ActivTrak

Preparing for a Pandemic:

How to Ensure Productivity and Security When Employees Must Work From Home

By Rita Selvaggi

The global reach of the coronavirus has elevated the discussion around the need for "social distancing" and working remotely to avoid spreading the infectious virus. Global companies like IBM, Goldman Sachs, and PwC are asking employees to work from home, as are smaller organizations, such as Seattle-based online payment company Stripe.

As organizations consider having employees work from home on a more massive scale, it's important to recognize that doing so also introduces certain risks to the business that must be mitigated. In this article, I'd like to cover three remote workforce-related risks: employee productivity, digital security, and compliance.

Not Every Employee is Productive at Home

A traditional work environment provides employees focus, stimulus, and engagement intended to optimize workplace productivity. So, it's no surprise that some employees simply aren't wired to work by themselves at home; with no co-workers or meetings, and plenty of distractions, the potential for lower productivity at home is significant. According to a study by Buffer, a lack of collaboration, loneliness, and motivation are challenges for those who work remotely.

So, how do you ensure employees deliver office-equivalent productivity levels? A few actions may be necessary:

- **Set the Expectation** – For some employees, setting expectations around working hours and productivity levels may be initially necessary. For instance, establishing that employees should plan to be working normal business hours when at home is a solid starting point. Additionally, hourly employees may need to be informed on how to keep track of their time – whether done manually or via a web-based time card application. Lastly, it makes sense for the organization to communicate what the employee should do when they believe themselves to have become ill.

- **Embrace the Digital Workplace** – Software vendors such as Microsoft and Google have spent years building out cost-effective solutions that allow users to communicate, collaborate, video conference, share documents, and use virtual desktops. When asking employees to work from home, it's important to evaluate how more consistent use of these types of solutions can help preserve productivity and engagement across teams.

- **Gain Visibility into Employee Productivity** – In a traditional office setting it's much easier to tell if an employee is working than when they are 30 miles away at home. But, it still can be a challenge to establish productivity baselines and identify when and where productivity is lost, even if the employee works onsite. Organizations should consider solutions that provide visibility and insight into whether employees are engaged and productive, regardless of their location.

Even if productivity isn't a concern, the organization does take on an added security risk with the introduction of a much broader remote access footprint.

Digital Security Becomes a Bigger Issue

While the vast majority of remote workers want to work from home (84%, according to Buffer), 37% of remote workers would pick a coffee shop as their second choice of work location. As humans, we need to connect, so finding a way to work while feeling a part of the world is still important. Giving employees the flexibility to work in various remote environments may be the key to ensuring productivity, and even retention in some cases.

When employees work outside the safety net of the corporate network, it opens the organization up to devices and WiFi networks that are potentially insecure – as well as users who no longer think they are "at work". This combination of lowered defenses is a perfect storm for cyberattacks that prey on unsuspecting employees. Using social engineering techniques, hackers can trick workers into giving up corporate credentials to online resources, install malware, commit fraud, and more.
Then how do you maintain security while working remotely?
Maintaining appropriate levels of security is a challenge with an anytime/anywhere/any device/any network-type of employee. The good news is there are things you can do, including:

- **Establish Shared Responsibility** – It's important to communicate that the employee has a role in ensuring the ongoing security of the organization's operations, data, and resources. A vigilant mindset is required, as cybercriminals watch industry trends and devise new scams and social engineering methods that continuously adapt to evolving circumstances.

- **Implement Layered Security** – Solutions such as multi-factor authentication (to make certain the person using a logon ID and password is the owner of those credentials), Single Sign-On (to give employees a single web-based portal to access applications securely), device-based antivirus, and email-based scanning (to spot malware-laden attachments and links before they reach the employee's Inbox), are just a few of the ways organizations can protect themselves against remote-work threats.

- **Monitor for Anomalous Behavior** – In a recent Verizon study, 39% of organizations had experienced an attack on mobile devices in the last 12 months. Solutions that provide visibility into employee productivity should have some means of also analyzing user activity to identify suspicious or anomalous behaviors. For example, an employee logging on to a system at 3am (something they never do) may be cause for review to ensure the activity is appropriate

Even if productivity isn't a concern, the organization does take on an added security risk with the introduction of a much broader remote access footprint.

Compliance Requires More Scrutiny

The number of regulations that address issues of data privacy and security continues to grow, from HIPAA and GDPR to the new California Consumer Privacy Act. In each case, these compliance mandates require organizations to ensure security controls around certain types of protected data – and to be able to know when those controls are not upheld.

When users work remotely, organizations expose themselves to an increase in potential compliance breaches from scenarios as simple as a stolen laptop, to more complex phishing scam-turned-data breach, and everything in between.

So, what's the right way to ensure you're compliant?

While security is a moving target, compliance is a bit more like a yes/no checkbox – once you know what's required, it's possible to simply put controls in place that meet the requirement. The basic steps include:

- **Know Your Regulations** – This should be a given. But having an understanding of what regulations your organization is subject to, and experts on your team to help you comply with them, is the starting point.

- **Understand What's Required** – Each regulation has requirements that need some level of subjective interpretation, especially with regard to remote workers. For example, GDPR states that personal data of EU residents must be "processed in a manner that ensures appropriate security of the personal data, " stipulating that organizations need to protect against "...unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures". While pretty general, this directive helps the organization narrow its focus; you can easily identify which employees, applications, data sets, etc. are subject to audit, and put controls, processes, and solutions in place to ensure the security of the regulated data.

- **Review Compliance Controls** – Compliance is about behavior, so it makes sense that the organization needs visibility into the behavior of its employees. Employees who have access to sensitive systems, applications, and data may be subject to activity audits to ensure specific data protection mandates are upheld. Solutions focusing on employee behavior monitoring can provide insight into, and context around, actions performed that either demonstrate compliance or signal a breach.

Keeping Remote Employees - and the Organization - Happy, Productive, and Secure

In the case of a potential pandemic like the coronavirus, the easy part may be the decision to have employees work from home. The real challenge begins as organizations strive to achieve the same levels of efficiency, productivity, and profitability that they do "at work". By considering the real-world implications of working from home through the lens of employee productivity, digital security, and compliance, organizations can set themselves up for success, despite the shift in how the company operates.

About ActivTrak

The ActivTrak platform is a cloud-native workforce productivity and analytics solution that helps companies understand how and what people do at work.

Unlike traditional employee monitoring solutions (that only provide a limited technical view of users), ActivTrak's AI-driven solution identifies unique user behavior insights that connect actions, context, and intent across multiple digital environments. This helps companies maximize productivity, security, and compliance, and make better business decisions rooted in data.

A free version of the award-winning solution can be configured to provide immediate visibility. Set up your FREE ActivTrak Account Now - you'll be up and monitoring in minutes!

CREATE FREE ACCOUNT

G2 CROWD

CAPTERRA

TRUSTPILOT