Synergy

Partners in delivering value

Covid: Day 180 & beyond

Operational impacts - A study

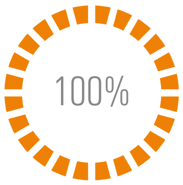
The Coronavirus pandemic has brought about ambiguities and uncertainties, which many businesses and existing team structures weren't prepared to handle. The pandemic has caught the entire world unawares, forcing businesses and industries to make arrangements for their employees to work from home. This arrangement has, for obvious reasons, hasn't been the easiest for IT professionals. As people continue to desire for a 'return to normal', we believe that work from home arrangement is here to stay and will be more of a permanent change. This implies that a lot of big and small structural changes will have to be brought about in larger organizations to get the wheels rolling.

Synergy conducted a survey, where CIOs and CTOs from various financial services institutions shared their views on how they plan to tackle apprehensions and formulate new plans. We identified 5 key focus areas in which many companies have faced struggles during remote working implementation - Infrastructure changes, Customer centricity, Training and awareness, Cybersecurity and Process Automation.

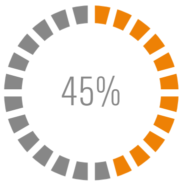
01 Infrastructure at doorstep

Infrastructure & applications had to be exposed for users to connect remotely. This meant that VPN and firewall changes will be the key. Organizations had to take a few crucial decisions on changing their firewall and VPN configurations to get their employees to access their applications and network seamlessly while working from home. IT service continuity, Business Continuity and the Security team had to reaffirm the standards as there was little or no time to investigate and plan the activity.

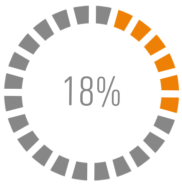
The survey, we conducted, showed there were significant actions taken by organizations to make sure work-from-home was a trouble-free arrangement for their employees. However, on the other end, security had become a major area of concern in this scenario. If not for effective and consistent monitoring, this change could prove to be catastrophic and an easy access for hackers.



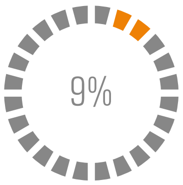
All of the survey respondents confirmed that they had to alter their VPN capacity to cater to work form home needs



A staggering 45% of the respondents said they had to make **significant changes in their firewall setting** in order allow employees to work from home



18% of the executives responded that they allowed **employees to access office emails directly without any MDM** (Mobile Device Management)

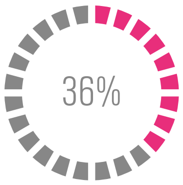


Though **9%** looks low, it is important to note that companies have allowed critical users without any restrictions

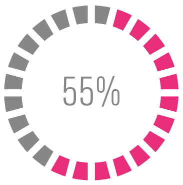
02 Customer Centricity in the new normal

Customer-centricity has long been one of the key facets of any organization, which is why front-office functions had become quite a challenge during this pandemic. Consumers were facing a similar lockdown situation too and could not visit front-desks. Hence, there was a significant rise in customer call volumes to contact customer support. Voice, email and chat-support were more significant than ever to address customer needs.

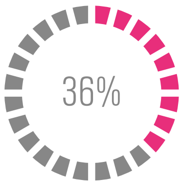
In any IT service continuity or business continuity management, usually front- desks are always planned with options for offsite or off-city location. This pandemic has revealed a challenge to both IT teams and business continuity teams in managing the situation. In specific to End-point setup, our survey shows the actions taken by companies to address their critical front-office functions.



36% of the respondents confirmed that they implemented a **separate voice infrastructure change** to manage call center / front office users



55% of the respondents confirmed that they **provided Authenticated Terminals for end users** to connect only to company applications and infrastructure.

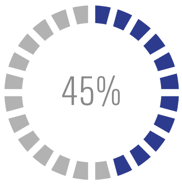


36% of the respondents confirmed that they implemented a **separate cloud based chatbots as an alternative** for call center / front office users

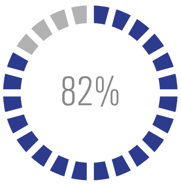
03 Remote working training

With an on-going work from home situation and no end in sight, another challenge faced by companies was to provide the right guidance and creating awareness on "Dos and Don'ts" for all the employees. This was a new way of working for the employees and the right direction was essential to keep them going.

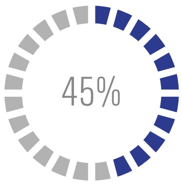
The survey we conducted showed that maximum efforts and focus was channelled towards regular communication and timely interactions between executives and team members. Only around 45% of the respondents said that they had SOPs in place (Standard Operating Procedures), which is one of the basic requirements from an IT or Security process standards point of view.



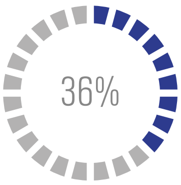
Surprisingly **only 45% of the respondents** confirmed they are conducting training regularly on usage and connectivity from working from home.



82% of the respondents said they have been sending regular guidance and have increased communications over email to all staff working from home



Only **45%** companies responded that they have SOPs even though this is one of the basic requirements for standard IT Operating companies



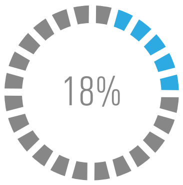
36% of the respondent mentioned that they have **established internal cohorts** to share best practices and insights

04 Cyber threat - outside everyone's door

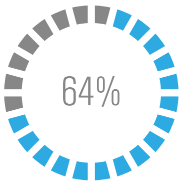
Cybersecurity is another most widely talked C-word after Covid-19 since this pandemic. Traditional security measures will not protect a fully remote staff from cyber-attacks. The need of the hour is to rethink our approach to cybersecurity. Organizations of all sizes must implement business-contingency plans that prioritize protecting their remote workforce from such attacks.

Many organizations inspect systems and data manually for the evidence of unexpected behaviour and indicators of a breach/compromise or defect. However, in a modern organization, this is a losing proposition. Increasing organizational complexity can be a hindrance if cybersecurity is not sufficiently scaled to effectively manage the changing environment by properly diagnosing, monitoring and responding to threats.

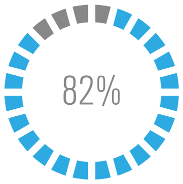
We asked our respondents, which Cybersecurity tasks do they feel their company will focus heavily on in future given that this arrangement of work from home will continue beyond the pandemic situation or may even become permanent.



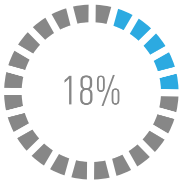
Only (a shocking) 18% of the respondents confirmed **they have a proper SOC** (Security Operation Center) **in place and will be further strengthening** to cater to the security monitoring needs.



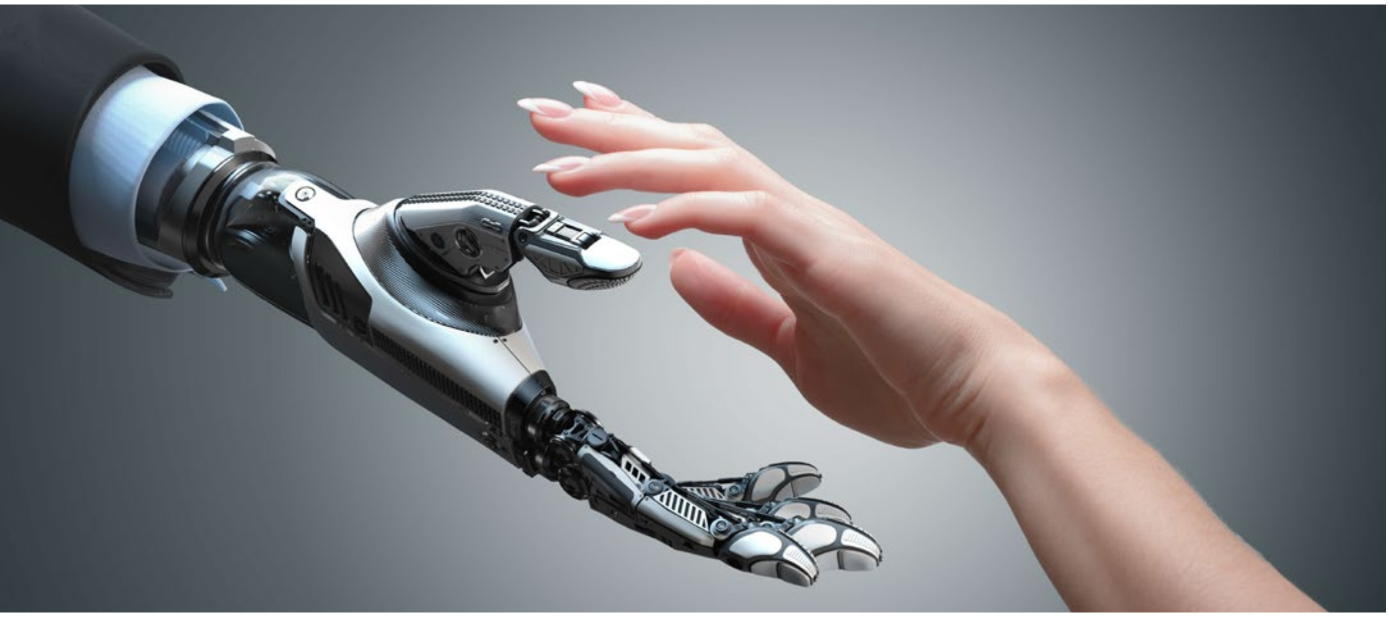
64% of the respondents showed an intent of increasing the event and log monitoring and will probably have to invest in a proper SOC (Security Operation Center).



82% of the respondents would like to continue imparting security awareness to all employees with regular communication & sending security awareness flyers



18% of the respondents said **additional and enhanced firewall rules** to be in place to control any unwanted intrusions. **Remaining 82% still have concerns implementing stricter firewall rules** as it could hamper work from home situation.

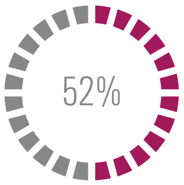


05 Automation is imminent

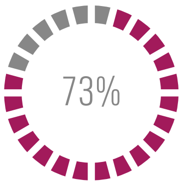
Robotic Process Automation (RPA) is another key area that has gained significant prominence. The sudden shift in workplace dynamics has severely impacted organizations who were traditionally banking heavily on manual processes. This has acted as a catalyst for organizations to turn to RPA as a long-term transition enabler.

Organizations that had already embarked on RPA journey are now focusing on enhancing the scope of RPA implementation. Now, they are focusing on the integration of AI/ML to move towards Intelligent RPA. Few organizations are testing waters with RPA, focusing on areas that can earn them quick-wins.

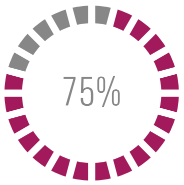
Our survey gives a clear direction, where a majority of respondents showed a keen inclination towards wider adaption of RPA in their organization moving forward.



52% of the respondents had already started some RPA initiatives and are looking to increase the RPA adaption in their organization.



73% of the respondents believe that digital workers would constitute at least half of the overall workforce in the post-Covid world.



75% of the respondents agree that Intelligent bots with AI integration would benefit their customer facing teams while working remotely.

Conclusion

The way the pandemic is imposing a stranglehold on the world, it is unlikely to see companies operating at 100% strength anytime soon. The guidelines suggest, to begin with around 10% or 25%, and gradually increase the strength if the situation improves. The task to bring, even a smaller percentage of workers, back into healthy workplaces is a monumental endeavour. We must consider factors such as the physical space, the trepidations of workers, new sanitation requirements, and healthy work practices — and additional costs — all at a time when the finance and resources are stretched beyond a limit.

While this report discusses specific steps for an organization to take in this work from home situation — all organizations will need to make substantiative changes to maintain the standards and also how they can plan the return-to-work, though it looks bleak in 2020, at least in some countries.

One thing is for sure, no matter the type of industry or working pattern (either from Home or Office), post-COVID-19 work situation is not going to be the same as what it was until now.

About Synergy Strategic Solutions

Synergy is a management consulting & technology solutions company with specialised focus on the Insurance sector. Synergy provides a broad range of professional services covering advisory, smart solutioning, digital & cybersecurity for the Insurance retails lines. By combining business and technical expertise, Synergy is headquartered in Hong Kong, Synergy has operations across Singapore, Malaysia and India.

Research demographics and approach

The study covered a focus group of 50 respondents from within the Insurance industry spread across Asia, some of whom have group headquarters located out of Europe & USA. The survey fielded from March through August 2020 helped to identify the initial impacts and slow transition of priorities in handling the Covid-situation.

Demographic details of respondents:

Industries:

Health, Life and Property & Casualty Insurance

Markets they operate in:

India, Hong Kong, Singapore, Malaysia, Indonesia, few HQs in Europe

Roles:

Chief Information Officer, Chief Operating Officer, Director of Technology,
Chief Information Security Officer, Director of Operations, Chief Technology Officer,
Chief Security Officer