DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

BUSINESS RESILIENCY AND SECURITY

During COVID-19

In consultation with leading CISOs of Indian Industry

https://www.dsci.in

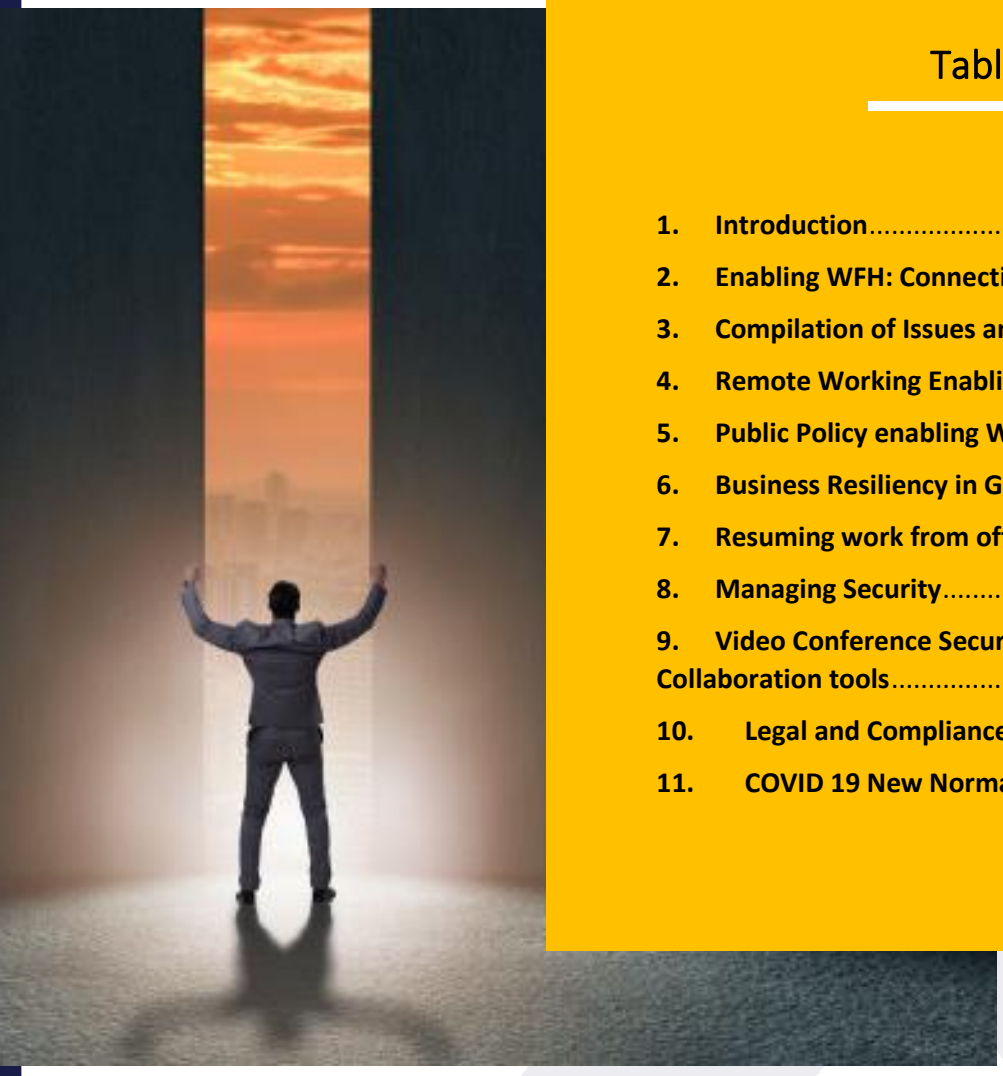

Table of Contents

1. Introduction

As COVID-19 continued to spread, Governments announced lockdowns in response, and companies had to allow employees to work from home. As there was a drastic increase in workforces joining company networks from home, attackers likely ramped up their efforts to take advantage of the inadequate or loose security posture of the WFH environment. The rush to move to work from home environment left security loopholes and made businesses vulnerable. Employees using home network and public internet services to access their official resources added another set of security challenge.

Security leaders from different industry verticals and DSCI came together in this challenging time for sharing experiences, learning, and best practices. In the series of several calls since the lockdown was announced, CISOs discussed their challenges, shared solutions and techniques they adopted, reflected on immediate problems, debated ideas, and put together strategies for addressing the long-term issues. In a couple of calls, CISOs also interacted with government authorities responsible for national cybersecurity.

This paper is an attempt to compile the discussion and deliberations for the benefit of the security community. It also serves an account of how the security fraternity, behind the wall, handled the unimaginable and unprecedented pandemic disaster.

2. Enabling WFH: Connectivity Options

The figure below depicts the options experimented for connecting the work environment to the corporate environment.

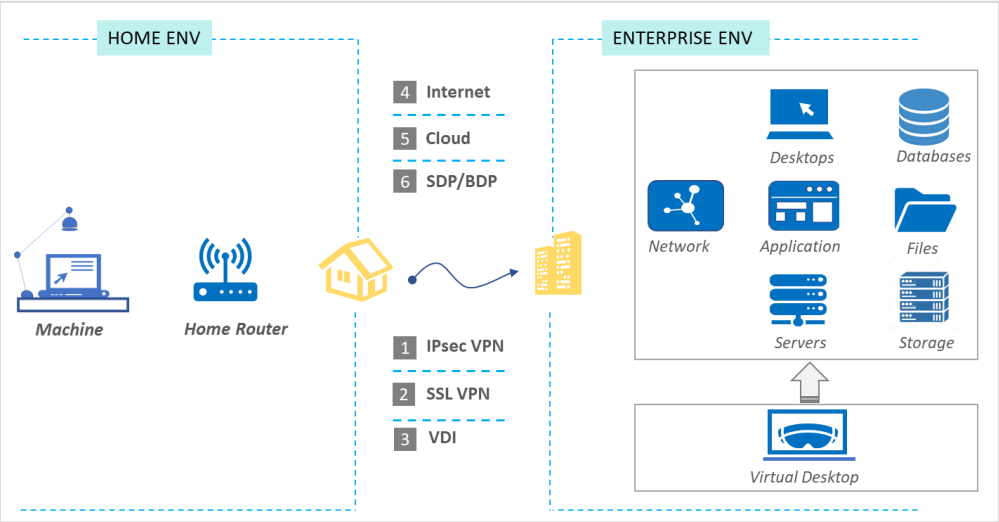

Fig. 1: Connecting home environment with Enterprise

While IPsec VPN is a popular option, many more options have evolved for remote or teleworking. SSL-VPN is the preferred option for providing access to applications. Due to cloud providers, Virtual Desktop Infrastructure (VDI) has evolved as an option as it allows connecting to corporate networks from any machine. As many corporate applications are moving to the cloud, provisioning access to the cloud application played a very significant role in handling the pandemic situation.

Advanced options like Software (or Blockchain) Defined Perimeter reduces dependencies on VPN, which is called out for the complexity of configuration and latency.

Access on company provisioned laptops	Critical sectors avoided providing access to employee machines. Access was provisioned only to the company provisioned machines
Shipping of the desktops/ machines to employee's home	
Configuring VPN agents to employee personal machines	Companies prepared early, determined the priorities, arranged the desired licenses, and carried out swift operations for the transition
Providing access through corporate SSL-VPN	
Some organizations adopted VDI solutions for enabling the access	
Some o used Software Defined Perimeter (SDP) solutions	In some cases rent was paid to the employee for carrying the official work

Fig 2: Various options adopted across the sector

Transition to the work from home environment was a daunting challenge, as the timespan was very short, and scale of operation was unprecedented where companies had to adopt various means and techniques.

3. Compilation of Issues and Challenges

The virtual meetings hosted by DSCI were quite intriguing and engaging. The CISOs from different industry verticals not only shared their experience of managing the unprecedented BCP and security situation but also deliberated on various strategies to manage the challenges. The figure below compiles them.

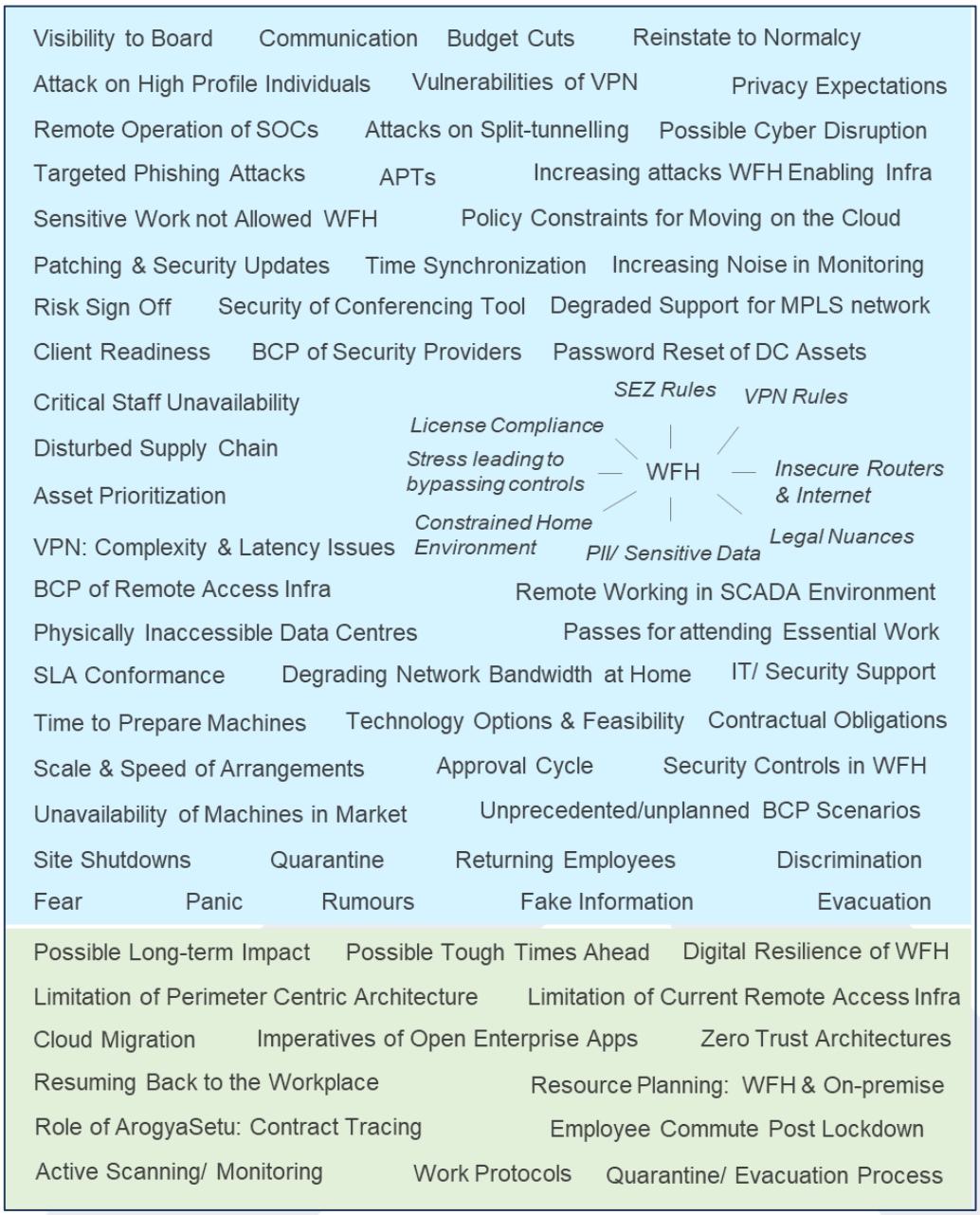

Fig. 3: Challenges to manage resiliency

4. Remote Working Enabling Infrastructure (VPN)

Virtual Private Network is the primary means that enabled moving to the work from home environment in the shortest possible time. CISOs discussed the nuances of the technology option. The following figure captures the experience, best practices, and insights associated with IPsec and SSL VPN technologies.

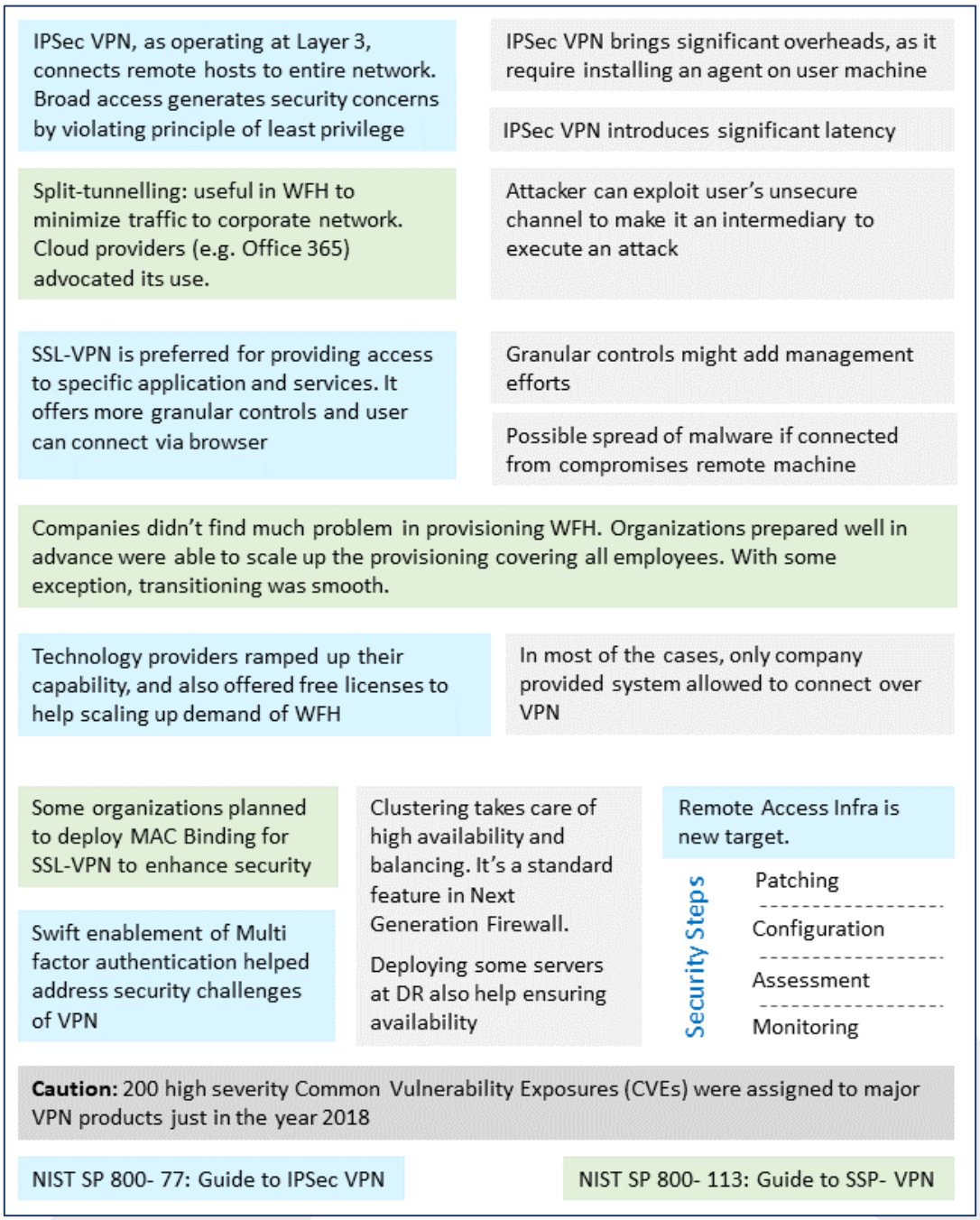

Fig. 4: Insights associated with IPsec and SSL VPN technologies

5. Public Policy enabling Work-From-Home (WFH)

CISOs across the industry verticals appreciated timely response and updates to the Government's policy to enable WFH. Since the lockdown began, NASSCOM and DSCI worked closely to push the Government on following two fronts:

- Relaxation guidelines, issued by Department of Telecommunication (DoT), towards terms and conditions for Other Service Provider (OSP) to facilitate WFH
- Issuance of ePass for employees working in sectors providing essential services

DoT issued guidelines for OSP to facilitate remote working on March 13, 2020 and later revised the guidelines on April 15, 2020. Both the versions covered four main aspects – requirement for security deposit, use of static/dynamic IP, need for prior permission and penalty for non-compliance. Below table summarizes the key points:

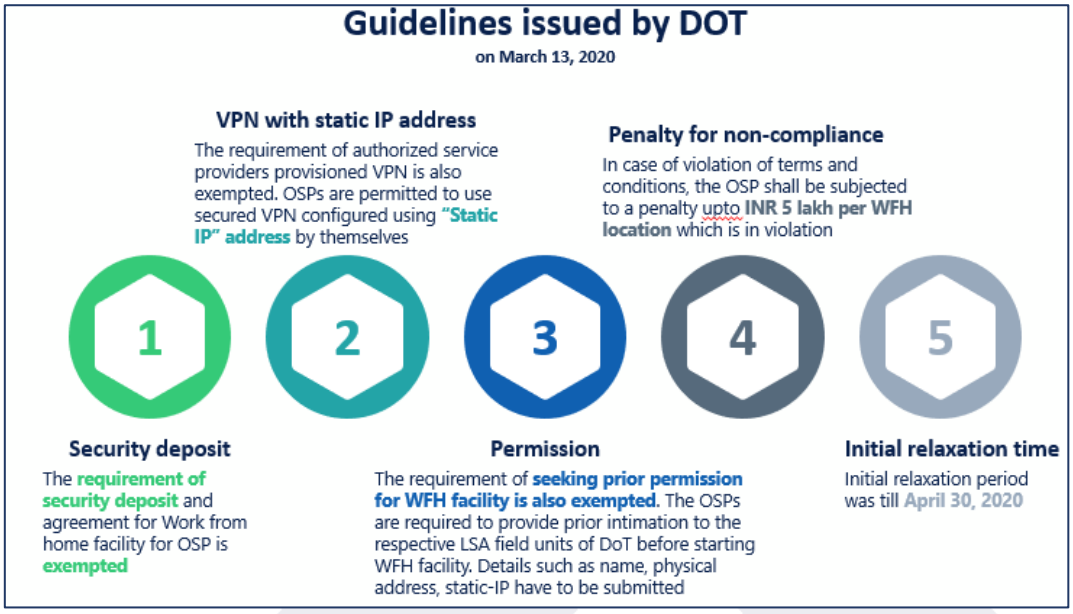

Fig 5: Initial iteration of DoT guidelines

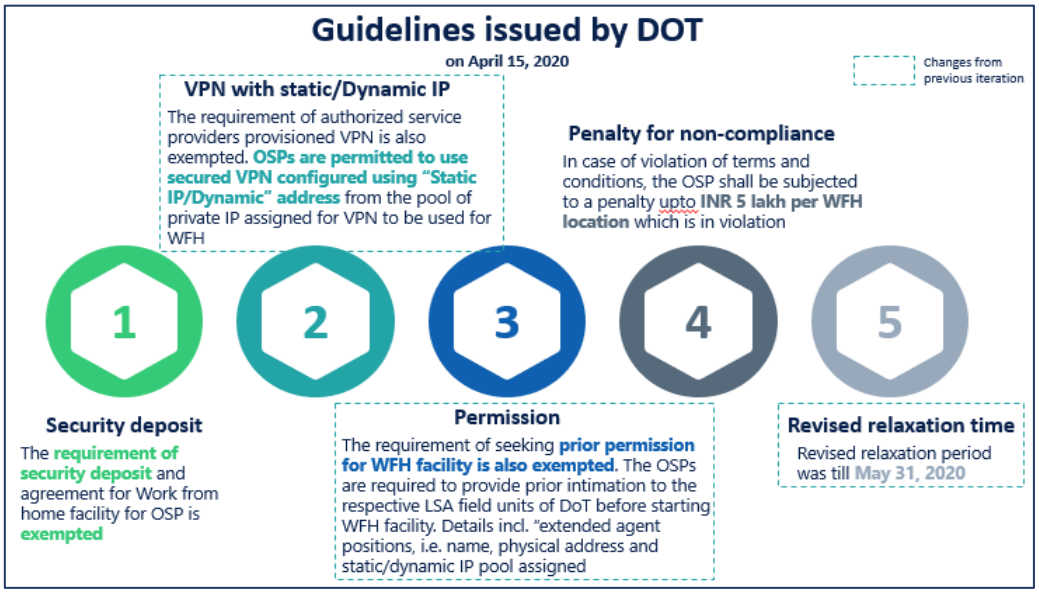

Fig. 6: Revised DoT guidelines

Clearly, the guidelines issued in April were further relaxed by the DoT. Another issue that was commonly discussed by our CISO community was the case of movement (or office commute) of workforce employed by organizations providing essential services, for instance employees supporting data center operations of a bank during curfew.

State government across many states – Delhi, Odisha, Telangana, Tamil Nadu, Kerala, Karnataka etc. have issued guidelines to procure ePass for their employees. NASSCOM has been helping in issuing advisories and spreading the awareness on the topic for easy reference.

6. Business Resiliency in Global Scale Pandemic

Recovery from the Pandemic is far from over, but the silver lining in this whole scenario is that our industry leaders are collaborating across the sectors to understand how businesses can be made resilient to this Zero-day attack on human lives. Naturally, this requires organizations apply unprecedented thinking for continuity planning.

Organizations need to think holistically when it comes to developing business resilience strategy for post-pandemic world. The possible pandemic scenarios from now on are depicted in the figure below, along with their impact on resiliency planning.

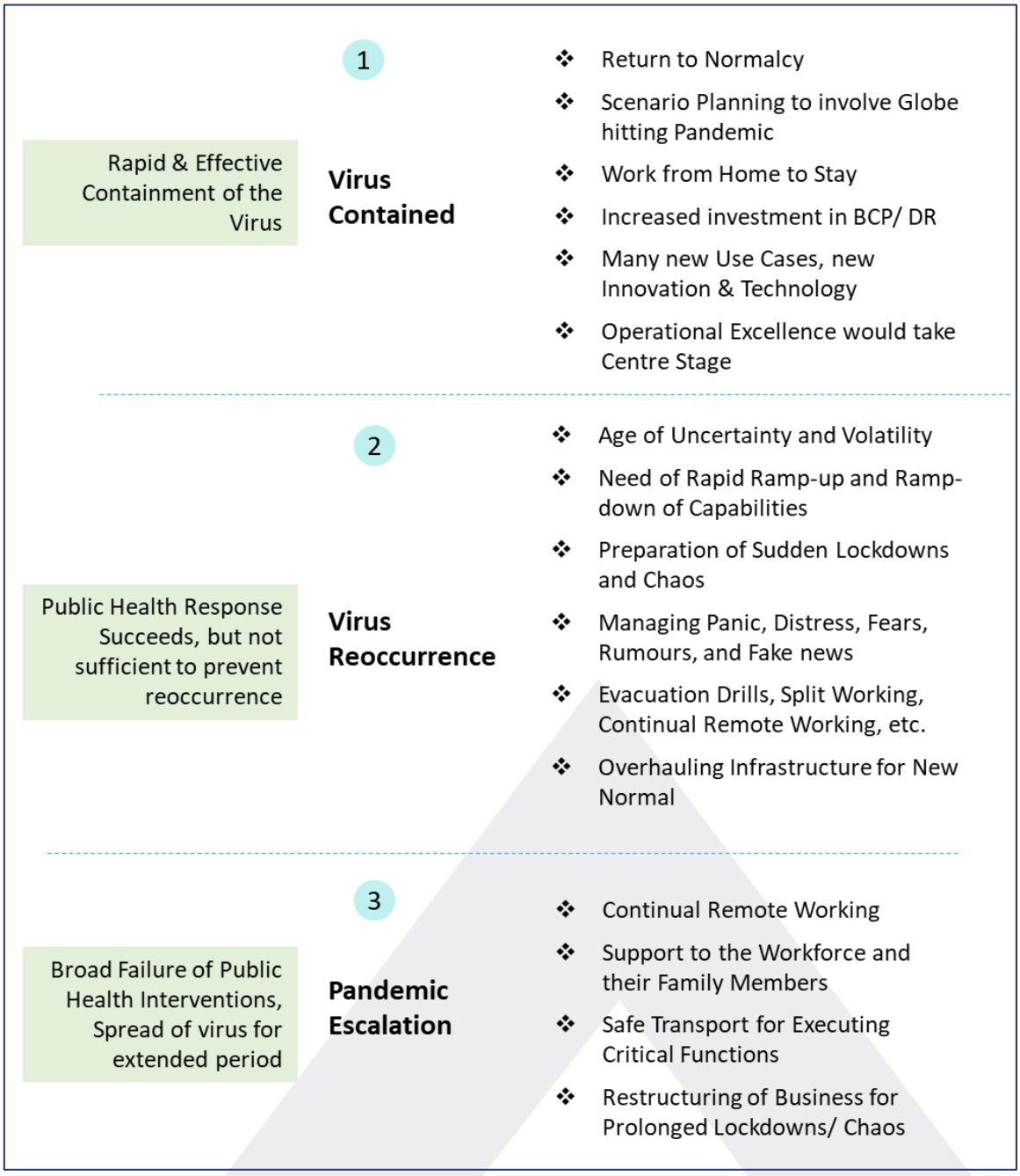

Fig. 7: BCP plan

BDM function traditionally focused on events like earthquakes, and fires fall short of the 'new-age' disasters caused by terrorists and 'pandemic hitting the world'

Scenario 1: In this scenario, the virus is rapidly and effectively contained, as per original plans and the lockdown ends as planned by the Government. Under this scenario, workforce may be expected to return to the office, at least partially. However, operational excellence will take center stage in planning of workplace setup and operational elements under the 'new normal'.

Plan to bring back workforce will be a critical element. As discussed in our paper titled "Resuming work from office under new normal", the very step will be to do people classification, either on the basis of administrative attributes such as vicinity to the office, availability of the private vehicle for office commute, or on the basis of business role attributes such as criticality of the project delivery, sensitivity of the data being handled and access to the specific areas such as lab for testing etc.

Scenario 2: This scenario will push businesses to go under lockdown again after certain time in future, but many businesses will be better prepared, given the prior experience. However, in order to transition back to the lockdown situation, would need attention towards segregation of certain capabilities that might be needed to scale up, while others that would be needed to scale down.

'COVID-19 brings unimaginative and unprecedented' scenarios for, 'One-off response needs to be translated into more bold, ambitious, and dynamic Resiliency Planning' as it's likely to be a 'long-term and reoccurring problem'

The BCP plan would require organizations to prepare the infrastructure (procuring the computing devices, end products, VPN, cloud infrastructure etc.) for new normal.

Scenario 3: There is yet another possibility that the pandemic escalates even before the lockdown is over. This would essentially require organizations to continue work from home. The scenario would require organizations to limit the workforce commute to the most essential services only. Organizations might fear chaos and challenges around productivity loss, and hence BCP must take such aspects into account.

7. Resuming work from office under new-normal

Resuming back to the workplace is a challenging task. The inputs from Kalpesh Shah, CISO, CIPLA helped to put up a 6-phase approach for it as depicted in the figure below.

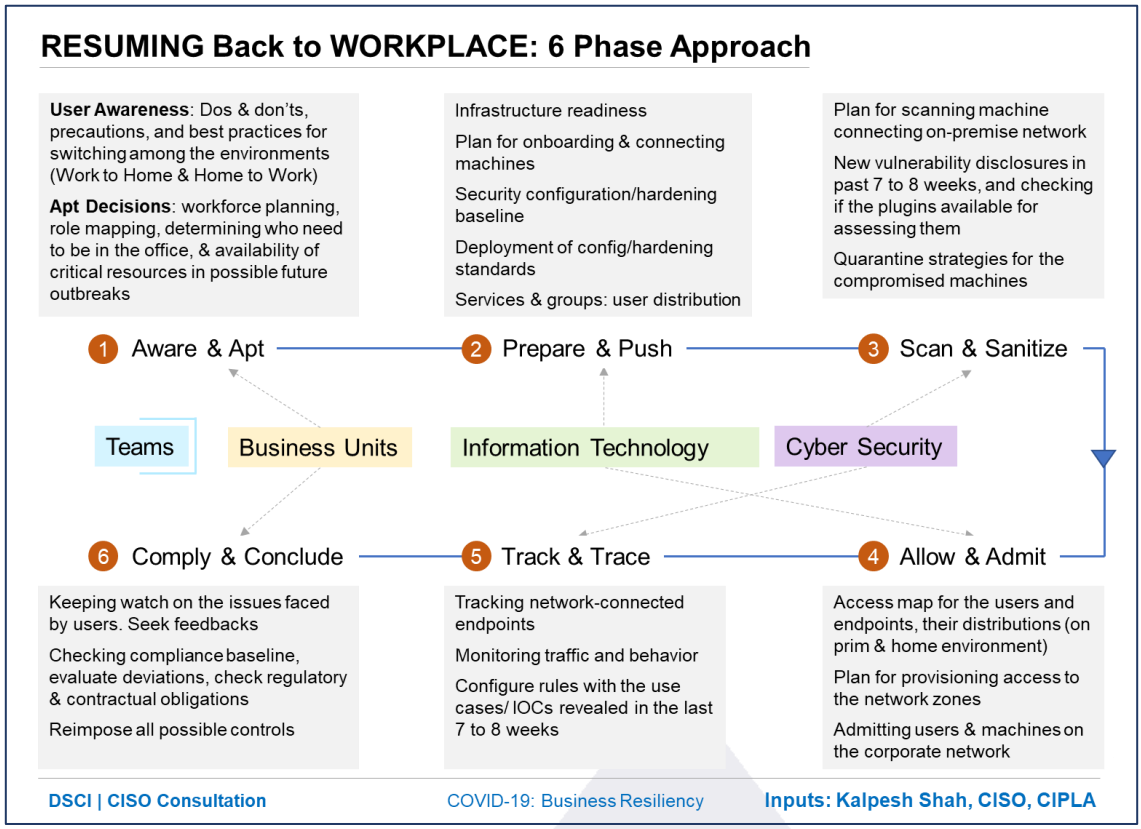

Fig. 8: Resume to work

1. **Aware & Apt**: Once the workforce planning is complete, as discussed in the previous section, CISO and his/her team must undertake efforts to develop user awareness. To be impactful and relevant, the awareness must be tuned to the specific needs of the teams.
2. **Prepare & Push**: Organizations need to develop controls to ensure infrastructure readiness, deployment of hardening standards and baseline security.
3. **Scan & Sanitize**: Scanning machines before they get connected back to the office network, check for new vulnerability disclosure in the past 7-8 weeks; check if plug-ins are available and have clear understanding of quarantining the machines becomes the next priority
4. **Allow & Admit**: Provisioning access to the network and allow employees' laptop and desktop back on the corporate network is the next step. Understanding the distribution of employees in the office premise, as well as those at home would be critical for this. Accordingly, access to the network zones should be provisioned.

5. **Track & Trace**: Organization need to step up monitoring network behavior. They need to re-configure rules based on use-cases and indicators of compromise observed and developed over the last few weeks. There is fair amount of 'noise' in the network, and hence monitoring needs to be finetuned.
6. **Comply & Conclude**: One thing that came out very clearly was zero tolerance to non-compliance. Specific efforts should be invested to bring the compliance posture back.

One of the members of the CISO community, Manikant Singh, CISO DMI Finance, shared his inputs on the possible controls that would be important. The controls depicted in the figure are derived from the inputs.

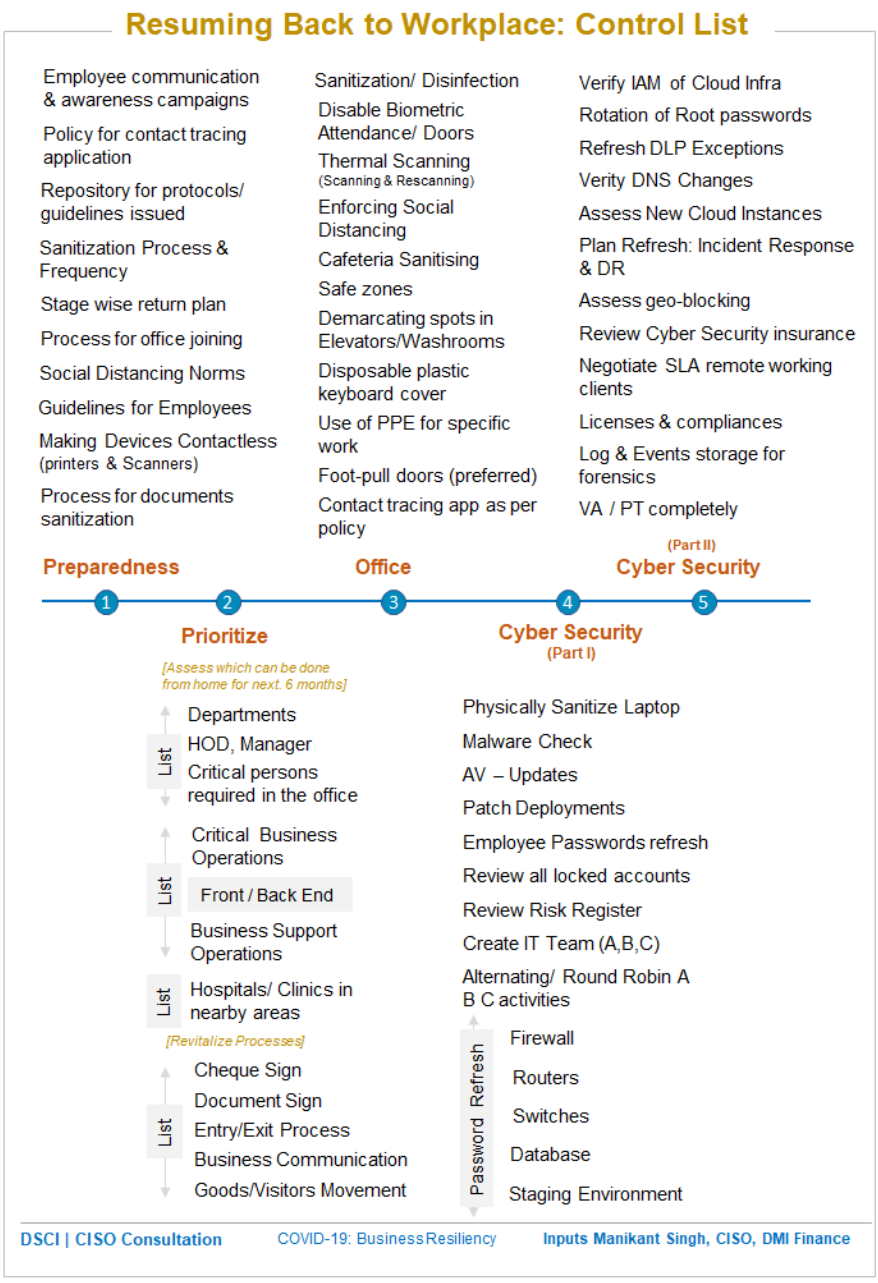

Fig. 9: Control list – resuming back to workplace

8. Managing Security

One of the global IT service providers became victim to the Maze ransomware attack. Even though this isn't a typical case of attack due to WFH scenario, this incident suggests that hackers will not miss out any window of opportunity to attack the organizations. Ever since organizations have adopted at-scale work from home, hackers have been finding ways of attacking employees and organization through phishing and ransomware attacks. The very initial step for any organization is to do the cyber-maturity assessment to understand the current status of the cybersecurity preparedness. This combined with risk appetite of the organization, CISOs will be able to have better understanding of the risk profile the organizations fits into.

Further, there are 4 aspects of managing security:

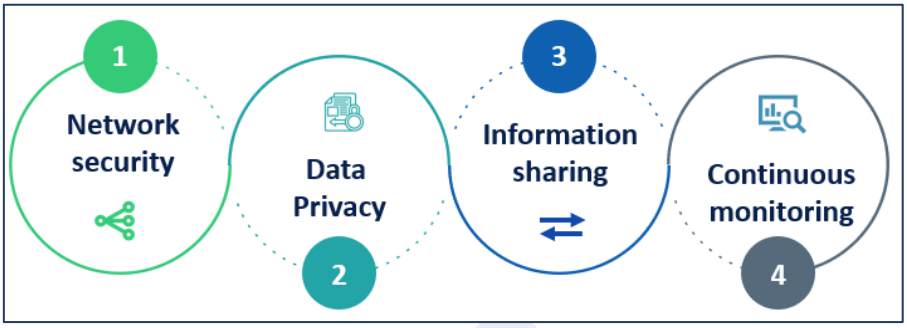

Fig. 10: Ways to manage security holistically

a) **Network Security:** Depending on the risk profile, companies can adopt following practices for network security, targeted at infrastructure to enable remote access:

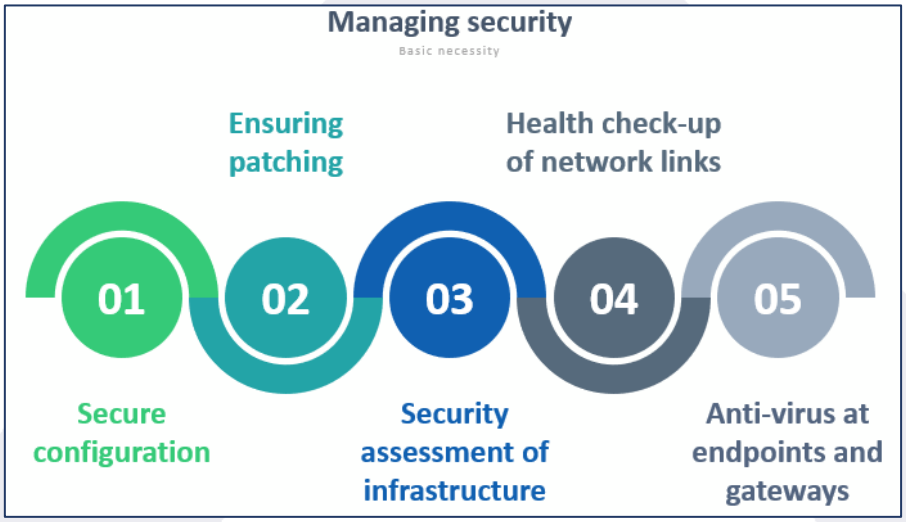

Fig. 11: Network security – basic requirements

Companies, which have higher risk profile and have appetite for investing more in security adopt following practices:

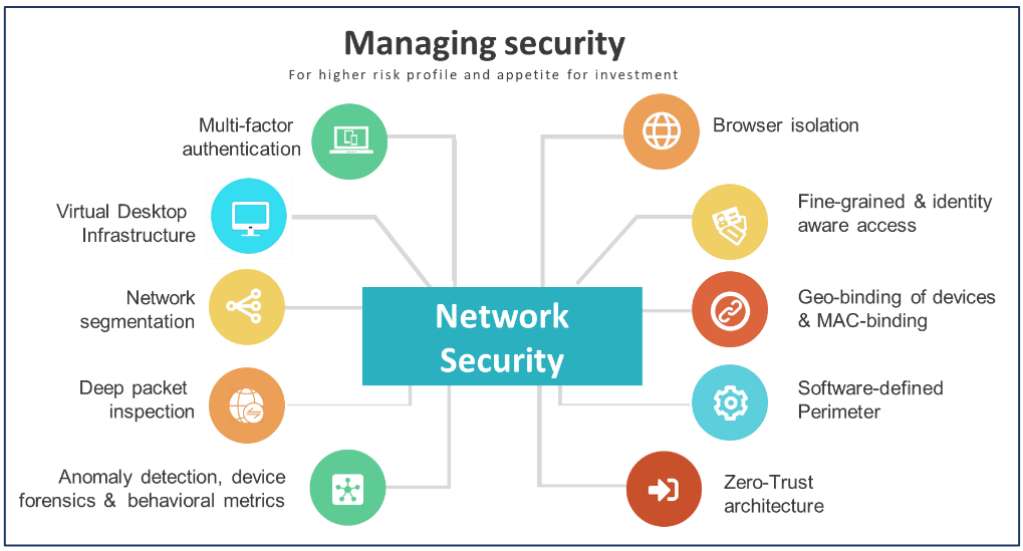

Fig. 12: Network security – basic requirements

b) **Data Privacy:** There have been multiple debates around data privacy being ignored in the wake of COVID-19. However, our CISO discussions doesn't point us in that direction. Surely, they have many other priority areas that have cropped up, data privacy still is on CISO's priority list.

Organizations should adopt following practices for securing the data:

- Encryption of channel connecting remote machines
- Monitoring of traffic and connections
- Secure protocols to accessing enterprise assets and data

Organizations, which have higher risk profile and have appetite for investing more in security adopt following practices

- Data classification
- Data leak prevention
- Information Rights Management
- User behaviour monitoring
- Forensic investigation
- Email encryption

c) **Information Sharing:** It has been observed over time that hackers keep getting better in coming up with the sophisticated techniques of carrying out breaches, it is important that information about changing threat vectors and landscape is shared within and across the sectors.

Though, the organizations and Government across the globe have been sharing information for many years now, for example creation of sector specific ISAC, there is a need to improve and increase the information sharing.

According to one of the Government officials who joined our CISO conversations there is a need of co-operation between organizations and Government, that is the information needs to flow both ways – from Government to organizations and from organizations to the Government, so that everyone in the ecosystem remains updated about the changing threat landscape and understands best practices and advisories that are being issued in response to the threats.

Only through information sharing, we can improve collaboration to enhance situational awareness in the organizations across different verticals.

d) **Continuous Monitoring**: Pandemic situation has changed the way and the scale at which we are interacting with technology. Hence for IT admins of any organizations, the network traffic that is out there for monitoring has increased many folds. This increase in the scale has led to another problem for our deployed monitoring tools – separating false positives and false negatives. There is a need to separate out 'noise'. CISOs agreed that organizations need to put in effort to reduce the noise and set-up monitoring activities.

9. Video Conference Security and Security Capabilities of Collaboration tools

As offices around the globe have advised employees to work from home, video conferencing have replaced physical meeting rooms. Recent increase in cyberattacks through collaboration tool such as Zoom has highlighted the need to follow stronger cybersecurity controls.

As an outcome of our conversations with CISOs, DSCI believes that collaboration tools must be assessed on 4 attributes – Security controls, Privacy, compliance with international standards and integration.

Fig. 13: Features in collaborative tools

a) **Technical Controls:** Some of the controls that must be in collaborative tools are as follows:

- Multifactor authentication, SAML-based single sign-on
- Single sign-on
- End to end encryption – for media (e.g. using Secure RTP), and for network communication (e.g. using OAUTH, TLS, Secure RTP)
- Advanced protection program, which includes – Threat protection policies, real-time report to monitor ATP performance, automated investigation and response capabilities etc.
- Backup encryption, etc.

b) **Privacy**: The tools must be compliant with some of the leading privacy frameworks such as GDPR, EU-US and Swiss privacy shield, Children's Online Privacy Protection Act (COPPA), the Federal Education Rights and Privacy Act (FERPA), the California Consumer Privacy Act (CCPA), and other applicable laws etc.

c) **Compliance with Security Standards**: These standards include ISO 27001, 27018, SOC2, TRUSTe, HIPAA, etc. The compliance provides the trust factor to the users that cybersecurity is being followed

d) **Integration**: If collaborative tools can integrate with other leading applications, the chances of air gap in security decreases.

Besides these features, there are some best practices that must be followed while handling video conferencing tools. Some of the practices are:

a) Don't click on video conference links shared by unknown individuals

b) Don't make meetings public, unless it is necessary

c) All meetings should require password and should have features such as waiting room to control the admittance of guests

d) Don't re-use or re-share the passwords and meeting tokens

10. Legal and Compliance

Legal and compliance is a very important component, especially in the current situation. Holistically covering this component will require to look closely into 4 interfaces, as shown in figure 14.

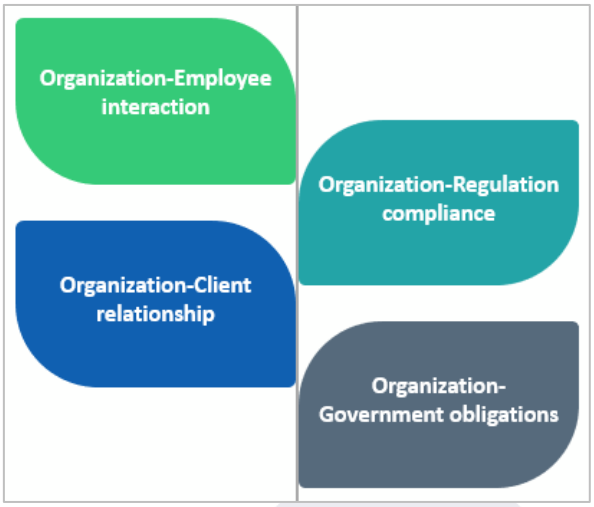

Fig. 14: Interfaces to understand Legal and compliance

a) Organization-Employee interaction

One of the key aspects to understand is that due to sudden lockdown, the entire ecosystem of organization-employee interaction has shifted from guarded and secured corporate setup to employee's home. This has resulted in potential legal risk, especially when it comes to non-disclosure agreements. According to many CISOs we interacted with, they brought up mandatory requirement for employees to sign advanced level teleworker NDA. Organizations are worried about sensitive data leakage at this stage, and NDA can help to assure that due care has been taken by employees for the data.

There is also an issue of licensing compliance within this dimension – organizations need to ensure that employees are processing (or consuming) the data on licensed version of the software, including Microsoft product suite and other specific tools and applications.

b) Organization-Client relationship

Clients want to ascertain that organizations adhere to the SLA agreement. SLA agreements cover two aspects – performance and security & privacy. The sudden shift from office to home has brought in cultural change aspect along with it and many CISOs and clients fear that they would impact the productivity and performance. However, as interactions with CISOs progressed over the seven weeks, it was very apparent that CISOs across the sector can either maintain or increase the productivity.

Another aspect to be considered is the legal sign-off from the client for work-product, milestone achievement, planning, vendor onboarding and various other aspects of day-to-day project management.

Conducting important meetings such as board meetings over virtual platform is another important aspect in this relationship. Though it can be made mandatory to sign declarations (just like in the case of physical meetings) before any important meetings, but security and privacy aspects in virtual tools worry companies.

c) Organization-Regulation compliance

This relationship can be studied through two lenses – Data privacy expectation and cyber incident reporting.

For data privacy, organization should ensure that all data controls are in place so that employees can work on sensitive data, without any data leakage. Such controls also become part of any organization's compliance program.

If any organization is breached, it is comparatively simpler to report the incident and act swiftly post the incident has occurred. However, if the personal laptop of an employee is breached, it becomes very difficult for organization to act swiftly and report such incidents to regulators. Hence this raises the legal and compliance concern for organizations.

d) Organization-Government obligations

Government (via CERT-In, DoT, NCIIPC and sectorial ministries etc.) is actively working on issuing advisories on technology usage, including collaboration tools, in work from home scenario, pushing wide-use of contact tracing app and sharing information on threats to Indian organizations.

This implies that organizations must be on a look out for frequent updates to the new advisories, so that new and updated protocols are being adhered by the employees.

11. COVID 19 New Normal: Security Architectural Paradigm

The COVID-19 pandemic outbreak, the transition towards remote working, and likely continual of it for a longer duration brings a new paradigm of cybersecurity. Although security engineering is moving far more beyond the enterprise perimeter, gradually moving to the cloud and putting its reliance on platformized capabilities, COVID-19 accelerated the process. During the series of discussions, the CISOs underlined the use cases that have become important during the pandemic. The following figure summarizes them.

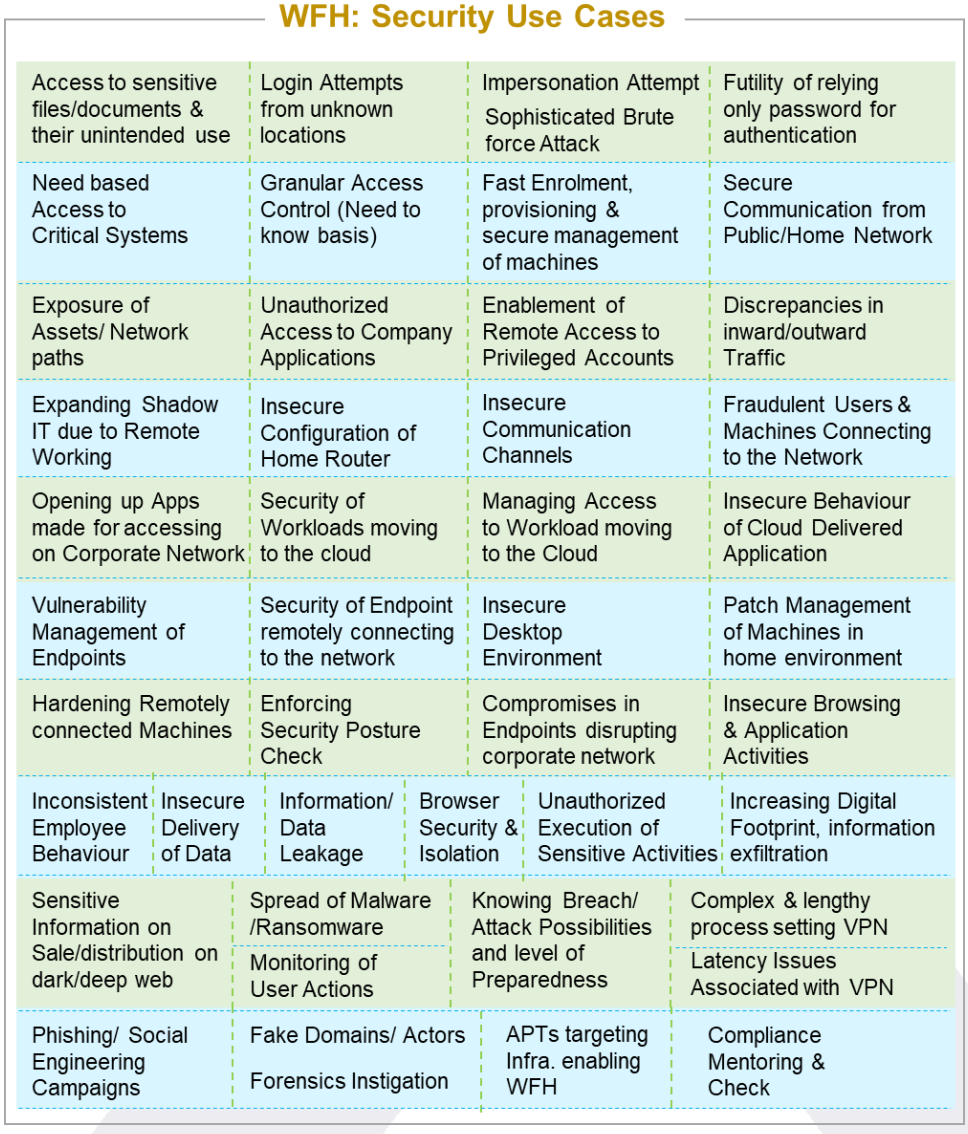

Fig 15: Security use-cases

The WFH paradigm challenges the existing security, which is focused on the perimeter and centralized defence, where all traffic is filtered through the gateway security solutions. It would not be practical in the new paradigm nor would it be feasible from the security

perspective. There is a need to overhaul security design, imbibe innovative ideas, and approach it with fresh minds.

The figure illustrates the architectural ideas that would be dominating the new security paradigm. Some pieces have been under experimentation, development and deployment. However, the COVID-19 pandemic pressed the accelerator for more innovation, development technologies and adoption.

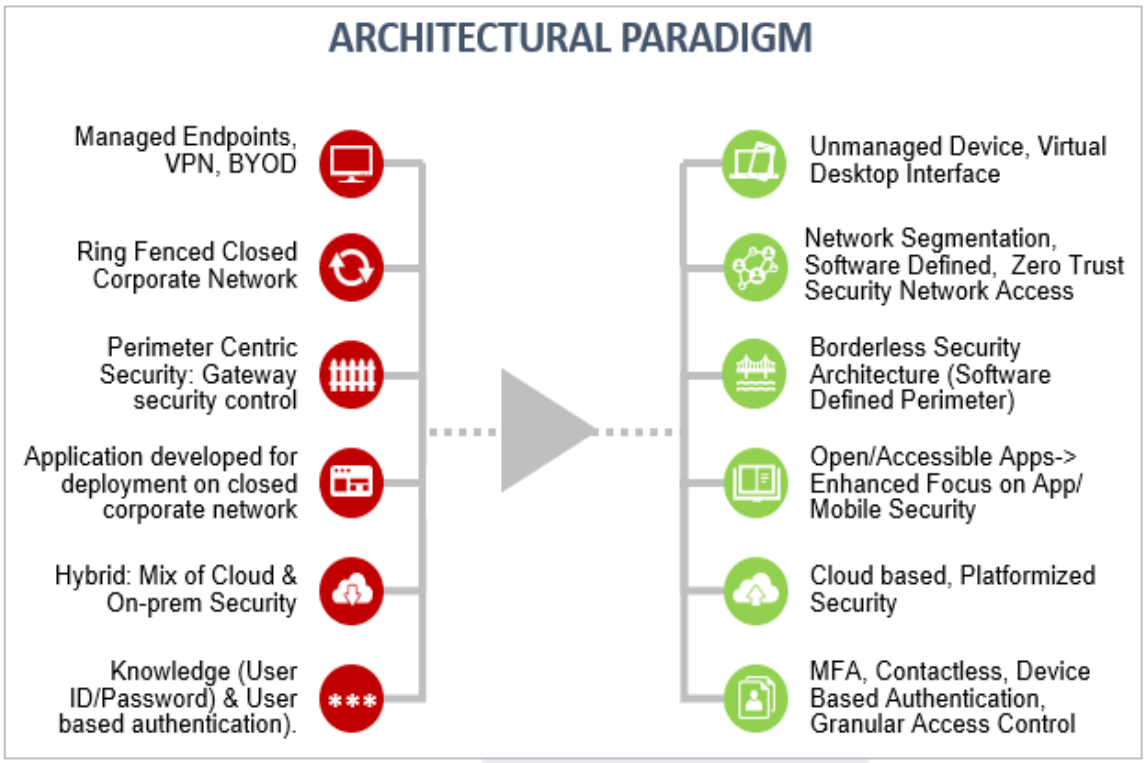

Fig 16: Architectural paradigm

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