Increased Cybersecurity Threats May Arise For Gig Economy Companies

Insights
12.05.19

The burgeoning gig economy helps companies attract talent and gain new levels of nimbleness in support of efforts to satisfy customers and gain an edge on the competition. The gig relationship is obviously attractive to many. It gives workers greater flexibility, with meaningful opportunities for those who are entrepreneurially inclined.

Thus, it's no wonder that almost one-third of American adults are now reportedly working in the gig economy. 49% of adults under age 35 are riding the trend, which extends well beyond companies like Uber, Lyft, and Grubhub. Now, even retailers and corporate offices may include a mix of employees and gig workers. While the gig boom is real, its progress is not without growing pains.

Litigation and legislative actions so far have focused primarily upon seeking greater protections for workers. The underlying concerns involve allegations of misclassification, encompassing a desire to guarantee workers access to benefits, minimum wages, overtime pay, the right to self-organize, and certain protections against discrimination that currently apply only to employees. Companies, however, also face new, apparently unanticipated threats. One threat is the fact that these new workplace paradigms can compromise cybersecurity.

Even though data breaches are already far too common, activities of gig workers and their unique relationships with companies can significantly increase the likelihood of a breach.

Why? The reasons lie in the unique, more *flexible* affiliation between companies and gig workers, as compared with the traditional employer-employee relationship. If that same level of flexibility applies to the screening, on-boarding, and training of gig workers, or their use of their personal smartphones and laptop computers, the company's cybersecurity will be far more vulnerable to resulting breaches. Cybersecurity is simply one area in which gig workers must be as carefully-trained and closely-monitored as employees. Data supports this conclusion.

According to a recent survey of Information Technology (IT) professionals, actions by malicious "insiders" and human error emerged as greater cybersecurity threats than those posed by third parties, including hackers. Employees typically have considerable access to and control over a company's information. If gig workers have the same access, that fact demands the same screening, training, auditing, and controls as employees.

Clicking on unsafe emails or links, downloading an unverified file or failing to maintain all current security updates can quickly lead to a data breach. Training and auditing can help reduce those risks – but it needs to be done in such a way as to not transform your independent contractors into employees. You will want to work with your counsel to implement a training program that doesn't veer too far into the employment path.

To the extent that you limit electronic access to information among employees, you must also thoughtfully limit gig workers' access. Since gig workers or contractors may work remotely, it can be easy to overlook threats posed by your external communications with your systems and these workers' use of their own devices, through which they access and store company information.

Connecting to company data bases through public wi-fi or leaving their personal device unattended, even briefly, can devastate your cybersecurity. Information can also be exposed if computer screen is visible to members of the public. In fact, the above-referenced survey revealed that almost half of the IT professions who responded had faced security threats during the past year due to specific devices having been compromised.

Thus, the fundamentally fast-paced, flexible nature of a gig relationship can easily undermine an otherwise sound cybersecurity program. And the foregoing concerns address only human errors or carelessness. They do not address the havoc that a malicious actor can inflict. Thus, it is vital to carefully screen gig workers before permitting them to access sensitive company information.

Finally, besides careful screening and training gig workers, you must periodically verify compliance and audit their cyber systems, to ensure their integrity.

In sum, the rapidly expanding gig economy offers many opportunities to workers, companies, and customers. But with respect to maintaining cybersecurity, you just can't afford to take shortcuts.

Related People

A. Kevin Troutman
Senior Counsel
713.292.5602
Email