Businesses Have an Opportunity to Maintain Productivity During Coronavirus Crisis with Teleworking

Michael Pelletier, MBA, MSCS

To say that the global outbreak of Coronavirus Disease 19 (COVID-19) has changed the way Americans conduct business, at least for the immediate future, would be a vast understatement. With the unprecedented wave of limited public access, social distancing and workplace restrictions meant to stem the spread of the disease, we have entered a period of adjustment for businesses that we likely haven't seen since the Great Depression and World War II.

Yet during this time, there are opportunities for many companies to adapt on the fly and maintain a solid level of productivity, despite the dramatic shift in how business is conducted for the time being. One way for businesses to do this is to strategically embrace the idea of teleworking, which simply put is having employees shift their operations to a home office during this public health crisis.

There are some businesses that have implemented the practice of teleworking for several years, though it has never been as widespread a business necessity as it is becoming now. Even for those businesses with a longstanding culture of working within the structure of a "traditional" office setting, there is a playbook they can follow to seamlessly integrate teleworking into their overall strategy without missing a beat.

Virtual Private Network—Teleworking begins with a Virtual Private Network, or VPN, a tool that connects remote users (as in people working at home or in remote offices) to a company's private internal network by using the internet for connectivity. With cloud-based technology, VPNs can be relatively simple for a company to establish—providing they have the capacity to make it work company-wide.

While a VPN can provide access to company resources, it may not be enough to enable a "useable" end-user experience. Some legacy applications are not well optimized to run over a VPN and the lack of responsiveness can be frustrating to end-users. Fortunately, there are solutions called Virtual Desktop Infrastructure (VDI) that provide a remote desktop experience. A VDI reduces the amount of bandwidth being consumed, allows the application to run within the secure confines of the business network and provides a more responsive experience for the end-user. Some VDI solutions can be deployed in the cloud providing both a fast deployment time and metered billing so that you only pay for what you need.

Ensuring Productivity—Once a VPN is established and the employees are given the capability to perform their jobs from home, the business then needs to develop a system of monitoring remote users to ensure productivity. This has to be implemented with a sense of balance—the company doesn't want to inject a lack of trust into the process, but it does want to ensure the

appropriate amount of work is getting done from home. Employees and employers can work together to determine what defines productivity for them and what level is expected while teleworking. This is a good starting point.

The next step is to define parameters for the home workspace and set expectations for the work day. Employers should stress that an appropriate space should be established, that proper workplace etiquette is transferred to the home office and that the employees have the right tools—such as access to instant messaging and internal communication chains, headsets and hardware needed to operate properly. The truth of the COVID-19 outbreak is we don't know how long current restrictions on personal interaction and the need for social distancing will take place, so remote workspaces need to be established with an eye on the long-term.

Security—As with every aspect of the modern work environment, proper security is paramount for teleworking, given the persistent threat of cyber security attacks that loom over most businesses. Supporting a telework capability is not open season on tried and true security practices. It is not the time to open up servers/services to outside users by relaxing firewall rules and restrictions. Any changes to your infrastructure to support remote work should include a review of the security approach to ensure you're not increasing potential exposure. It should go without saying that all protocols followed by a company for on-site users—password protections, encryption, alertness to and notification of potential scams and more—should be put in place in the home office as well. In fact, in many circumstances, vigilance needs to be heightened—as not all network traffic on the user's PC is necessarily protected by the corporate firewall. As with all aspects of doing business in the digital age, everything needs to be done with security in mind

Telework has evolved into something much more than simply opening up a laptop at the kitchen table; it truly should be viewed as a direct extension of the main office, with all necessary rules and processes in place. But during a time as extraordinary as this, telework is a vital tool that not only can help businesses stay afloat, but continue to thrive and even grow. It is a new way of thinking for many companies, but it can bring tremendous value and stability during a time of such uncertainty.

Michael Pelletier, MBA, MSCS, is the Chief Innovation Officer for blumshapiro, the largest regional business advisory firm based in New England, with offices in Connecticut, Massachusetts, Rhode Island and Virginia. The firm, with a team of over 500, offers a diversity of services, which include auditing, accounting, tax and business advisory services. blum serves a wide range of privately held companies, government, education and non-profit organizations and provides non-audit services for publicly traded companies. To learn more visit us at blumshapiro.com.