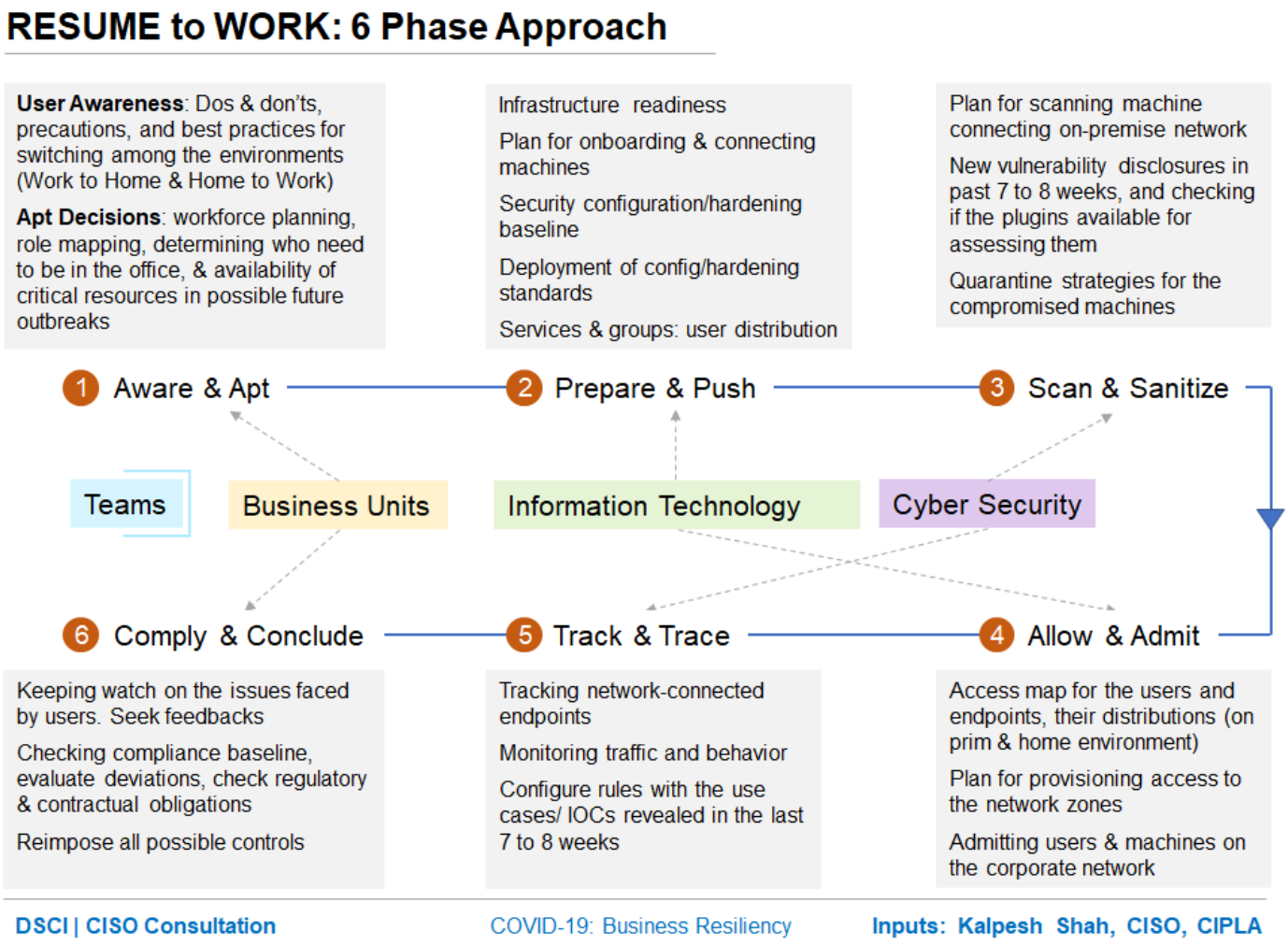


Figure 1: 6-phase approach

> COVID-19 is like a **Zero-day attack** on human lives. Hence there is a need for us to re-think and re-design our processes and think about the implications of those processes on the teams

The six-phase approach encompasses various technological and administrative controls. At the onset, it requires CISOs to identify the teams and business units that will be impacted.

Aware & Apt: Once the workforce planning is complete, as discussed in the previous section, CISO and his/her team must develop user awareness about best practices of switching the work environment (from home to office). To be impactful and relevant, the awareness must be tuned to the specific needs of the teams.

Prepare & Push: Since employees will be returning to office after prolonged lockdown, organizations need to develop controls to ensure infrastructure readiness, deployment of hardening standards, and baseline security.

Table 3 (below) shows some of the initial steps that organizations must take early-on, even before workforces return to office:

Control areas	Potential controls
Physical infrastructure controls	• Printers & scanners can be made contactless • Biometric Attendance can be disabled • Disable Biometric doors • Procure and use disposable plastic keyboard cover for multi shift employee • Foot pull doors instead handle
Administrative controls	• Frequently sanitize cafeteria (may be every 30 Mins) • Mandate the testing of employees returning post lockdown • Enable Sneeze guard partitions • Clearly communicate "Safe zones" in office • Mark spots to stand in elevators • Provision thermal Scanning and infrared temperature readings at the entrance

Table 3: Physical and administrative controls

Scan & Sanitize: This step requires CISO teams to develop plan for scanning machines before they get connected back to the office network, check for new vulnerability disclosure in past 7-8 weeks, check if plug-ins are available and have clear understanding of quarantining the machines. Only once this step is planned in detail, it makes sense for CISO teams to plan for "allow and admit" step.

Steps	Example controls
Scan & Sanitize	• Scan laptops and desktops for Malware detection, anti-virus updates and patches • Mandate password change before connecting to the corporate network • Review all locked accounts • Refresh password access for firewall, routers, switches, databases, staging Environment • Review your Risk register

Table 4: Basic checks before allowing access to the corporate network

Allow & Admit: This is the step where IT team plan to provision access to the network and allow employees' laptop and desktop back on the corporate network. But before this is achieved, the IT team must understand the distribution of employees in the office premise, as well as those at home. The IT team should plan for provisioning the access to the network zones.

Track & Trace: Till now, the approach allowed all devices to re-connect back to the corporate network. Track & trace is all about monitoring the network behaviour and re-configure rules based on use-cases and indicators of compromise observed and developed over the last few weeks.

CISOs across Indian sectors agree that there is fair amount of "noise" in the network, and hence monitoring needs to be fine-tuned and there is a need for proactive monitoring, may be on daily basis.

Comply & Conclude: Given that in weeks following lockdown, many devices will be back on corporate network; hence the need for continuous tracking and compliance. From our CISO community, one thing that came out very clearly for zero tolerance to non-compliance, irrespective of the criticality of the alert. Continuous information sharing among IT personnel and business is needed at this stage.

Technology – A need for re-calibration

While four out of the six-phased approach provides good understanding of the expectations from IT and cybersecurity team in any organization, CISOs agree that technology needs to be seen from a different lens altogether.

> CISOs agree that there should be **zero-tolerance to non-compliance** irrespective of criticality

Among the very initial steps, IT and cybersecurity team must re-evaluate the security baseline across the organization. Soon after the baseline assessment, the team must ensure that all devices and endpoints across the organization, adhere to it.

If there was a unanimous agreement during the CISO meetings, it was on how IT teams should handle patch management, importance of phishing drills across organization and managing BYOD (Bring Your Own Device). Given the rise in cyberattacks through unpatched vulnerabilities, IT teams must ensure the all known vulnerabilities must be remediated, irrespective of the threat they pose. BYOD needs more policy level intervention as level of threats have increased significantly.

Audit and compliance teams have important roles in the "new-normal" environment. It is highly likely that audit may have taken backseat in the last 5-6 weeks, and hence organizations should re-prioritize efforts towards audit and compliance.

As many employees will continue to work from home for many weeks or months, the IT team should keep supporting various technology means of accessing corporate network such as VPN and Virtual Desktop Infrastructure (VDI). As many corporate applications have moved to the cloud, provisioning access to the cloud application will continue to play a very significant role in handling the post-pandemic situation. IT teams should also continue to explore advanced options like Software (or Blockchain) Defined Perimeter that will reduce dependencies on VPN.

	Few other aspects to be noted
Additional tech. focus areas	Re-visit and verify identity and access to Cloud Infrastructure
	Rotate root passwords
	Refresh DLP exceptions
	Verify DNS Changes
	Keep logs & events in vaults for forensics
Additional Non-tech focus areas	Refresh Incident Response & DR PLANS
	Review Cyber Security insurance
	Negotiate SLA remote working clients

Table 5: Additional aspects to be noted

Summary

Organizations across sectors in India have shown their resiliency and agility as they were quick to respond to the lockdown. However, the pandemic has increased the workload of CISOs and cyber teams, given the threat landscape has changed significantly. If pre and during the pandemic required IT teams to focus on employees who were either connected through corporate network formerly or now through VPN, the post-pandemic situation will require their focus on both kind of traffic as employee base will be divided between work from home or work from office.

Another key aspect that was highlighted during our CISO engagements was the need for increased information sharing within organizations, as well as with Government agencies such as CERT-In.

Until vaccination for COVID-19 becomes a reality, organizations will have to focus on not just technical controls, but also administrative and physical controls such as thermal scanning and frequent building sanitization.

Acknowledgement

DSCI would like to extend its gratitude and thank the entire CISO community, who made these conversations enriching. Representation from various sectors – banking, insurance, healthcare, travel & tourism, oil & gas and public sector - over seven weeks ensured that the learnings could be adopted across sectors. These meetings also encouraged each CISO to not only share the best practices that they have adopted in their respective organization, but also answer specific questions raised by other CISOs.

Special mention
We would like to especially thank and mention that this paper would not have been complete without the valuable inputs and best practices shared by **Mr. Kalpesh Shah**, CISO, Cipla, and **Mr. Manikant R. Singh**, CISO, DMI Finance.

A **NASSCOM**® Initiative

Data Security Council of India

4th Floor, NASSCOM Campus, Plot No. 7-10,
Sector 126, Noida, UP -201303


dsci.connect


DSCI_Connect


www.dsci.in


dsci.connect


dscivideo


Data-Security-Council-of-India