BEING RESILIENT

ASSURING DIGITAL TRUST IN THE NEW WORLD OF WORK

Infosys®
Navigate your next

BEING RESILIENT. THAT'S LIVE ENTERPRISE.

SUMMARY VIEW

Recently, in just three weeks we moved 80 percent of our 240,000+ employees - the world over - to securely work from their homes, and we are happy to share the learning from our experience. We looked at the challenge from a perspective of securing the move to remote working *by design*, securing it *at scale* and securing it *for the future*. Here's what assuring digital trust in the new world of work entails:

Dealing
with the expanding and new threat surface

Protecting
against data breaches and attacks on remote assets

Balancing
security with user experience and productivity

Prioritizing
and re-calibrating governance and compliance

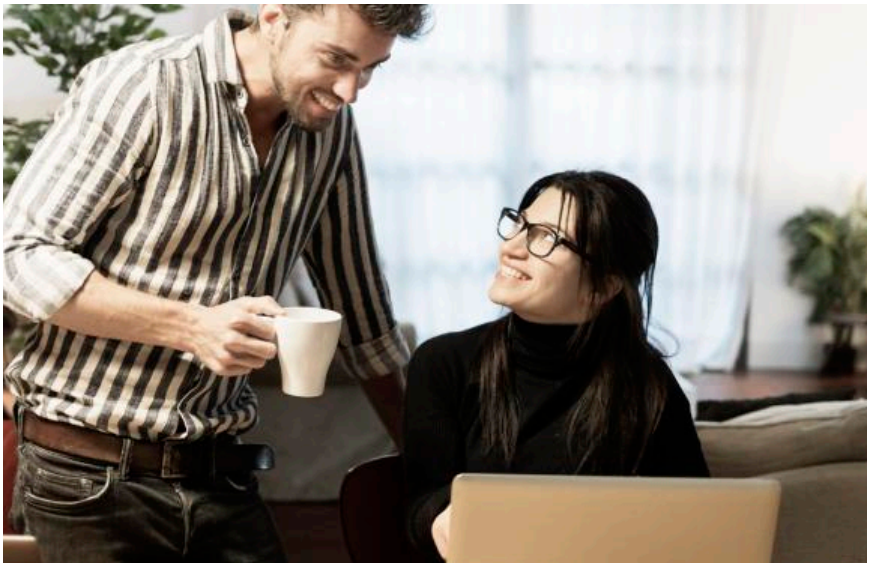
Making
cybersecurity a foundation for the new digital era

Humanity has woken up to the realization that we can feel so defenseless in the face of calamity. For many of us, this feels like being in the middle of a wartime drama, or watching, as if in a movie, the Great Depression unfold around us. Only, this sudden shadow in our lives is very real. This rude awakening from our collective complacency is driving a deep need in us all to protect against further perceived risks and take back some of our sense of lost control. Understandably, this apprehension is spilling into our work lives as well. In many ways, our enterprise digital infrastructure is helping us get started on the path to greater confidence and resilience, but the fact remains that this digital infrastructure has not been stress-tested before in an exponentially stretched situation such as the one we are up against. Nor do we know that we truly have the ecosystem of digital resources we will need to meet the challenge in the moment, and in the days onward. *Is our preparedness enough?* is a question that we need to continue to ask, answer and evolve.

Our approach to work will shift almost entirely to the digital, because the distributed remote working that we are facilitating today, driven by our adoption of physical distancing, may become the norm tomorrow.

With this will come the inevitable discomfort of potentially exposing our organizations to cyberattack if the right precautions are not taken to adapt to this new world. The urgent upgrade of infrastructure and the need to expand virtual private networks is all consuming. So is the need to update the technology backbone that supports it all. Beyond the technology, policies are also coming under the scanner in a bid to make them more relevant for this new reality, including briefing remote workers on their right to be aware of the risks, company privacy and security policies, guidelines, monitoring process information, and several other essentials like adhering to the right security behavior.

Remote work fundamentally changes the dynamics, especially for teams habituated to working side-by-side every day. People suddenly forced to change their behaviors can experience loss in productivity, collaboration snags, communication hitches, and other unforeseen hurdles as they shift from their corporate fortresses to modest home offices. And these unexpected changes can seed and drive security risks especially where we fail to recognize this change and adapt to this new way of conducting business.



Employees working from home rarely have the same firewalls, network-based intrusion detection, and other defenses integral to the offices we are all accustomed to working from. What's more, at home, there is a tendency to let one's guard down because we feel safer. Poor computer security behavior at home, however, can lead to insecure actions in the context of work tasks, significantly expanding the attack surface. This exposes the vulnerability of the one place we feel least vulnerable in – our own homes. Fittingly enough, the cybersecurity industry's response has been a call to embrace Zero Trust Security - centered on the belief that users should not automatically trust anything inside or outside the perimeters of the work landscape, and instead verify anything and everything trying to connect to the organization's systems before granting access. A well-intentioned, and arguably effective strategy if fully realized, however, it does little to truly shore up our trust capital at a time that most tests it. Besides, the Zero Trust Model is a hard nut to crack especially for organizations that are still on the journey to retiring their legacy systems. Recently, having walked a highly effective alternate path ourselves, when in just three weeks we moved 80 percent of our 240,000+ employees - the world over - to securely work from their homes, we are happy to share the learning.

We looked at the challenge from a perspective of securing the move to remote working *by design*, securing it *at scale* and securing it *for the future*. To put it simply: *Digital Trust. Assured.* And here's what that entails:

Dealing
with the expanding and new threat surface

A 2019 survey of over 1,500 US and UK workers found that work and watercooler chatter blur as remote workers use workplace collaboration apps. 76 percent discussed their personal lives on these platforms, a quarter talked negatively about their bosses, and another quarter shared confidential company information. How securely third-party platforms store information cannot be entirely controlled, and this is a risk for employers. Employees too can land in trouble with their company and even risk being blackmailed.

We are looking at a future when we must move from less than 10 percent to 100 percent of our workforce in the remote working mode. This will not only expand the threat surface but also create new surfaces for attack in the form of remote access infrastructure, remote access methods, collaboration platforms, and the like. The need to focus on modernizing our critical legacy systems to make them accessible remotely is urgent and real. So is the need to build new use cases to identify new attacks and fraud patterns. Because, it's the same technologies arming remote workers with powerful new capabilities that are also exposing them to new threats, that they need to be defended from. These hazards are born from both technical and behavioral vulnerability.

- Collaboration tools for remote working, such as Zoom, Citrix, Confluence, Slack, Skype and Google Suite, now outside enterprise controls, could be targeted by threat actors and used to access confidential information, especially if users use their personal laptops, desktops, and phones to connect into the office.
- Remote connections through VPN without multifactor authentication and encryption will increasingly become targets for malicious activities and the playground for coordinated malware attacks.
- Voice assistants at home could be potentially compromised and the possibility of official conversations and recordings falling into the wrong hands cannot be ruled out.
- Data traffic passes through that same router that's connected to many devices, including various smart home appliances, which may not have up-to-date protection. These are potential easy access point for hackers.
- With remote working becoming the norm, hackers will increasingly target specific remote workers for phishing attacks after having gathered personal information from publicly available sources like Linkedin and Facebook. We could also expect intensified attacks during the early fragile phase where organizations are grappling with stabilizing this massive shift and fine-tuning their security gameplay.
- Misconfiguration of cloud services – so integral to remote work setups – is common when implementation is on the fly and at large scale thus increasing the organization's risk.
- Provision to transfer work data to personal devices can cause unintended outflow of information outside of the safe zone.
- Instances of misuse of PCs and mobile devices, logged in to the network, but left unlocked and unattended are not unheard of.
- With employees accessing systems at unusual times, and also accessing systems they otherwise regularly didn't, the behavioral analytics trackers may alert the administrative teams to false positives, overwhelm them, and compromise the veracity of valid alerts and associated priorities.
- When applications prescribed for use in home offices are not supported by adequate documentation and user-help, it can leave employees confused but with jobs to carry out, often creating

situations of risk for the company. For example, users unable to join in a video conference conducted over the VPN, because they have difficulties configuring the VPN, may conduct the meeting on a more vulnerable platform.

- Even if the existing controls could easily squash new attacks, the introduction of so many new remote devices in networks can lead to changes in the playbooks which might overwhelm SOC analysts and their processes.
- Unsecured public wifi networks, at places that remote workers may temporarily choose to work in as they juggle their work and personal priorities, are prime spots for malicious parties to spy on internet traffic and collect confidential information.

QUICK CHECK

- ✓ Build secure connectivity models and standards for remote working leveraging VPN with multifactor authentication. Recalibrate security policies and standards to adjust to the new connectivity models and possible attack paths.
- ✓ Ensure connectivity only from hardened and managed corporate endpoints (desktop/laptop) with updated antivirus, security patches, anti-Advanced Persistent Threat, data loss prevention agents and encryption enforced.
- ✓ Carve out a segregated network for VPN clients connecting to the corporate network and allow them to access corporate resources.
- ✓ Recalibrate fine-grain access control to corporate infrastructure and applications.
- ✓ Ensure strong network and system-level authentication before granting access to corporate systems via MS RDP.
- ✓ Disable insecure protocols/ services such as SMB/ NetBIOS over TCP/IP to reduce vulnerabilities and attack paths.
- ✓ Harden security for VDI infrastructure including but not limited to security updates, antivirus, anti-Advanced Persistent Threat, and data loss prevention agents.
- ✓ Whitelist IP addresses and domains for outgoing traffic where appropriate and feasible. Block all unwanted domains and ports.
- ✓ Enforce restrictive permissions to prevent data leakage. For example, disable clipboard functionality on Citrix and other RDP setups.
- ✓ Recalibrate the rules of behavioral analytics and security operation centers to minimize false positives.
- ✓ Put together a robust security incident management plan and 24/7 open communication channels for users to report incidents and monitor incidents.
- ✓ Secure configuration and heightened auditing of cloud services to avert data leakage.
- ✓ Bring renewed focus on screen lockouts and session time-outs.

Protecting
against data breaches and attacks on remote assets

Surveys in the US point to the fact that 47 percent of data breaches are caused by human error. And with breaches costing companies an average of $3.6 million annually, the role employees play is too significant to ignore, especially when left to work from their home offices without in-person guidance, peer-reviews or supervision.

Data breaches can cause distressing financial and reputational losses for organizations. From lost business to regulatory fines and remediation costs, data breaches have far reaching consequences. Human error has a well-documented history of causing these fissures in our security systems and need to be prevented.

- Careless exposure of data printed out in physical form is a greater risk with remote workers operating outside of secure corporate offices.
- Users need to be alerted and protected against malware designed to harm devices or software. They commonly masquerade as warnings against harmful software and convince users to download varying types of software that can steal, encrypt or hijack computer functions.
- Home offices are more vulnerable to attacks through emails, sometimes with malicious attachments. Phishing scams are one of the most common ways hackers gain access to information. Phishing involves sending fraudulent emails that appear to be from a trusted source, with the goal of deceiving recipients into either clicking on a malicious link or downloading an infected attachment.
- Virtual networks connect with multiple remote workers. However, the encrypted tunnels in virtual networks are rarely inspected, allowing attackers to go undetected. Cyber criminals can use these tunnels to create man-in-the-middle attacks to eavesdrop on encrypted traffic, tamper or steal data.

- Denial-of-service perpetrators are likely to begin to target remote working employees to gain access to enterprise resources and make these unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

QUICK CHECK

- ✓ Conduct frequent training sessions and establish lines of communication to educate employees about cyber threats and their responsibilities in relation to the company's information security program and the dos and don'ts linked to remote working.
- ✓ Address topics including but not limited to malware, phishing scams, acceptable usage of company resources, clear screen; clear desk, disconnecting from corporate network when not in use, keeping personal devices secure with strong passwords, up-to-date antivirus, personal firewall, encryption, patches and incident reporting.
- ✓ Seek electronic end user consent and acknowledgment to ensure acceptable usage of company resources while working from home.
- ✓ Continuously reiterate best practices to users and clearly demonstrate extent of compliance to stakeholders and executive leadership.
- ✓ Disable print access to corporate as well as personal devices while working from home.
- ✓ Disable screen scrapping and print screen applications on endpoints.
- ✓ Implement advance endpoint detection and response capabilities for all end points to protect employees from zero day attacks.

Balancing
security with user experience and productivity

Qualitative feedback from surveys point to the fact that remote workers tend to abandon security procedures that interfere with their workflow, and as a result, are often willing to jump over the security check, if they can, at the expense of cybersecurity. When they cannot, their work productivity is hampered. This indicates that, apart from changing human nature, the only way to prevent remote workers from taking security shortcuts is to provide a streamlined and hassle-free work experience while building transparent cyber security controls.

Traditionally enterprises have centered on creating security for systems, but the time has come to focus on developing security for people. With adversaries increasingly targeting remote workers, additional vulnerabilities are created when these workers do not correctly follow security processes. Our default reaction tends to be to blame the victim, even penalize for not following the procedures. It may be valuable, however, to look at why that incident happened. What gaps existed in the defenses that exposed the employee to threat actors? What was it about the security solutions and processes that caused the employee to sidestep them and create additional risks?

- Dispersed remote workers need access to seamless collaboration, consistent connectivity, and assurance against security breaches.
- Organizations doing all they can to prevent endpoint breaches targeting employees, frequently locking access to resources, blacklisting websites and conducting time-guzzling security-awareness tests, can be oblivious to the not-so-insignificant costs this entails in terms of employee productivity.
- Applications that require significant Internet speed and capacity to download or to use can also hamper the productivity of remote workers.
- Inadequate or unclear instructions for users exposed to a plethora of new and potentially confusing spread of work-from-home enablers can slow them down.
- Employee analytics that try and simulate 'in-the-building' and 'at-the-desk' metrics with focus overly on time and effort metrics, instead of outcomes can be counterproductive to real employee productivity. Even for remote workers whose working hours on a project are billed to clients, outcome-based metrics drive better productivity.
- Extra security can mean extra roadblocks. It's hard remembering several usernames and passwords. Factor in two-factor authentication, SMS text messages and more, and this can likely frustrate users.
- Session time-outs that improve security and drive optimal management of resources, may indirectly impact user experience and productivity leading to user frustrations.

QUICK CHECK

- ✓ Upgrade VPN infrastructure to allow more bandwidth and ensure fast and seamless access to company resources for remote workers.
- ✓ Amplify help-desk capabilities with intelligent self-service to drive higher service capacity and lower cost per service-request lower, as the remote workforce scales.
- ✓ Test new models for connecting effectively. For example, creating various levels of authentication based on a trust score and built from the risk factors found for each user or activity, in other words adaptive authentication.
- ✓ Implement security technology and processes that are designed with user experience in mind. For example, Fine-tune session time-outs to achieve a fine balance between user experience and security considerations.
- ✓ Ensure security is ingrained as an integral part of remote worker behavior. Publish FAQs and other supporting documentation, conduct workshops and training to allay confusion and any resulting risks with respect to remote access. Hygiene in the healthcare industry is a good example of this approach in action – observing the behavior of physicians and iterating on signage in hospitals leads to more consistent handwashing, and therefore better patient outcomes.
- ✓ Ensure processes keep users informed, and manage their expectations. For example, publishing that a service will take five or 20 minutes to activate will help reduce potential frustration and minimize impact on the workflow.

Prioritizing
and re-calibrating governance and compliance

Just 51% of respondents in a recent CISO Benchmark Study said they feel they are doing an excellent job of managing employee security. Risky user behavior (For example, clicking on malicious links in email or websites) remains one of the top CISO concerns. Having organizational governance that starts with pervasive security awareness training and builds all the way up to nurturing a secure-first organization culture is crucial in the time of remote working.

Most current security organizations are still driven from a mostly work-from-office perspective. The resulting structures, decision rights, and processes are inadequate to deal with cyber risk associated with remote working. We need to bridge the historical gaps in information security, business continuity, and crisis management. We need to align with relevant industry standards so that we can more effectively work with others to manage incidents. Establishing strong architectures for data, systems, and security 'by design', 'at scale' and 'for digital resilience and trust into the future' is key.

- Since the protection of data is the liability of the organization, internal policies need to be established for the protection and retrieval of such data should it be lost or compromised by a remote worker.
- The right to monitor remote workers comes with several limitations, including obtaining the consent of the employees, the notification of surveillance, with specified limits on the monitored areas. These need to be addressed before the process of monitoring.
- Monitoring guidelines must not violate the right of privacy that a remote worker has. For example, organizations cannot collect data from personal chats or conversations unless having obtained judicial authorization.
- Work from home policies are often not reviewed from a security-first lens, and when corresponding learning resources are not made available to remote workers, security can be compromised.

QUICK CHECK

- ✓ Establish strong governance processes to ensure that any remote connectivity to client networks is enabled only after highlighting applicable risks to them and obtaining relevant consent.
- ✓ Build mechanism to access bird's eye view of remote operations.
- ✓ Consider recommendations from the Data Privacy Office when framing policies for remote user monitoring.
- ✓ Obtain employee consent for monitoring and surveillance in compliance with applicable legal and regulatory mandates.
- ✓ Budget for greater investments in intelligent automation to amplify the staffing model.
- ✓ Budget for investment in new systems and software required to support new use case scenarios emerging from the need to secure remote working. For example, keystroke dynamics authentication.

Making
cybersecurity a foundation for the new digital era

In a 2020 Marsh & McLennan survey of 1,500 executives, respondents claim that security's overall role in organizational digital transformation has improved both in awareness and involvement in earlier stages of the design process. Today CISOs, more than ever before, need to be integral to the transformation as they look to transform their own capabilities to respond to a new normal where the work and talent value chain are both fully digitized and remote as scale.

- With the adoption of agile ways of working, like remote workers building upon each other's work in iterative cycles of simultaneous collaboration, security considerations can take a backseat.
- Investments in transformative technologies can be meaningless if they can't protect the business, its customers or other vital assets, and the complexity and speed of development continues to challenge the most robust security organizations.
- IT and operational technology integration brings new connectivity, data sources and potential vulnerabilities that need protecting, and it is challenging to connect the dots between the organization's security and its ecosystem of partners and vendors.
- There is merit in exploring distributed security models such as having security leaders attached to every digital practice but also reporting centrally to the corporate security organization.
- Security teams can no longer be the 'office of nay sayers'; they need to be agile and ramp up capabilities to add security at the speed of transformation.

QUICK CHECK

- ✓ Recognize cyber security as part of the core foundation and an integral part of the strategic response plan to thrive in the new normal.
- ✓ Assure clients of ongoing security and business continuity plans. Build the governance models and interventions that make these assurances credible.
- ✓ Initiate daily stand-up calls with security operations and design teams to ensure fidelity of security policies, standards and execution to meet the changing requirements of remote working at scale.
- ✓ Focus on stabilization and implementation of best practices and industry collaborations.
- ✓ Be nimble in changing policies, reviewing new risks and draw clear plans for remediation with complete transparency and visibility to the organization's leadership.

A glimpse into how we did this for ourselves

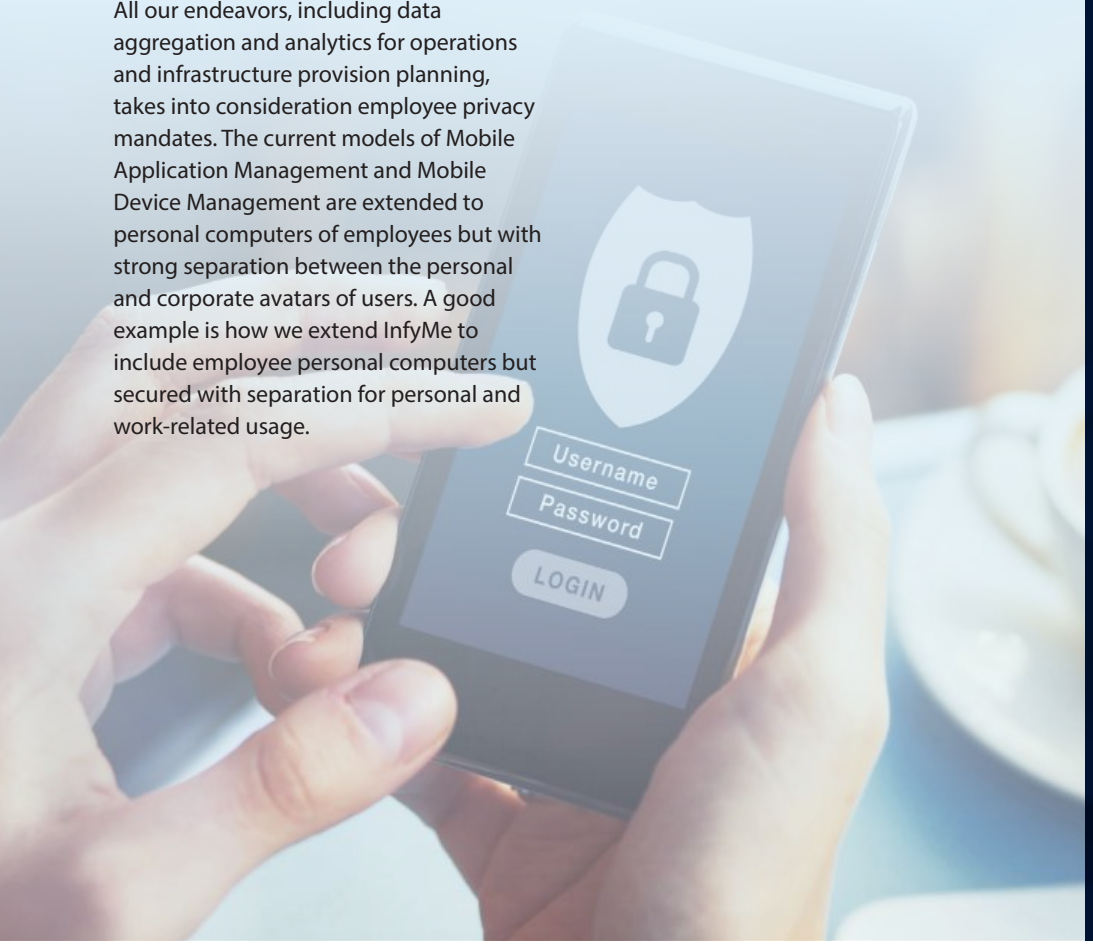
For any enterprise to be able to protect data, in a distributed network of remote workspaces, information tracking and security policies will need to be deployed with the ability for the business to minimize security risks. Control will continue to move to the edge – and the user device will become a converge of wide area networking and network security services like CASB, FWaaS and Trust Assurance in a single, cloud-delivered service model. We made sure we adopted Secure Access Service Edge. Our cyber defense centers are being operated remotely too.

We made significant adjustments to the rules for monitoring and use case generation so we could adapt to the new ways of working, and work past the clutter of false positives which we expected will be potentially created. We also identified new rules and use cases for adversarial actions.

All our endeavors, including data aggregation and analytics for operations and infrastructure provision planning, takes into consideration employee privacy mandates. The current models of Mobile Application Management and Mobile Device Management are extended to personal computers of employees but with strong separation between the personal and corporate avatars of users. A good example is how we extend InfyMe to include employee personal computers but secured with separation for personal and work-related usage.

We developed new models to monitor employees for reasonable assurance of their productivity without conflicting privacy mandates. Preparing for this scenario included behavioral coaching for managers to not pose unduly probing questions – for example – about the employee's personal routine.

We have invested in a modern security stack (Multifactor Authentication, Conditional Access, VPN, Terminal Access, Endpoint Protection Platform, Endpoint Detection and Response, Data Leakage Prevention, Patching, Hardened Build, etc.) for endpoints which gives us ongoing assurance of security of these devices and relevant insights as well. Our remote monitoring and management solution stack provides unified control and visibility into our entire IT infrastructure, so servers, networks, and endpoints can be actively and remotely managed. We are rapidly upgrading this infrastructure to support the exponential need for remote access.



OUR QUICK CHECK

- ✓ Upgrade and expand infrastructure for VPN and extranet.
- ✓ Accelerate patching for critical systems.
- ✓ Identify and monitor high-risk user groups.
- ✓ Confirm the security of third parties. Should any of them fail to demonstrate adequate security controls and procedures, consider limiting or even suspending their connectivity until they remediate their weaknesses.
- ✓ Keep an eye out for new shadow-IT systems that employees use or create to ease working from home, to compensate for in-office capabilities they can't access, or to get around obstacles.
- ✓ Build a policy portal for remote workers to find solutions for frequently occurring scenarios where they might need guidance. For example, the different rules that govern usage of a device in a client network and in the Infosys network.
- ✓ Communicate creatively focusing on what to do rather than what not to.
- ✓ Build a portal to track incoming user with auto recommendations for effective action, based on established track records.
- ✓ Maintain a risk register to track risk-related decisions and reassess them over time. This also facilitates robust reporting to the executive leadership and guides policies for risk identification, evaluation and mitigation.
- ✓ Augment support team with staffing and automation-led amplification to ensure greater support and faster problem resolution for our greatly expanded workforce of remote workers.
- ✓ Connect with clients to request contractual consent for employees on their projects to work from home. The contract appraises them of potential risks and the proposed security assurance plan. This is a mandatory process preceding the activation of systems and devices enablement for employees to work from remote locations.

End Notes

Our digital muscle - be it mobility, remote access, collaboration platforms, cloud adoption and cyber security - has served us well in these unprecedented times. However, there's a lot to be done in terms of making our systems more stable, robust and secure while equipping our workforce to embrace this new way of working.

In many ways, employees working remotely are the true front line of the organization and play an important role in keeping it both functioning and secure. Businesses will need to consistently reiterate to employees their safe remote-working protocols and procedures while helping them focus on being productive. With this in place, CISOs can play their part in creating a resilient and assured digital future for their organizations.

For more information, contact askus@infosys.com

Infosys®
Navigate your next