Considerations for a secure remote working environment

Ever since the COVID-19 outbreak was declared a pandemic by the World Health Organization (WHO), there have been widespread concerns about the continuity of business operations worldwide as more countries are declaring lockdowns and advising people to practice social distancing. Business leaders need to plan for agile workspaces and workforces that can function remotely.

Knowing about the current technology and security limitations of the current work environment and planning for future remote working needs can help an organisation ensure business continuity and minimise disruption.

Here are 8 key considerations for building an agile and secure workspace

01 | Who will work remotely?

The first step an organisation should take towards building an agile workspace is to identify which functions can work remotely to ensure business continuity. It is important to estimate the number of employees who need to work remotely and the infrastructure needed to support them. Organisations also need to ensure that while working remotely, employees are thoroughly aware about:

- secure practices (these should be reiterated through frequent email communications)
- contact details of information technology (IT) and information systems (IS) teams to seek advice relating to suspicious emails, calls and messages.

02 | IT and security tools

Internet connectivity imperative for all tools needed for collaboration, communication, task assignment and reporting while working remotely. When a large number of employees are working remotely, an IT or a cyber security incident can have a catastrophic impact on an organisation. A crisis management team may also need to work virtually. Employees who need to work remotely must be equipped with proper resources such as a virtual private network (VPN) to access company resources securely, appropriate tools for collaboration on a laptop/desktop/mobile device, communication resources (access to emails, video conferencing using voice over internet protocol), and appropriate tools for tracking and reporting the work done.

pwc

03 | IT and cyber security governance

The IT and cyber security policies of an organisation should be similar for both remote and onsite work. A central repository of critical process documentation should be made available remotely. Organisations should consider how threat vectors change with the introduction of different work environments, including the shift of employees to remote workspaces which requires changes in access management processes and policies.

Operating remotely requires devices to be used in multiple locations, including an employee's residence, conferences, during travel and at coffee shops. The mobile nature of devices exposes the data they contain to theft or loss. Therefore, it becomes extremely critical to have in place stringent security policies, email security measures, measures to ward off attacks at the entry points of the secure network and secure email gateways when employees work remotely.

04 | Hardware and data centres

Employees who need to work remotely will need a computing device (laptop, desktop, handheld device) and it may not always be possible for organisations to provide one. In such cases, organisations can assess whether it is acceptable for their employees to use personal devices for company work. The security of the systems accessing a company's resources needs to be given special attention.

An organisation should also ensure that all its data centres are equipped with live/hot network failover to accommodate business continuity challenges that might arise during a crisis. The security infrastructure should be robust and scalable within a short time to meet rapidly evolving requirements. If an organisation relies on the support of a managed services IT partner, it is important to ensure that they are adequately staffed to address the change in the volume and nature of IT support requests in a scenario where large number of employees are working remotely.

05 | Software and licensing

Creating an agile workspace needs appropriate software along with the right hardware. Agile workspaces need software solutions that allow organisations to help their employees in remote working conditions. It is important that organisations consider the following while selecting the necessary software and hardware:

- Which type of solutions (traditional or cloud-based) are the best and most secure for an organisation?
- Which programs and systems are necessary for its daily business operations?
- How will employees access these systems from home?

Most cloud-based services allow users to log in from any computer, but traditional software needs to be installed on individual devices.

06 | Bandwidth sizing and data backup

If thousands of employees access a company's servers remotely, will the servers be able to withstand the load productively? One of the key aspects of working remotely is to ensure that the internet service provider (ISP) and the VPN solution have sufficient bandwidth (both downstream and upstream) to handle such situations. Planning for a peak-load scenario helps in understanding how the IT infrastructure handles unusual and unplanned events.

Adequate bandwidth to support high network traffic from a VPN helps in preventing inadvertent denial-of-service (DoS) cyberattacks. At the same time, continuously monitoring the actions of employees over a VPN is of utmost importance for identifying unusual or suspicious activities.

07 | Cyber security considerations

People become more vulnerable to cyberattacks as they spend more time online. Below are a few examples of possible modus operandi by hackers during the ongoing crisis:

- Hackers may design phishing attacks themed on the COVID-19 outbreak to exfiltrate key/sensitive information.
- Hackers may target critical systems in use by the government and medical agencies engaged in combating the COVID-19 pandemic.

While many employees access various services and applications remotely, only authorised users should be granted access to relevant resources. Multifactor authentication and adaptive/risk-based authentication can help prevent the threat of unauthorised access. Identity management solutions should be updated to allow for user access provisioning, deprovisioning policies and the enabling of technology aligned to a remote working model.

08 | How to work remotely?

Apart from having in place adequate IT infrastructure and security requirements, it is important that organisations train users in the nuances of remote working to enable them to understand and adopt these practices effectively. It is a good idea to use the day in the life of (DILO) a user template to make remote working simple and self-explanatory.

The current pandemic will certainly make us think of a new normal. Organisations can turn this crisis into an opportunity to create agile workspaces by incorporating agile practices into their daily work.

Contact us

Gagan Puri
Leader, Forensic Services
PwC India
Mobile: +91 98187 56955
gagan.puri@pwc.com

Vishal Narula
Leader, Crisis Management
PwC India
Mobile: +91 97698 76426
vishal.narula@pwc.com

Abhijit Majumdar
Partner and Leader, Technology Strategy Consulting
PwC India
Mobile: +91 9819854482
abhijit.majumdar@pwc.com

Siddharth Vishwanath
Partner and Leader, Cyber Security
PwC India
Mobile: +91 91 6719 0944
siddharth.vishwanath@pwc.com

pwc.in

AW/March2020-5331