Protecting Your Remote Workers' Data

REMOTE DATA PROTECTION PRACTICES TAKE CLARITY, CONTROL AND COLLABORATION

Remote working has been on an upward trajectory since 2005[1] but it wasn't until the COVID-19 crisis that the practice essentially moved from 'optional' to survival. Even as recently as 2018, Global Workplace Analytics estimated only 3.6% of the U.S. employee workforce (5 million) were currently working-at-home half-time or more. A new survey just released by the Conference Board[2] shows a significant change. A year from now, 77% of organizations expect at least a quarter of their workforce to be working from home at least three days a week.

The impact of this unprecedented shift will be felt in everything from fuel supplies to food delivery. It will also prompt a more permanent transition for IT and security teams who now face the challenge of properly protecting and securing remote devices and the data they generate. Add to this the trend of BYOD and employees using rogue devices outside the protected network and the evidence is clear: organizations need an actionable game plan for not only protecting remote workers' data but creating a long-term strategy to manage and organize the new work-from-home generation.

[1] Global Workplace Analytics, Latest Work-at0Home/Telecommuting/Mobile Work/Remote Work Statistics
[2] The Conference Board, From Immediate Response to Planning for the Reimagined Workplace

ipm SUCCESS BRIEF

IPM consolidated disparate storage solutions for a leading **State University**, providing a central repository for file shares, home directories and archives.

CLARITY, CONTROL AND COLLABORATION

Employees have responded favorably to remote working – flexible schedules, more family time and less tedious commuting are just some of the advantages. Still, remote working is not the Wild West. For organizations to fulfill their business goals and ensure data security and compliance, these essential dynamics must be smoothly functioning:

- **Clarity:** Particularly for employees embracing remote working for the first time, they need clear direction from HR, IT and their managers on what is expected in terms of device protection, in reporting any possible breach threats and in daily practices to support data security.
- **Control:** In terms of data security, the over-arching objective of management must be executing all necessary device and application controls to prevent threats without limiting employee productivity or inviting frustration via lack of help desk response when security questions arise.
- **Collaboration:** Remote working can present challenges for the basic reason that employees are unable to experience the day-to-day personal interaction in meeting rooms, break rooms, the company gym or the local lunch bistro. Fostering a sense of 'oneness' becomes vital and is a part of encouraging employees to follow data protection protocols. HR executives interviewed by the Conference Board list employee engagement and experience as one of the top five focal points in the post-COVID remote work environment.

REMOTE DATA PROTECTION PRACTICE IMPROVEMENTS

Technology requirements and data security are in the top tier of concerns[3] managers have about implementing a remote work policy for the long term. IT teams, along with expertise from a consultant experienced in security and data protection, can implement and/or improve these practices to ensure that the remote workforce can function productively in a secure data environment:

Reduced employee productivity is a major concern for 82% of managers of remote teams.

World Economic Forum

- **Updated Protection Policies.** Remote workers will be putting more demand on using the cloud for data workloads. It is imperative organizations update their cloud security protocols to accommodate this increase. Experienced IT consultants will advise that an updated protection policy needs to include application and access controls, prioritization of data importance in the event data recovery from the cloud is needed, and full knowledge of the lifecycle of applications. Unsupported/unpatched software in the corporate network is a ripe opportunity for a cyberattack and resultant data breach.
- **Enabling Self-Service Data Access.** Once an updated privilege management and application control policy is in place, organizations can implement an automated self-service platform. Turn to the experienced guidance of end user computing expert consultants to make self-service the most effective for your users. This will give remote workers flexibility and support productivity by not having to go to a manager or help desk for access. Reduced employee productivity[4] is a major concern for 82% of managers of remote teams. Streamlined data access can help alleviate this concern.
- **Protecting Popular Applications.** Microsoft 365 including OneDrive, SharePoint, Teams and Outlook; Zoom and other popular applications are an important part of remote work and collaboration. Microsoft Teams[5] on March 31st saw a new daily

[3,4] World Economic Forum, "6 charts that show what employers and employees really thing about remote working"
[5] Microsoft 365, "Remote work trend report: meetings"

record of 2.7 billion meeting minutes. It's a stunning number and reinforces the need to ensure these applications and the data sharing that occurs are protected by all appropriate access and data privacy controls. Additionally, it would be smart to develop and distribute any data protection and privacy plan you put into place. With an unprecedented number of employees relying on video conferencing, IT also needs policy controls on using Zoom or Teams. Microsoft offers built-in controls[6] that everyone should be aware of and use as further data protection support.

- **Ensuring Compliance and Governance.** Widely used platforms like Microsoft 365 answer the need for cloud-based, collaborative tools that help enable remote worker productivity. However, they are not necessarily set up to provide backup and recovery at the level businesses need when a disruptive event occurs. Also, to comply with GDPR and other privacy regulations, data cannot be retained after a meeting ends, for example. Organizations need to supplement these cloud-based applications with a cloud-aware data protection solution and strategy that will help protect data, prevent risk and simplify compliance. Here the expertise of an IT advisor with compliance and governance experience can deliver valuable insights. This will assure compliance teams have the tools they need to respond to specific data discovery requests via self-service in many cases.
- **Simplifying Administration.** Supporting a hybrid environment of cloud, on prem, remote and onsite workers demands a simplified, manageable approach to protecting data. One solution, which will save IT budget and time, is using a secure digital workspace to bring the management of on-premises, cloud, web, SaaS and mobile apps into a single administrative experience. A unified control plane lets IT manage and secure every element of Microsoft 365, for example, as well as workspace elements such as virtual apps and desktops, from a single place. This greatly improves visibility and simplifies troubleshooting, helping IT get more done, more easily.

Safeguard Your Business without Compromising Productivity

Read how to optimize security and productivity to realize better business outcomes.

Download PDF

A PRODUCTIVE, REMOTE FUTURE

The COVID-19 crisis awakened the sleeping giant of employees realizing that they could work productively at home. With as much as a quarter of employees expected to be more off site than on, it is up to organizations to update data protection controls and administration to support their employees who are now the vanguard of the new generation of remote workers. By applying clarity, control and collaboration you will not only secure and empower productive employees but ensure effective data protection as well.

[6] Microsoft 365, "Our commitment to privacy and security in Microsoft Teams"

IPM is a US-based IT Consulting partner with 35 years' experience planning, deploying and supporting all aspects of IT infrastructure for our customers. We enable customers to transition to the cloud by selecting the right cloud model for their goals. We partner with best of breed technology partners to help organizations collaborate and be more productive, wherever they are working. Security is the cornerstone of all of the solutions we develop with a special focus on highly regulated industries and compliance. With strong partnerships and certification at the highest levels with partners including Microsoft, DellEMC, Citrix, VMware and Amazon, we have the ability to create and deliver secure IT solutions to meet your business needs and project budgets.

ipm

151 W. 30th Street, 8th Floor | New York, NY 10001
646.421.2801 | www.ipm.com | services@ipm.com