2021 STATE OF WORKFORCE PRIVACY & RISK REPORT

Sponsored by DTEX
Independently conducted by Ponemon Institute LLC
Publication Date: June 2021

DTEX
WORKFORCE CYBER INTELLIGENCE

Ponemon
INSTITUTE

EXECUTIVE SUMMARY

A challenge all organizations face is protecting their business and operations while not infringing on employees' privacy in the workplace. This challenge has only been exacerbated with the shift to hybrid work, as many organizations desire more insight into workforce engagement beyond the office.

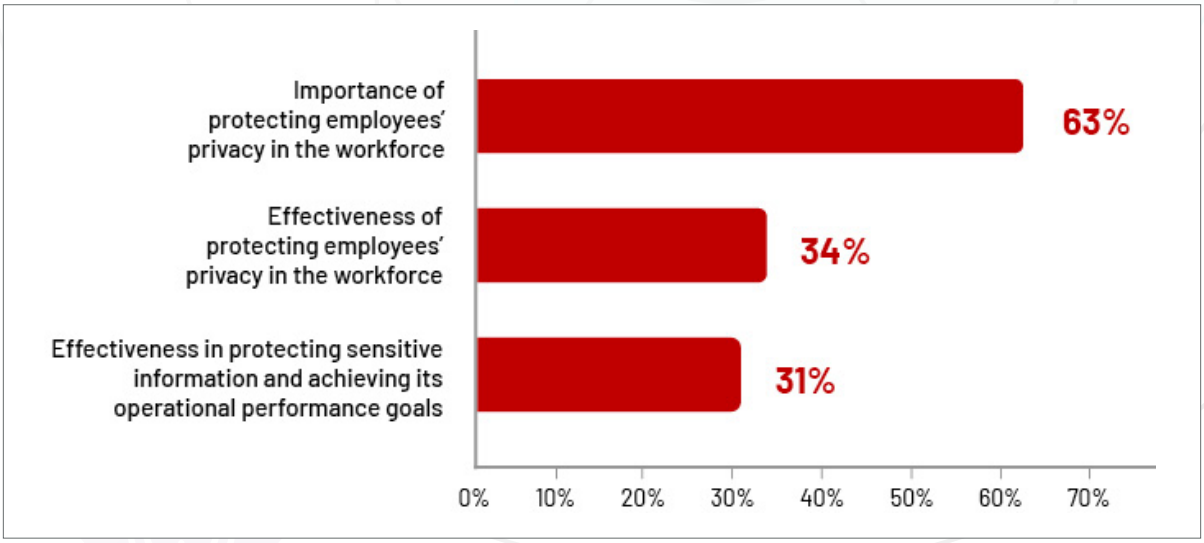
Furthermore, data privacy regulations enacted during the past several years, including the General Data Protection Regulation (GDPR) and California Privacy Rights and Enforcement Act (CPRA), have mandated that companies focus their attention on protecting the privacy of their customers' data. This regulatory wave has not yet addressed employee data privacy.

Against this backdrop, DTEX partnered with the Ponemon Institute to research and issue the first-ever State of Workforce Privacy & Risk report. Based on a comprehensive survey of 1,249 IT and IT security professionals in North America, Western Europe and Australia/New Zealand, the research revealed a significant workforce privacy gap. Employers acknowledge it's critical to protect the sensitive information of their team members and respect employee privacy, but they continue to fall short of these expectations and goals.

Respondents were asked to rate the importance of protecting employees' privacy in the workforce, their organization's effectiveness in protecting employees' privacy, and effectiveness in protecting sensitive information and achieving operational performance on a scale of 1 = not important/not effective to 10 = very important/very effective. Figure 1 shows the most important and very effective responses (7+ on the 10-point scale).

The data shown here clearly illustrates a workforce privacy gap. Sixty-three percent of respondents say it is important or very important to protect employees' privacy in the workforce, but only 34% of respondents say they are effective or very effective in doing so. Furthermore, only 31% of respondents say their organization is effective or very effective in protecting sensitive information while achieving their operational goals.

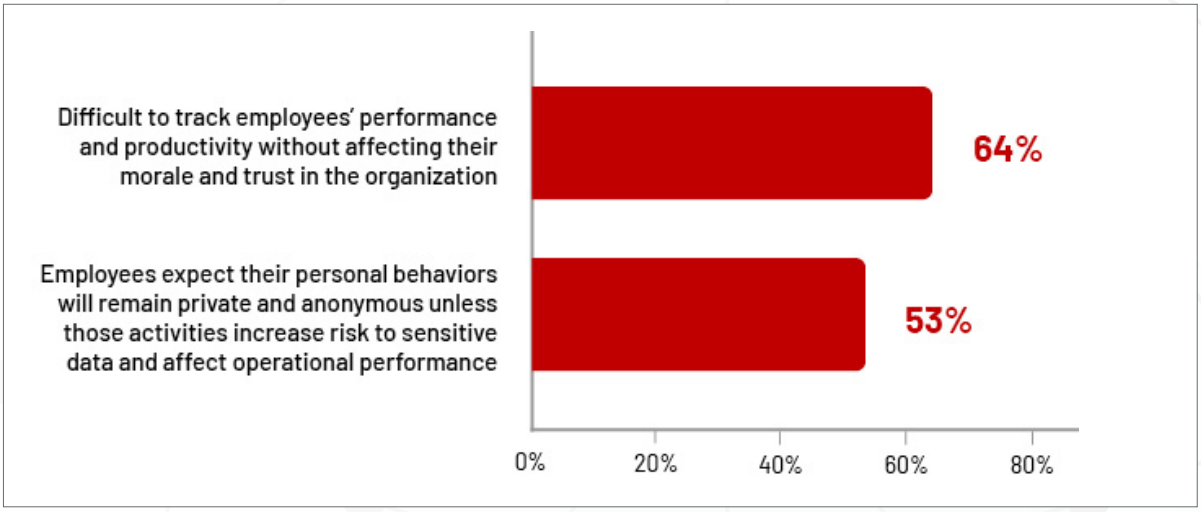
FIGURE 1



WHY A NEW APPROACH TO PRIORITIZING AND PROTECTING WORKFORCE PRIVACY IS REQUIRED

Figure 2 reveals the challenges organizations face when balancing workplace privacy and internal risk. Sixty-four percent of respondents recognize that it is difficult to understand employee engagement without affecting their morale and trust in the organization. More than half (53%) of respondents believe that their employees expect their personal behaviors and activities will remain private and anonymous unless those activities create risk to sensitive data or can decrease the efficacy of operational processes and outcomes.

FIGURE 2. PERCEPTIONS ABOUT PRIVACY IN THE WORKPLACE
STRONGLY AGREE AND AGREE RESPONSES COMBINED.



THE WORKFORCE PRIVACY GAP

The COVID-19 pandemic has changed the workforce privacy landscape. The sudden shift to remote work brought new concerns about employee effectiveness and productivity that led to well-reported increases in the use of workforce monitoring technologies.

At the same time, organizations are paying lip service to protecting workforce privacy, as 63% of 1,249 companies surveyed by the Ponemon Institute and DTEX say it is important or very important to protect employee privacy, but only 34% say they are effective in doing so. This shows a significant workforce privacy gap that companies need to close.

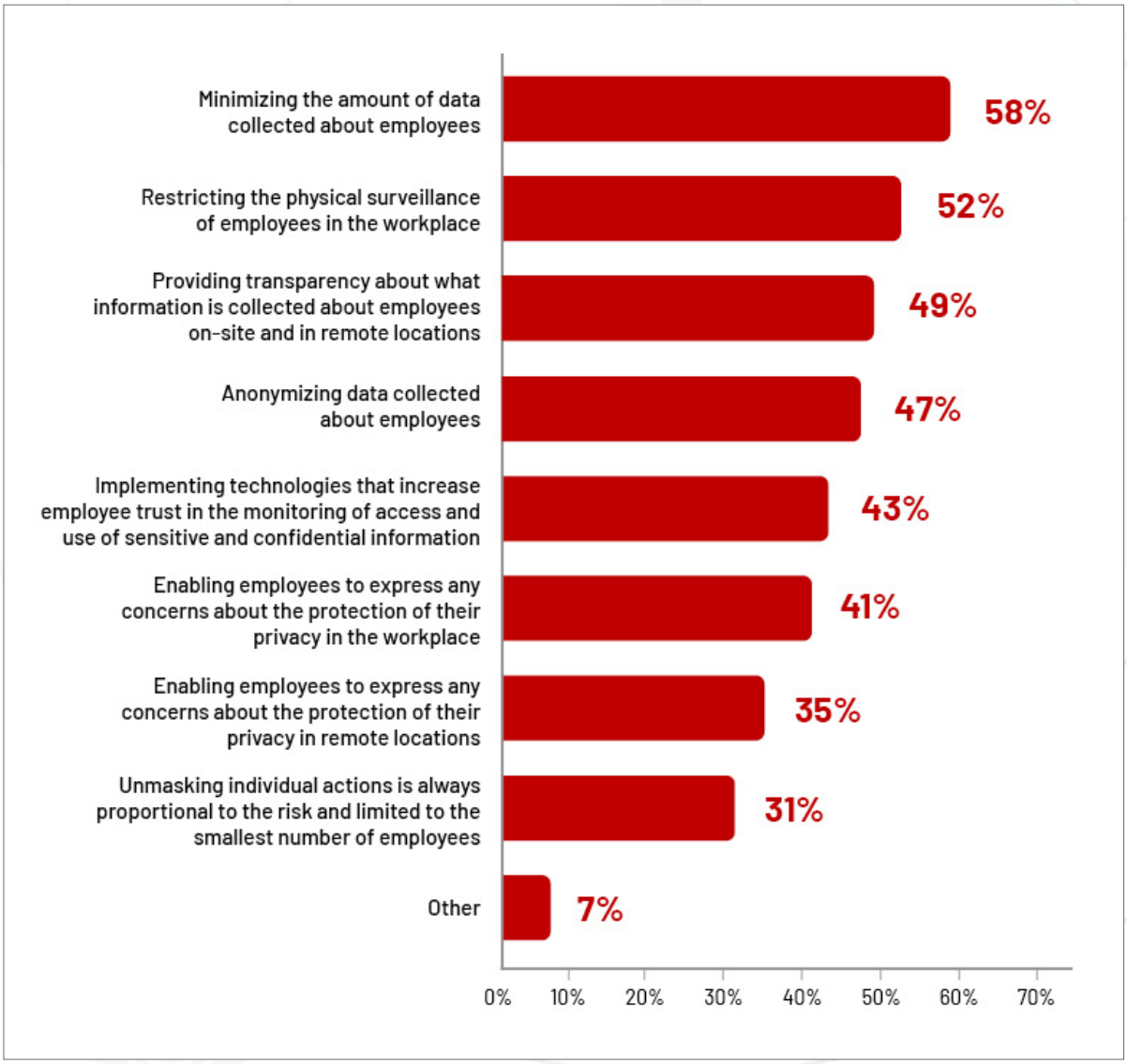
To understand this gap better, we drilled into issues that are at play. One is a disconnect between the expectations of employees about how well their personal information is protected and IT's understanding of these expectations.

MINIMIZING THE AMOUNT OF DATA COLLECTED ABOUT EMPLOYEES IS THE NUMBER-ONE STEP TAKEN TO PROTECT EMPLOYEES' PRIVACY.

According to these results, 58% of respondents say online privacy is being protected by limiting the amount of employee data collected. This is followed by 52% of respondents who say physical privacy is protected by restricting the physical surveillance of employees in the workplace.

Despite the findings mentioned above, respondents then admitted that their organization is not effective in protecting employees' privacy in the workplace. Reasons for this ineffectiveness are presented in Figure 3. Specifically, less than half (47%) of respondents say employee data collection is anonymized and only 43% of respondents say technologies that increase employee trust in the monitoring of access and use of sensitive and confidential information are implemented. There are clear conflicts in what IT security professionals say is happening, and what they admit is being practiced day to day.

FIGURE 3. WHAT STEPS DOES YOUR ORGANIZATION TAKE TO PROTECT EMPLOYEES' PHYSICAL AND ONLINE PRIVACY?
MORE THAN ONE RESPONSE PERMITTED.

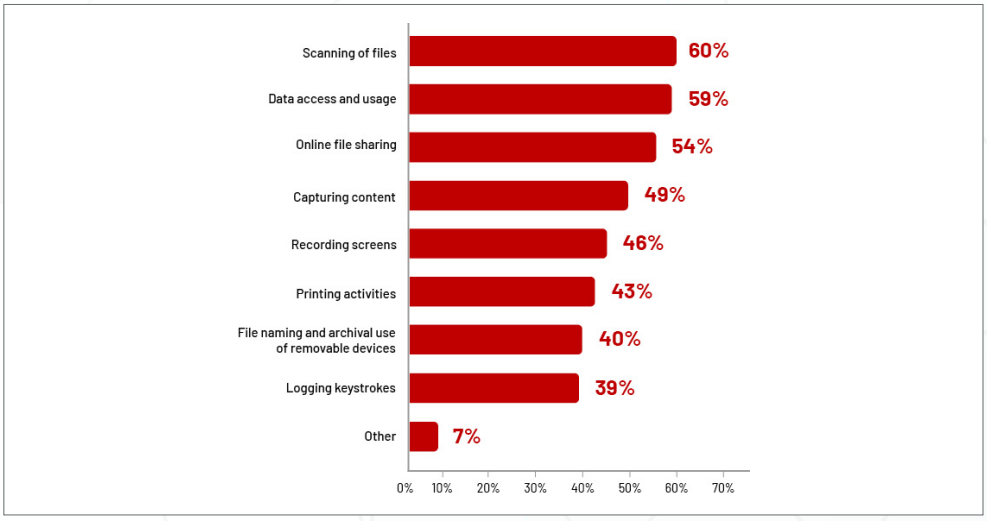


WHEN DRILLING DEEPER INTO HOW EMPLOYERS ARE MONITORING THE WORKFORCE IT IS CLEAR THAT FILE SCANNING TOPS THE MOST COMMON TECHNIQUES (60%).

This is interesting, especially when compared to the fact that just 39% of employees feel their organization's monitoring methods are effective in protecting sensitive information – showing that companies may not be prioritizing the right monitoring strategies.

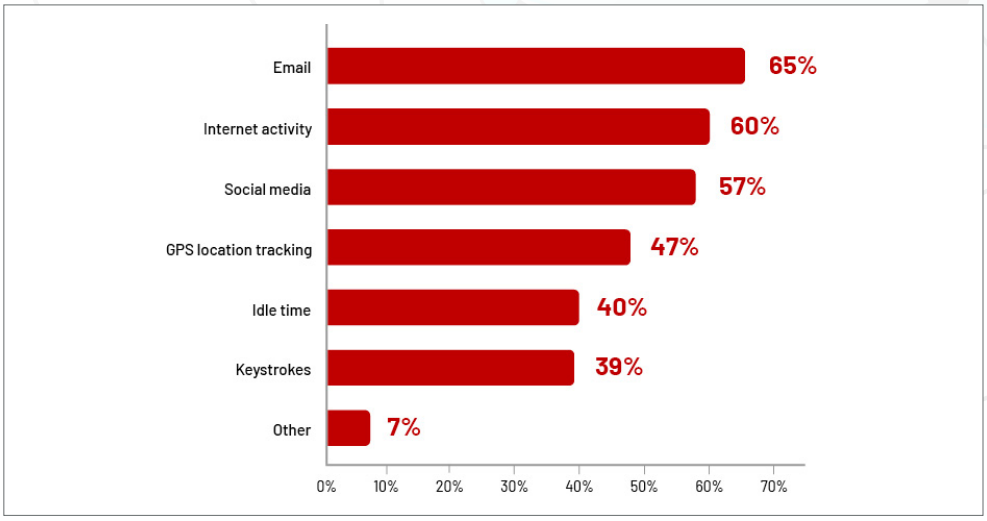
Even though employees know they're being monitored and that organizations are infringing on individuals' privacy, only a little more than half (56%) of respondents say their organization has a formal policy that describes its workforce monitoring practices. Why the lack of transparency and communication?

FIGURE 4. DOES THE MONITORING OF EMPLOYEES INCLUDE ANY OF THE FOLLOWING ACTIVITIES?
MORE THAN ONE RESPONSE PERMITTED.



As shown in Figure 5, emails (65% of respondents), Internet activity (60% of respondents) and social media (57% of respondents) are most often monitored.

FIGURE 5. WHAT DOES YOUR ORGANIZATION MONITOR?
MORE THAN ONE RESPONSE PERMITTED.

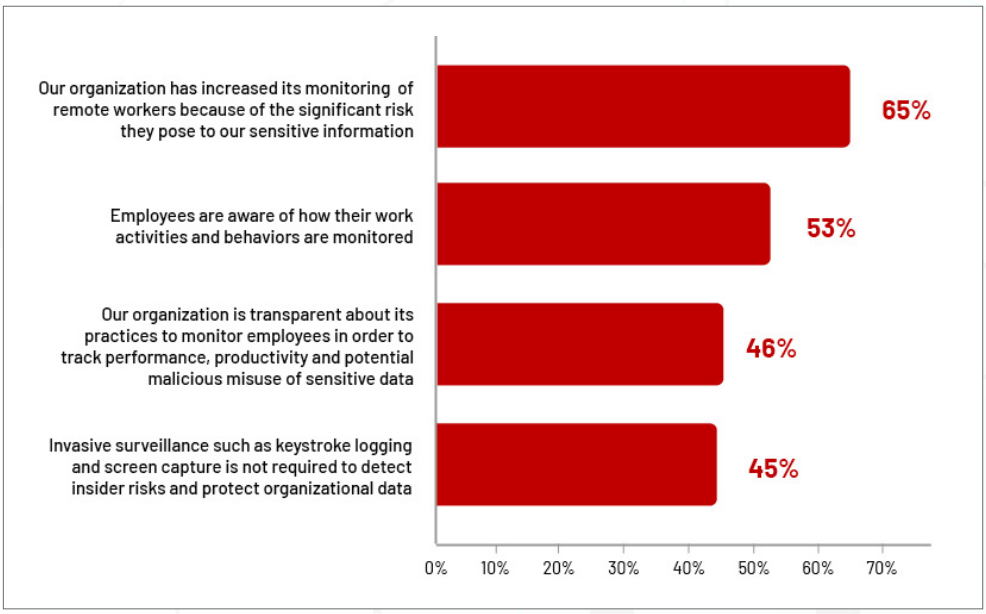


COVID-19 AND REMOTE WORKING HAVE INCREASED THE TRACKING OF EMPLOYEES, WIDENING THE WORKFORCE PRIVACY GAP.

As a result of the COVID-19 pandemic, most employees were required to work remotely. As shown in Figure 6, 65% of respondents say their organization has increased the monitoring of remote workers because of the perceived increase in risk these employees pose to the company's sensitive information.

Still, only slightly more than half of respondents (53%) say their employees are aware of how their work activities and behaviors are monitored. And only 46% of respondents say their organization is transparent about its practices to track performance, productivity and potential misuse of sensitive data, which is in-line given the 56% of organizations that have formal policies in place.

FIGURE 6. PERCEPTIONS IN THE USE OF MONITORING TO REDUCE WORKPLACE RISKS
STRONGLY AGREE AND AGREE RESPONSES COMBINED.

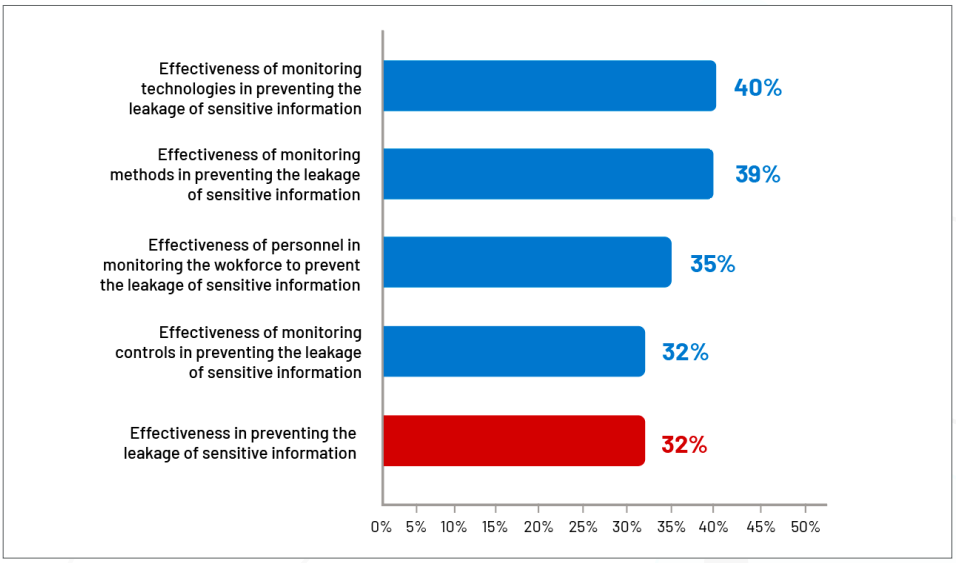


EVEN THOUGH OVER HALF OF ORGANIZATIONS LEVERAGE THESE TYPES OF TECHNOLOGIES, VERY FEW ORGANIZATIONS ARE TRULY EFFECTIVE AT ACHIEVING SENSITIVE DATA PROTECTION.

Not only are the current technologies these organizations are using introducing risk, but the solutions they're deploying are not very effective. Respondents were asked to rate the effectiveness of various monitoring controls and practices on a scale of 1 = not effective to 10 = very effective. Figure 7 presents the 7+ responses (very or highly effective). Only 32% of respondents say their organization is very or highly effective in preventing the leakage of sensitive information, and only 32% say their **monitoring controls** are very or highly effective in preventing the leakage of information. More respondents (40%) say their **monitoring technologies** are very or highly effective in preventing the leakage of sensitive information.

FIGURE 7. EFFECTIVENESS IN MANAGING WORKFORCE RISKS

ON A SCALE FROM 1 = NOT EFFECTIVE TO 10 = VERY EFFECTIVE, 7+ RESPONSES PRESENTED.

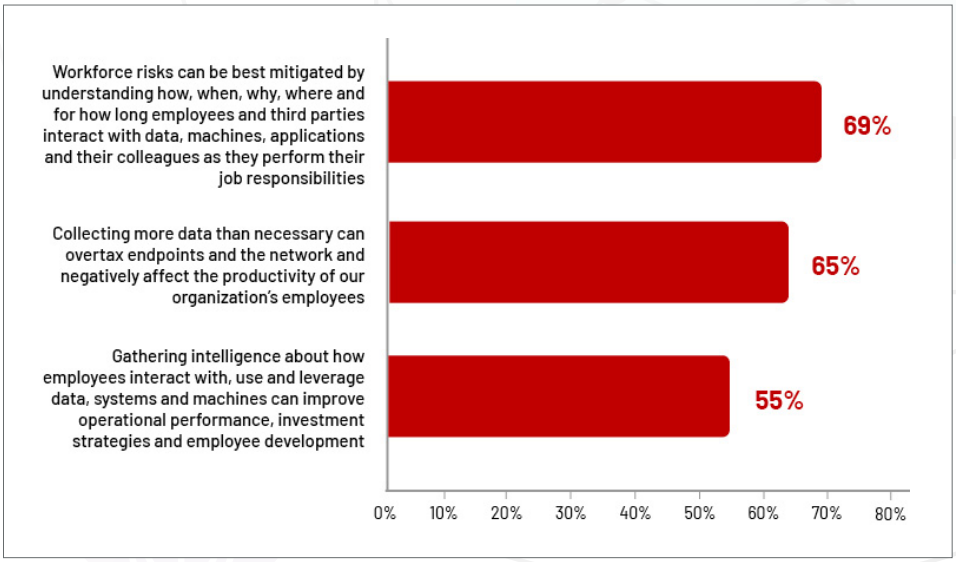


SOLUTIONS THAT HELP ORGANIZATIONS TO UNDERSTAND HOW, WHEN, WHY, WHERE AND FOR HOW LONG EMPLOYEES AND THIRD PARTIES INTERACT WITH DATA MACHINES, APPLICATIONS AND THEIR COLLEAGUES MITIGATE RISKS AND IMPROVE OPERATIONAL PERFORMANCE.

As shown in Figure 8, 69% of respondents say workforce risks can be reduced by tracking employees' activities in the workplace. However, organizations need to be cognizant of the impact of collecting more data than necessary, as this can overtax endpoints and the network, while reducing productivity. In fact, 55% of respondents say gathering anonymized intelligence about how employees interact with, use and leverage data, systems and machines can improve operational performance, investment strategies and employee development.

FIGURE 8. HOW MONITORING PRACTICES IMPROVE OPERATIONAL PERFORMANCE

STRONGLY AGREE AND AGREE RESPONSES COMBINED.



DIFFERENCES AMONG REGIONS

In this section, we present the most interesting differences and consistencies among the following regions: North America (595 respondents), Western Europe (451 respondents) and Australia/New Zealand (203 respondents).

FIGURE 9. DOES YOUR ORGANIZATION USE EMPLOYEE MONITORING DATA TO IMPROVE OPERATIONAL PERFORMANCE?

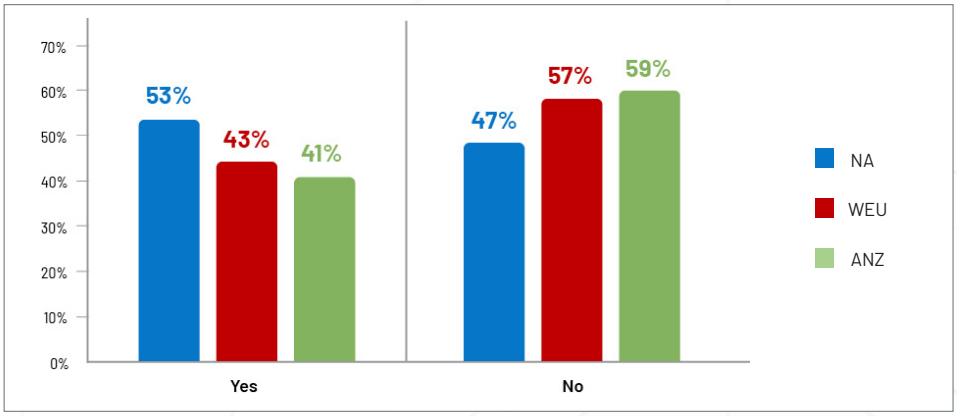


FIGURE 10. EFFECTIVENESS IN PROTECTING SENSITIVE INFORMATION AND ACHIEVING ITS OPERATIONAL PERFORMANCE GOALS
ON A SCALE FROM 1 = NOT EFFECTIVE TO 10 = VERY EFFECTIVE, 7+ RESPONSES PRESENTED

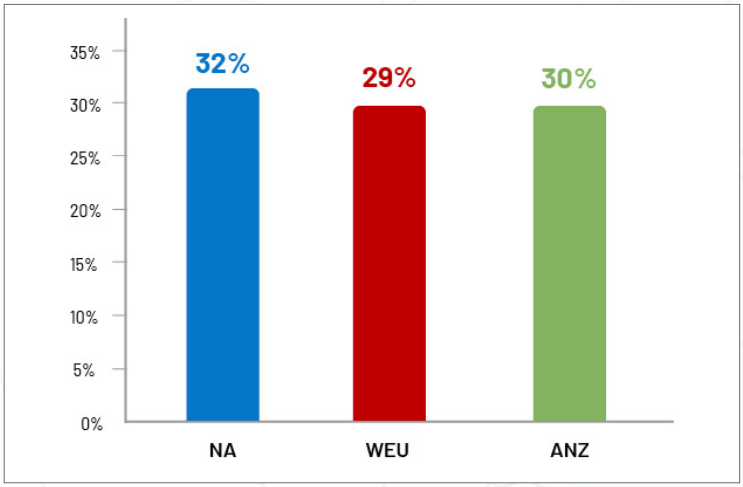
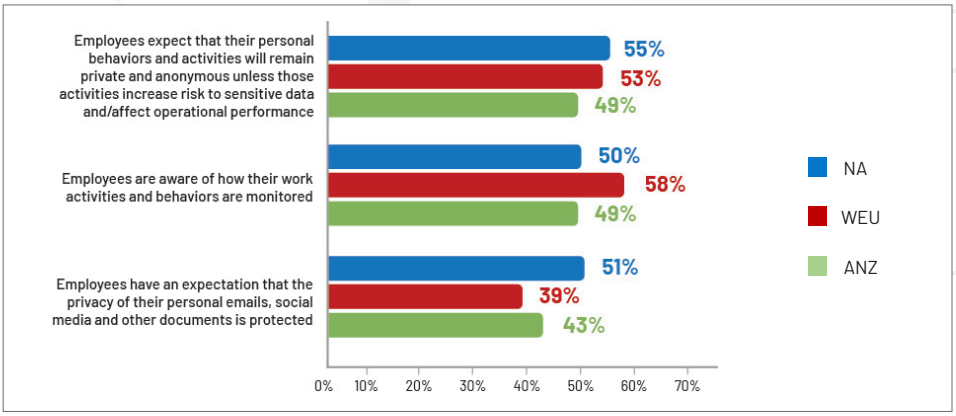


FIGURE 11. EMPLOYEES' PERCEPTIONS ABOUT THEIR PRIVACY IN THE WORKPLACE Q 20, 22, 23
STRONGLY AGREE AND AGREE RESPONSES COMBINED



CONCLUSION & RECOMMENDATIONS

As is evident from the findings of this survey, the state of workforce privacy & risk is in need of improvement. It's not only the technological solutions being leveraged that need to be reevaluated to minimize this privacy gap; there needs to be a critical shift in organizational/employer mindsets. The following recommendations are examples of how organizations can both earn employees' trust in their workplace privacy initiatives and the organization's operational performance.

EMPOWER EMPLOYEES TO HAVE MORE CONTROL OVER THEIR PRIVACY.

The first step is to provide transparency about what employee information is collected on-site and in remote locations. Second, give employees a voice by enabling them to express any concerns about the protection of their privacy in the workplace and in remote locations. Third, have a formal policy that describes your organization's workforce monitoring practices.

TO MITIGATE RISK WITHOUT AFFECTING EMPLOYEE TRUST, ORGANIZATIONS NEED TO BE MINDFUL OF HOW AND WHAT DATA IS COLLECTED.

Organizations should anonymize and minimize the amount of data collected. Additionally, organizations should consider implementing technologies that increase employee trust in the monitoring of access and use of sensitive and confidential information. Only 38% of respondents to this survey said their organization has the right technologies in place to mitigate workforce risks without invading personal privacy, showcasing a clear workforce privacy gap that needs to be closed.

EMPLOYEE TRUST IN HOW THEY ARE BEING TRACKED AND WHAT INFORMATION IS COLLECTED ABOUT THEM IS CRITICAL TO AN ORGANIZATION'S ABILITY TO IMPROVE ITS OPERATIONAL PERFORMANCE.

Only 31% of respondents say their organization is very effective in both protecting sensitive information and improving operational performance.

REDUCING FRICTION WITH THE IT DEPARTMENT IS CRITICAL TO IMPROVING AN ORGANIZATION'S SECURITY POSTURE.

Fifty percent of respondents say the lack of collaboration between IT/IT security and lines of business is putting sensitive information at risk. A closer collaboration between these two functions would result in employees believing they are partners with their organization in both the improvement of data security and operational efficiencies. Many of the respondents to this survey are using antiquated, draconian technologies. The solution to resolving these privacy issues and modernizing is referred to as Workforce Cyber Intelligence.

Workforce Cyber Intelligence is a new approach to enterprise data collection and analysis that results in a more secure workforce, an increase in organizational performance and the protection of employees' privacy. It focuses on creating a safer, smarter and more secure enterprise by understanding how, when, why, where and for how long employees and third parties interact with data, machines, applications and their peers as they perform their job responsibilities. This not only protects enterprises, but employees as well.

Interested in learning more about Workforce Cyber Intelligence?
Please visit: **https://www.dtexsystems.com/why-dtex/what-is-workforce-cyber-intelligence**

For any questions directed to the Ponemon Institue, please contact research@ponemon.org or call us at 800.887.3118.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institue is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high-quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Insights Association**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.