SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Program Best Practices > Insider Threat >

Issue Spotlight: Overemployment

The remote work boom that began with the COVID pandemic – and in some sectors, before it – has raised questions about the nature of work, employer and employee expectations, and the potential benefits of a remote workforce.

But businesses haven't been the only ones contemplating how to glean new value from the remote work arrangement. Employees have been looking for new value as well – and many of them have found it in overemployment.

Prior to 2020, the term overemployed simply meant overworked. But in the last few years it's been increasingly used to describe remote employees who work two or more full-time jobs simultaneously. Overemployed workers aren't just doing side hustles or moonlighting gigs, which typically start after regular business hours end. They're collecting full-time pay and benefits for different positions at different organizations at the same time.

The Mercyhurst University Center for Intelligence Research, Analysis, and Training (CIRAT) was recently tasked by the Security Executive Council (SEC) to research and analyze the issues, impacts, and risks posed by fraudulent simultaneous employment. The resulting report found that 37% of the total remote workforce has a second full-time job. For 45% of those people, both the first and second job are remote.

What's more, the report said, fewer than a quarter of overemployed workers work the 80 hours a week that two full-time jobs would be expected to require. Many overemployed workers feel justified in "double dipping" because they have negative views about corporations' commitment to their workforce, especially as inflation rises and the cost of living outpaces pay.

Much of the media conversation around overemployment has revolved around questions of ethics, but security leaders would be wise to consider the trend from another angle: Does it pose a new threat to company assets or associates?

It can be argued that an employee who is willing to lie, even by omission, about having a second full-time job may be willing to dissemble in other ways as well. Employees working two

jobs at the same time may be more motivated and see more opportunity to use one employer's resources and information for the other employer's gain.

Hopefully there are already monitoring and mitigation measures in place to guard against insider theft of sensitive information and assets. If not, now is a good time to communicate to management that this trend represents a new likelihood of compromise that is only going to increase.

Many companies already have non-compete and non-disclosure policies to protect against direct competitors, but overemployment cases don't have to involve direct competitors to present a risk. Security leaders should reach out to HR and Legal professionals to discuss policies that make clear the company's stance on overemployment and intellectual property.

Consider this as well: When employees don't feel obligated or inclined to disclose additional work that could be considered unethical, does this indicate a deeper problem with corporate culture? Are their jobs meaningless to them? Do they feel used, resentful, or burned out?

These expressions can be warning signs of other threats, like workplace violence and other forms of fraud. If it's confirmed that employees are engaging in overemployment, perhaps security should consider the root cause and dig deeper to ensure it isn't masking other risks as well.

The bottom line: Security leaders should consider their organization's workforce carefully -- not only remote workers, but in-office personnel who may be holding down remote jobs for other companies while at the office.

Existing mitigation measures against insider theft, fraud, and workplace violence may need to be revisited, revised, or strengthened. New policies should be considered. And the security leader should ensure that executive management is made aware of this trend so they can factor it into any potential changes to their stance on remote work in the future.

The SEC/CIRAT's full report on overemployment is available to Tier 1 Security Leaders. More about becoming a Tier 1 Security Leader here.

Visit the Security Executive Council web site to view more resources in the Program Best Practices : Insider Threat series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com/

