Digital Fortress to Digital Bunker – the new cybersecurity model

India is a key source of outsourced IT services for overseas entities. These services often comprise critical dependencies for regulated entities, such as banks and insurance companies. The majority of these IT services are provided from metropolitan areas such as Mumbai, Pune, Hyderabad, Gurgaon and Bangalore, which have all been hit hard by COVID-19. These cities have been put under lock down until May 3, 2020, with the likelihood of extension (at least in some form) beyond this date as well.

Under the lockdown, the preferred model for continued IT/ITES operations has been to implement a 'work from home' ("**WFH**") policy, and IT service providers have executed continuity plans based on the WFH model on an unprecedented scale. Nonetheless, COVID-19 has challenged (and, at times, disrupted) the ability of service providers to deliver on the security and service levels originally contemplated under their contracts.

What is the impact on services?

A combination of arrangements such as relocation including nearshoring and WFH, limited client *in situ* delivery and very limited services being rendered on-site from provider locations (with lockdown exemptions from the government) have ensured that most contracts are serviced (at least to some extent). Nonetheless, it is not business as usual. Service levels (especially for voice-based IT services and "sanitized" data-based delivery) have suffered, with service providers being unable to maintain pre-pandemic service levels.

Customers and providers have been very measured and mature in their reactions to these disruptions; with providers offering their best efforts to continue services, and customers (largely) accepting that there may inevitably be a fall in service levels and working with providers to determine what leeway their contracts allow for. This has surprisingly meant that there have not been too many force majeure calls being made in large contracts.

The big issue that now faces both customers and providers is, if the lockdown is in any form extended beyond May 3, 2020, will this stop-gap fix continue to work? How long can BCPs sustain? How long will customers be able to live with reduced service levels? Is the "new normal" business model going to be based on WFH and, if yes, what is the impact on services being provided to regulated entities?

This also raises some very critical questions on the security aspects of the "new normal" business model, particularly for regulated entities in the US (amongst other jurisdictions).

What security risks are we talking about?

Indian outsourcing services typically come packaged in a "sanitized" delivery model. This means isolated and dedicated networks for storage, computing resources and service delivery, dedicated IT terminals, network security applications, automatic failover and load balancing and uninterruptible power supply, amongst other features. Delivery centres are almost like digital fortresses that are manned by highly specialized IT and IT security technicians on a 24/7 basis, thus ensuring service security.

The transition of the service provider's workforce to a WFH model means that, from a security perspective, the digital fortress model doesn't work anymore. Each employee operates in an environment

that sits outside the fortress with less robust data security controls, increased use of personal devices, lack of reliable power supply and limitations on communications infrastructure. The WFH model also raises a number of new challenges linked to dependency on digital infrastructure such as constraints on bandwidth, back up and reliance on remote access technology, which the workforce may not be familiar using. The result is increased vulnerability to cyber threats.

What should service providers and customers do?

If the lock down persists and WFH or remote working becomes the new business model, providers and customers may have to fundamentally change their security blueprint and protocols. In such a scenario, be prepared to transition quickly from relying on digital fortresses to converting each employee's workplace at home into a "bunker", security-wise. Series of bunkers will also need to be closely interlinked to a remote monitoring and crisis response centre. This will require a number of measures, some of which are highlighted below:

1. Create a heat map identifying "zones" based on criticality. For instance, the prioritised "red zone" at the top would include domain and system access providers with elevated privileges, those handling business critical or sensitive personal data etc. Identify and target these users as top priority for secured access and for rolling out pilot incident response drills, daily communication etc. Gradually roll these implementation plans down the amber and green zones.
2. Ensure laptops / servers deployed for remote working have key security controls including MFA, encryption, data loss prevention, automated backup solutions etc. Determine sufficiency of network capability to support the required scale of WFH.
3. Sensitize employees to be extra vigilant in reporting potential threats to the organization. Ensure employees have access to designated phone lines and web links to enable effective reporting and monitor these lines to identify complaints from employees about processes, controls or technology limitations that are hindering access or productivity. Preserve logs and analyse these for anomalous activity.
4. Establish a QRT to manage all incidents of breach and ensure that a senior level manager is heading this QRT. If and when an incident is reported, activate the QRT, empower them to take quick decisions and take immediate mitigation measures within the first 24/48 hours of the incident (the golden hours).
5. Ensure the Board, regulators and customers (where required) are kept updated at the "right" time, but don't under or over report. Instruct lawyers to establish privilege and bring in third party independent advice to protect the Board and managers in terms of management and reporting. Plan for investigation (involving external and internal resources) with minimal disruption to the already disrupted operations.
6. Redesign your cyber audits, security infrastructure and cyber risk insurance coverage to deal with remote working or the "bunker" model.

How will regulators react?

Recent guidance released by a number of regulators is indicative of their concern over what measures regulated entities and their third party service providers are taking to deal with the new business exigencies, whether services will be affected and, if yes, how. Therefore, information flow is key. Regulated entities and their providers should communicate, and do so effectively, with regulators. If they are able to demonstrate that they have put in "best efforts" and that there have been no breaches, this should satisfy regulators in the short term.

However, and very soon, new security models/programs demonstrating “bunker” cyber protection will be requested by regulators, and one has to be ready with this revised model.

Irrespective of the above, regulators always look at how, and how quickly, regulated businesses/providers reacted when a cyber breach was reported, and this is where the WFH/remote working model may prove deficient. Providers have to really drill down the criticality of reporting requirements and also ensure that employees are trained to spot potential and actual cyber breaches. They then have to install senior-level cyber breach response units to deal with these incidents promptly and effectively.

BTG maintains all material on the ongoing COVID-19 crisis and legal implications here. Please click to access.