Teneo®
The Global CEO Advisory Firm

Addressing Increased Insider Threat in this Era of the Great Reshuffle

Teneo Insights
January 2022

Executive Summary

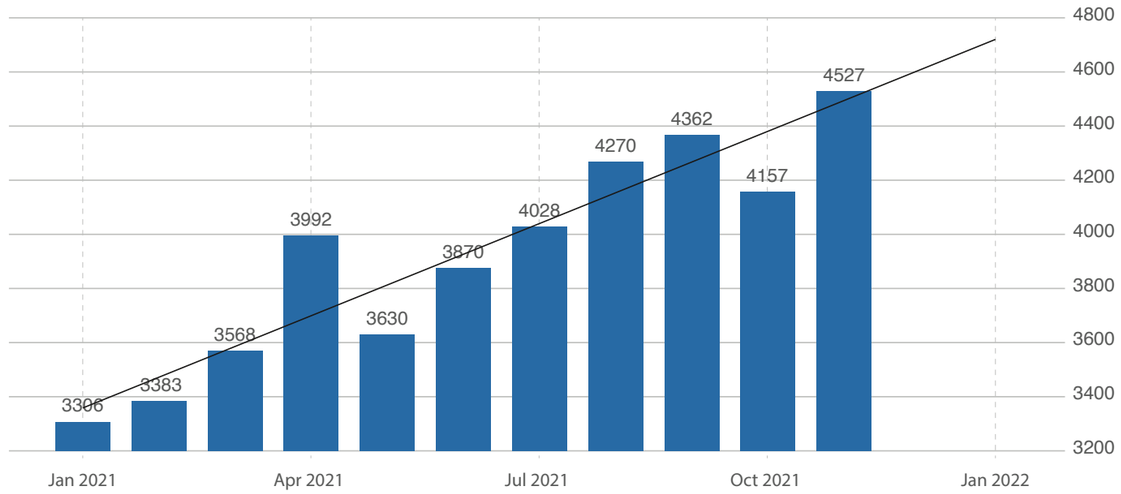
As organizations revisit strategies to manage unprecedented turnover and increased insider threat, Teneo assessed workforce attitudes toward mitigation tactics such as enhanced employee monitoring and surveillance.

A Unique Environment

A peculiar thing happened to the global labor market in 2021. Over a year into the pandemic in the US, the Bureau of Labor Statistics reported record numbers of "quits,"[1] defined as workers who left their jobs voluntarily. As businesses and corporate organizations went through a series of fits and starts with return to work and return to office over the course of 2021, the Bureau recorded an all-time high of 4.5 million quits during November, with lower wage jobs in leisure, hospitality, healthcare, transportation and utilities leading the charge. Yet quits have been happening at all employment levels and across all industries, even including salaried workers.

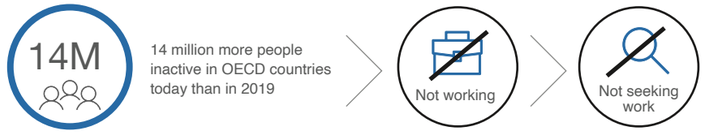
As businesses and corporate organizations went through a series of fits and starts with return to work and return to office over the course of 2021, the Bureau of Labor Statistics recorded an all-time high of 4.5 million quits during November.

"Quits" as reported by the US Bureau of Labor Statistics in millions



Source: TradingEconomics.com / U.S. Bureau of Labor Statistics

Many are out of a job and not looking for a new one



The situation is not unique to the US. The Organization for Economic Cooperation and Development (OECD)[2] reported that across its 38 member countries in 2021, 14 million more people were not working or were not seeking work as compared to 2019.

These employment gaps are wreaking havoc on small and large businesses alike as they experience significant turnover while also trying to retain and attract talent. Dubbed the Great "Reshuffle" or "Resignation" and even the "Big Quit," analysts and economists see no signs of this workforce upheaval slowing in 2022. With more jobs chasing fewer candidates, prospective employees have choice and leverage. They will use that to their advantage as they make more moves from job to job or re-enter the workforce as pandemic fears subside.

Whether people switch jobs for better opportunities, seek a fundamental career or life change or even exit the workforce altogether, all of this "reshuffling" has an impact on employers. These departing employees may introduce risk to the organizations they leave behind. While HR and Ops functions deal with the loss of good talent and grapple with holes in the workforce, security leaders are simultaneously dealing with the potential data leakage or outright IP theft associated with employee turnover. Lest we think this isn't a problem, consider these statistics from Code42's 2020 Data Exposure Report on Insider Threat:

- **59% of departing employees move to a job in the same industry, implying that your company information may land in the hands of the competition;**
- **63% of employees who admit they take data with them upon departure have done it before;**
- **87% of employees report that no one approached them from their prior employer to either prevent or confirm that they did not take data with them;**
- **32% of employees were encouraged by their new employer to share their exfiltrated data and information with their new work colleagues.**

Experts also highlight that employees typically begin exfiltrating company information and other related data about 90 days before departing.

No matter what you call it, we must face the reality that this global phenomenon poses big risk. Insiders have access to proprietary and potentially market moving information ranging from source code, formulas and trade secrets to customer and sales figures, earnings reports, business strategies and deal data.

Dubbed the Great "Reshuffle" or "Resignation" and even the "Big Quit," analysts and economists see no signs of this workforce upheaval slowing in 2022.

[1] TradingEconomics.com, United States Jobs Quits Rate https://tradingeconomics.com/united-states/job-quits-rate#:~:text=Job%20Quits%20Rate%20in%20the%20United%20States%20averaged%201.95%20Percent,Percent%20in%20August%20of%202009

[2] https://www.oecd.org/employment-outlook/

Depending on the nature of the work and the employer, insiders may have a company issued mobile phone, laptop and/or other company device to access corporate information. In today's hybrid work from home, work from office or work in transit operating model, it has become increasingly challenging to keep an eye on who is doing what from where and on which network.

Intermittent in-person attendance at the place of work also limits the ability to see personnel context or early warning signals that an employee may be disgruntled, frustrated or prone to certain behaviors that may introduce risk to the organization – such as intellectual property or data theft. Teneo Senior Managing Director and former Bank of America Chief Security Officer Brian Stephens notes that, "insider risk broadly spans both online and offline threats, from sensitive information to workplace violence to a host of others in between. These complex challenges require an integrated approach and delicate balance of technology and monitoring, behavioral analysis, inter-personal connections and reporting."

Organizations have typically addressed this through monitoring technology focused on employee email, chat and text tools and video surveillance in public workspaces.

In highly regulated industries such as financial services and pharma, or similarly government agencies, employees are already attuned to workplace monitoring practices. However, companies across different sectors recognize that preemptive employee surveillance and monitoring activities are more important than ever and are asking themselves, "how do we do this in today's environment?" "How much is too much?" "How much is too far?" We were interested as well, and this is what we found.

Results Highlight Varying Degrees of Awareness and Expectation

Teneo Research conducted a study of over 1,000 non-CEO, US employees of mid-to-large sized companies across gender, age groups, geographic regions and business sectors to understand attitudes toward employee surveillance and monitoring practices – and to identify how employers should best communicate such policies and practices.

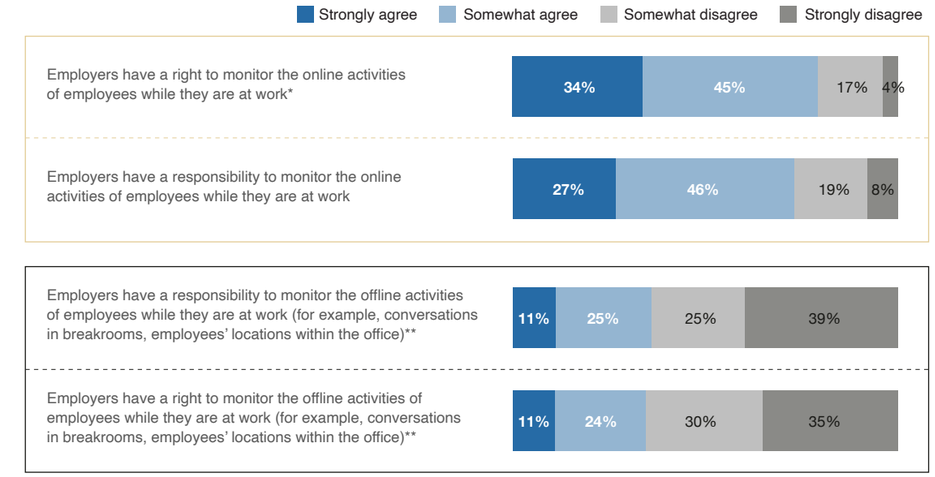
As part of the study, we learned that employees were generally more accepting of monitoring practices within the trusted employee-employer relationship as opposed to the prospect of social media platforms tracking and using data regarding usage, advertising companies tracking online activity or smart speakers listening to conversations.

Regarding online activity in the workplace such as web-browsing, email and chats, employees generally expressed both acceptance of and an expectation that employers were monitoring such activity. Interestingly, the results indicated a low level of concern regarding offline monitoring practices such as location tracking via work issued device, or camera surveillance in the workplace.

However, the results also suggested that this might be the case because employees were not expecting or assuming that this type of surveillance was happening.

As we sought answers regarding "how much is too much," respondents reinforced the acceptability of monitoring online activities while at work, but then drew the line when pressed to consider privacy and monitoring of offline activities at the workplace. Two-thirds of employees said employers have neither the right nor responsibility to monitor offline activities.

- Employees reinforce **acceptability** of **monitoring online activities while at work** with 3-in-4 agreeing employers have a right or responsibility to do so.
- But **draw the line when it comes to their privacy offline**, with two-thirds saying **employers have neither the right nor responsibility to monitor offline** activities.



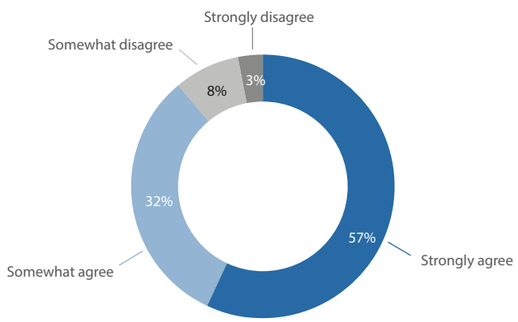
*/**Each pair split among sample: half of respondents saw "right to monitor" and half "responsibility to monitor."

With these insights in mind, we wanted to understand where employers stand on the need to introduce or enhance current practices in light of the workforce dynamics underway and ahead of us in 2022. Our survey results revealed that employers aren't exactly delivering on expectations when it comes to disclosing their monitoring practices today.

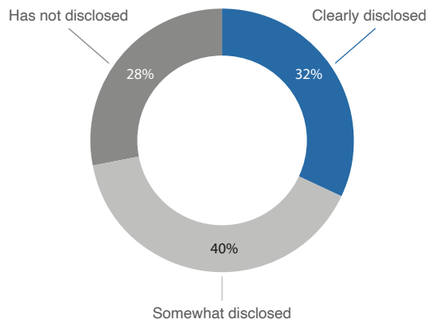
90% of employee respondents believe that employers are responsible for disclosing monitoring and surveillance tactics, but only one-third feel that their employers have done so clearly.

Our survey results revealed that employers aren't exactly delivering on expectations when it comes to disclosing their monitoring practices today.

Do you agree or disagree with the following statement:
"Employers have a responsibility to disclose monitoring activities to employees"



How well has your employer disclosed their employee monitoring practices?



And these expectations hold regardless of whether an employee has been granted a work issued device. 90% of employees with a work issued device and 85% without agree that employers are responsible for clearly disclosing monitoring policies.

Stephens notes that, "these survey results validate that many organizations need to improve upon how and where companies disclose monitoring practices. Too often these disclosures, if they exist, are buried in employee handbooks or annual trainings that cover a variety of other topics. The results also confirm the need to enhance training that amplifies the importance of insider threat identification and mitigation."

While security professionals revisit monitoring and surveillance practices, or contemplate introducing net new strategies, it is important to understand how employees think about insider threat, risks to the organization and acceptable reasons for monitoring and surveillance.

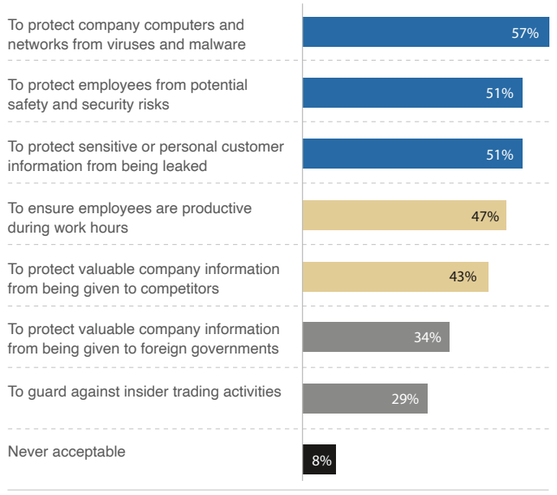
- Roughly 60% of employee respondents expected monitoring practices to be on the rise in the future. It is our estimation that this is due to the preponderance of cyber breaches and the growing awareness of very high-profile ransomware attacks, phishing and other email impersonation incidents impacting global organizations.

- Almost 50% of employees view risks such as computer viruses/malware, employer concern over lack of employee productivity during work hours and potential leaks of personal or customer information as the biggest risks facing their organizations.

- Only 24% of respondents thought valuable information given to competitors posed a significant risk and only 13% believed valuable information landing in the hands of foreign governments was a risk. This could be attributed to employee lack of awareness of just how many people exfiltrate company data upon departure, or perhaps employees don't believe that taking information that they have personally created at the workplace is problematic. Alternatively, employees may think that insiders looking to steal or sell company information to the competition or foreign governments is the stuff of movies or occurs very infrequently.

Employees felt that monitoring activities were acceptable largely for the purposes of protecting company computers and networks from cybersecurity incidents, ensuring employee safety and security and for protection of data leakage of sensitive information like personal or customer data. They did not, however, find protecting company information from making its way to either the competition or to foreign governments as a compelling reason to conduct monitoring activities.

Which, if any, of the following do you feel are acceptable reasons why an employer may need to monitor employee activities? (select all that apply)



80% of workers would consider leaving their jobs if they learned that their employer was monitoring activity in a way that made them uncomfortable.

Our survey results uncovered that transparency and clear communication over incentives were key to fostering employee comfort and compliance with monitoring and surveillance practices. Over 60% of employee respondents expect that if employers are to enhance monitoring activities, they should clearly explain:

- ✓ Which platforms and activites are to be monitored;
- ✓ The rationale for conducting monitoring activities;
- ✓ Behaviors in the workplace that are allowed and those that aren't;
- ✓ Consequences for violating company policies.

As such, failing to offer that kind of transparency is extremely risky for the employer. 80% of workers would consider leaving their jobs if they learned that their employer was monitoring activity in a way that made them uncomfortable.

Millennials and Gen Z expressed particular concern, which could further compound the growing recruitment and retention challenges if disclosures around monitoring aren't communicated in a way that meets expectations.

Roughly 20% of respondents expected some kind of incentive for complying with monitoring practices such as a new device, pay increase or a related bonus, with Millennials and Gen Z having more of an affinity toward such incentives.

Pathways Forward for Organizations Looking to Implement or Strengthen Practices

Our key takeaways suggest that employees are generally aware of and accepting of certain monitoring and surveillance practices in the workplace. Employees even expect practices to continue or become more stringent, which bodes well for those managers and leaders charged with protecting the organization. However, employees made it very clear that transparency is key for acceptance and compliance, and employers risk losing staff or even facing potential reputational blowback if rollout and implementation of monitoring practices isn't handled appropriately.

Our analysis uncovered a clear discrepancy in numbers between the high percentage of employees who admit to taking data with them when departing to an employer in the same industry, versus a low percentage of employees who see that same behavior as a risk. In that regard, we see a significant training and awareness opportunity on the topic of insider threat, and the various forms insider threat takes such as data leakage, outright IP theft and corporate espionage. This training could even be integrated with phishing and other cyber-related issues.

In light of these themes, we offer the following recommendations:

- **Employers should evaluate the degree to which they are currently open and transparent about workplace monitoring practices;**
- **Employers should be deliberate about introducing and communicating relevant details regarding monitoring practices through written documentation such as employee handbooks and policy statements;**
- **Employers should develop an approachable internal campaign on the topic of insider threat and the importance of such campaigns in protection of both the company and employees, including appropriate description of company mitigation tactics such as monitoring;**
- **Employers should reinforce policies through relevant training for staff and potentially even simulation drills for managers and leadership teams;**
- **Employers should provide an outlet for employees to confidentially report issues of concern related to potential data leakage, data theft, etc.**

It is crucial that employers educate their staff on the concept of insider threat and corresponding risks related to issues such as data leakage, IP theft and even corporate espionage. Training and education should include an overview and discussion on the potential financial, operational and reputational impact to organizations if these risks were to become a reality. It should also highlight the role that people, processes and technology have in the mitigation process and protection of the organization. It is our view that such education can help bolster the partnership between employer and employee and helps reinforce a 360° sense of ownership of safety and security outcomes among company stakeholders.

While an exciting time for employees, this great reshuffling may seem like more of a headache for the employers trying to manage it. Despite this, it can also be a great opportunity for business leaders across HR, IT, legal, security and operations to collaborate in strengthening connections with employees and prospective employees on the importance of trust, security and transparency. This can ultimately help employers build a culture that combats insider threat instead of promoting it.

How Teneo Can Help

If any of these issues resonates with you, please contact Teneo's team of situational and sector experts below:

Courtney Adante
President, Security Risk Advisory

courtney.adante@teneo.com

Brian Stephens
Senior Managing Director

brian.stephens@teneo.com

Sarah Meirama
Vice President

sarah.meirama@teneo.com

Teneo®

The Global CEO Advisory Firm

New York address:
280 Park Avenue, 4th Floor
New York, NY 10017