

Balancing Cybersecurity and Productivity to Optimize Work-From-Home



During an important video chat sales presentation, an account executive attempts to bring up critical information. But the system denies her access to the file. Frustrated, she limps through without the data. In the current environment, the perfect blend of effective cybersecurity and productivity can prove elusive. But with careful planning, businesses can achieve both goals.

In today's data-driven and work-from-home business environment, organizations need strategies that give the good guys ready access to data while keeping the bad guys out. Several factors make finding that balance a challenge.

First, to work productively, employees need quick access to quality data. This often requires sharing data between departments. Additionally, decision makers frequently need to access data remotely.

Second, in recent months, the work-from-home trend took a huge leap forward. In the race to implement remote work without damaging productivity, many organizations opted to relax security policies. To compound the problem, when employees run into roadblocks, they often circumvent IT by using unsanctioned apps to share information.

Consequently, businesses face a dilemma. They must find ways to empower employees, both in the office and out, while still protecting data assets. When organizations integrate cybersecurity with business processes, implement a data safety net, update security practices, and educate employees, everyone wins.



Simplify Cybersecurity

When employees view data security as an obstacle, they look for ways around it. However, when companies prioritize user experience and make security easy, employee productivity improves.

For example, when employees must remember login credentials for dozens of applications, they tend to use weak or redundant passwords. A password manager makes it simple for workers to use strong passwords. This saves time spent searching for passwords while increasing data security.

Additionally, to combat the widespread use of unsanctioned apps, survey employees to determine what tools they need. Then provide safe ways for them to use the productivity apps they prefer. A multifaceted collaboration tool like Microsoft Teams, for instance, can increase both cybersecurity and productivity.

Check Your Safety Net

Backups form a critical component of a cybersecurity strategy, paving the way for continued productivity in the event of equipment failure or ransomware. Use World Backup Day (March 31) as an opportunity to ensure [backup best practices](#). Automate backups where possible. Test them regularly. Use encryption. And then store multiple copies of the backup, including off-site.

Update Security Policies to Match Needs

Cybersecurity strategies must keep pace with the evolving work environment. For example, the access policies and security infrastructure that sufficed when most employees worked at the office may not meet the productivity needs of a remote workforce.

In addition, as more employees use personal mobile devices for business, BYOD policies and [mobile device management](#) become indispensable. Take time to review existing security policies and tools. Then, with input from the workers most affected, adjust policies as necessary.



Train Employees

End users play a key role in the success of a cybersecurity strategy. Consequently, businesses need to ensure that users understand cybersecurity best practices. Ongoing [security training](#), targeted to the worker's role and level of access, will produce results. And as workers understand how to use built-in security tools, they will see them as less of a roadblock.

Cybersecurity and Productivity: Partners for Success

As organizations prioritize user experience, aligning security strategies with business needs, employees feel empowered. And when they have the tools they need to work both safely and efficiently, whether in the office or out, productivity increases.

The data security experts at eMazzanti understand the challenge of balancing cybersecurity with productivity. They live that challenge every day, and they have helped businesses of all sizes implement [data security](#) strategies and remote work productivity solutions designed for today's unique environment.