McAfee™

The Top Five Strategies for Improving Digital Wellness

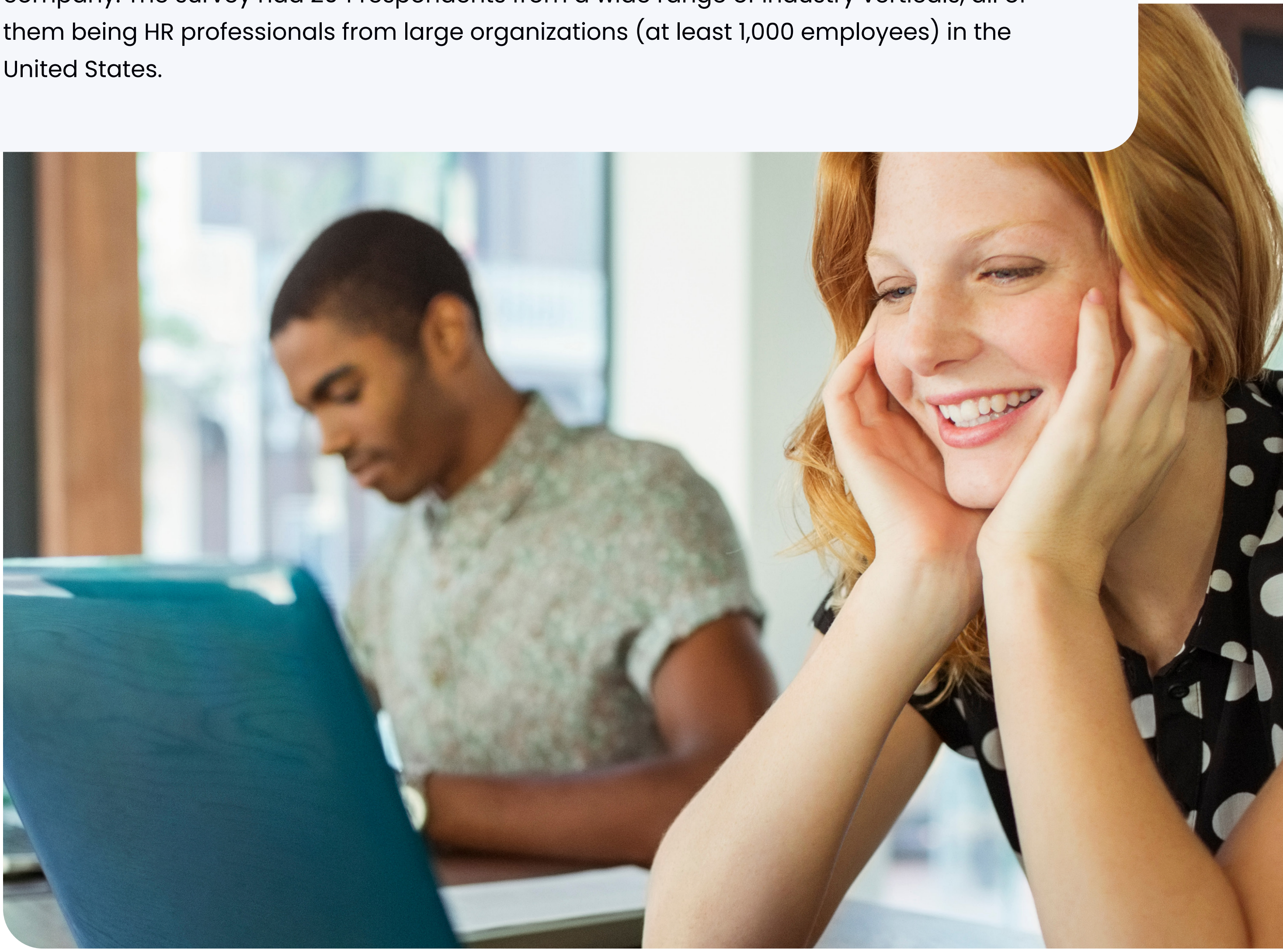
hr.research INSTITUTE

POWERED BY HR.COM

McAfee Digital Wellness™

About the Research

In this article, we allude to data from the HR Research Institute's survey on Digital Wellness that was fielded in 2023 in partnership with McAfee, the global computer security software company. The survey had 204 respondents from a wide range of industry verticals, all of them being HR professionals from large organizations (at least 1,000 employees) in the United States.



Today's organizations prioritize employee well-being as never before. Because so many people spend most of their workdays on computing devices, digital wellness has become especially critical to employee well-being. We believe organizations can adopt five key strategies to boost digital wellness in their workforces.

First, Leverage the Right Technologies and Support

It's no surprise that technology plays a role in digital wellness, but how can it be used most effectively?

First, consider which technologies are best suited to your employees' needs. Do existing work technologies enable digital wellness or are they so inefficient, insecure, and stress-inducing that they diminish it?

Potential problems are made more complicated by remote and hybrid work arrangements, which have become standard in so many organizations. For example, many companies now need to consider the security risks of more employees using personal devices for work purposes. Our study found that 99% of organizations have employees who use personal devices for work at least some of the time. Understandably, 80% of responding firms are "concerned or very concerned" about employees exposing confidential information.

So, what should one look for when considering an employee digital wellness solution? To ensure the well-being of employees, organizations should consider software that allows proactive and comprehensive protection. Specifically, those that prioritize online privacy, preferably with the inclusion of a reliable VPN (that is, a virtual private network) and robust protection against identity theft. Further, such user-friendliness and ease of integration across all devices must be ensured.

Beyond technical features, it can be crucial to consider customer support. Does the digital wellness solution offering provide easily accessible customer support? An ideal digital wellness solution ensures that users can receive prompt assistance whenever needed.

Of course, organizations also need to educate and inform employees about digital wellness and the necessity of it. If an employee finds a virus checker, VPN, or any other tool troublesome, that can engender a negative attitude and inhibit learning. Worse, employees can start to assume that other similar tools aren't worth using.

Second, Formulate the Right Policies and Guidelines

While digital technologies tend to be essential at work, they can also create more significant personal and professional vulnerabilities.
In 2022, the U.S. Internet Crime Complaint Center reported 2,385 complaints identified as ransomware with adjusted losses of more than $34.3 million. That same report stated there were $2.7 billion in losses due to business email compromises.

Policies and guidelines play a vital role in reducing such threats and enhancing digital wellness. For example, the following practices could ensure better cybersecurity.

Create and maintain strong passwords: Implement passwords that combine different letter cases and symbols. Consider changing these passwords every few months to account for employees who have left the organization but still have access.

- **Audit and update technology as needed:** Conducting thorough audits helps identify potentially vulnerable weak links that could pose security risks. By keeping technology up-to-date, organizations can not only enhance security but also foster an environment that boosts employee productivity. Security patches released in updates block hackers from exploiting previously identified weaknesses within a system.

- **Limit access to sensitive information:** Give employees access to sensitive information only on a need-to-know basis. This will help enhance data privacy and security.
- **Establish a plan in case of incidents:** While most organizations do their best to protect from security breaches, incidents can still happen. So, it's important to have a plan in place if something were to happen. For example, assign a team to deal with security issues and encourage employees to report incidents to that team.
- **Encourage employees' personal digital wellness:** By acknowledging the impact of digital habits on mental and physical health, companies can demonstrate a commitment to a balanced work environment.

  Incorporating guidelines for mindful and safe technology use can contribute to enhanced security. It can also improve productivity and overall job satisfaction, ensuring a healthier and happier workforce.

For such guidelines to work, make sure employees understand why the policy exists. Policies work best when employees accept them as being in everyone's best interest. Be sure to listen to any concerns they have and address those concerns. For example, if they feel that strong passwords are troublesome, show them how today's tools can make managing such passwords relatively easy.

In terms of employees' general digital well-being, also consider a right-to-disconnect policy. This policy would allow employees to enjoy their time away from work-related digital devices. Ultimately, this tends to create a more productive and engaged workforce.

Third, Engage in the Right Communications

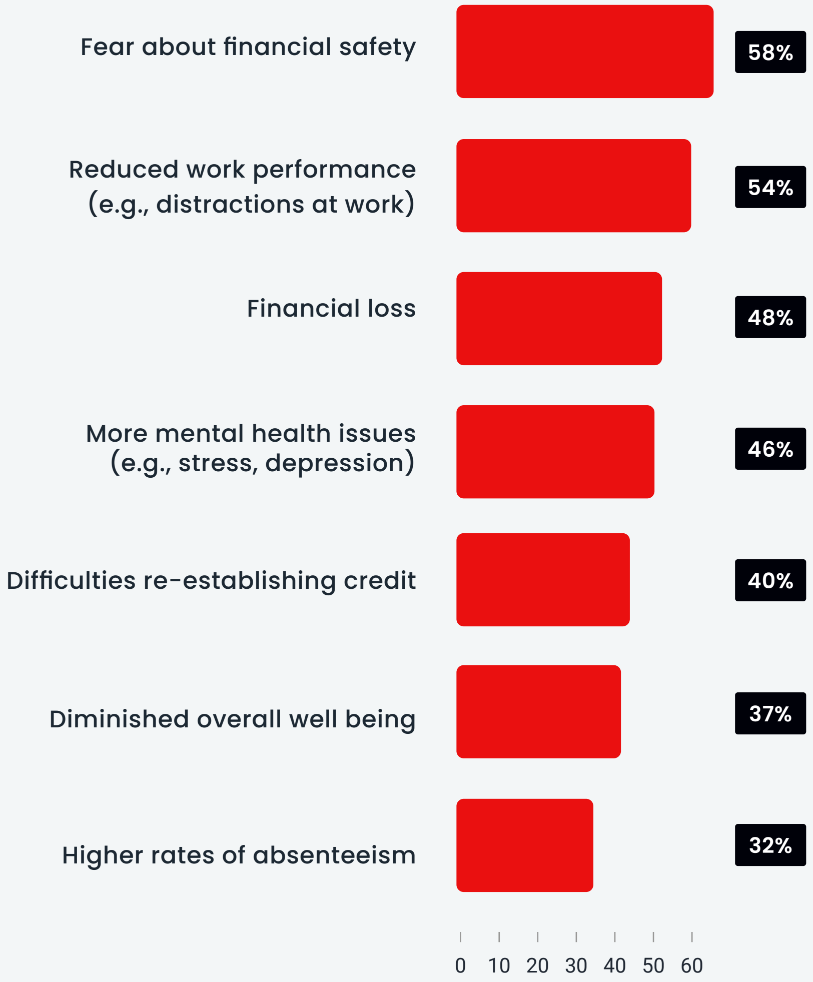
Communication is vital for organizational success in various ways. But how does it specifically pertain to digital wellness?

For one, communication channels such as messaging applications and email allow employees to escalate any security issues to leadership in real-time. Through these means, security breaches can be dealt with quickly, thereby reducing the amount of damage caused to the organization.

Further, our research found that 61% of organizations have suffered from security breaches due to human error. Communication plays a large role in reducing these breaches. For example, HR can collaborate with the IT department to determine the top sources of human error. From there, organizations can act by communicating the issues to employees and offering training and education to reduce the risk of human error in the future.

In some cases, organizations can make employees aware of issues related to identity theft. Our study revealed that 91% of organizations believe employees are at least moderately concerned about identity theft, highlighting the significance of this issue. Additionally, approximately half of responding organizations view reduced work performance, financial loss, and mental health issues as potential outcomes of identity theft.

Survey Question: What do you view as the potential outcomes of identity theft for employess? (select all that apply)



Fourth, Implement the Right Training and Education

Empower employees with the knowledge to improve digital wellness. There are many ways in which organizations can train employees on how to get the most use out of their digital wellness solutions protect themselves and enhance their organization's well-being too.

For example, employers can provide resources such as articles and bring in experts to speak on these issues. They can also incorporate related training and videos into their e-learning systems. And, they can offer incentives or rewards for employees who actively participate in cybersecurity training and demonstrate good digital wellness practices in their personal lives.

Consider tailoring the training content based on the role of every employee. Address the important elements of employee digital well-being solutions such as real-time protection, personal data clean-up, virtual private networks, and identity monitoring/identity theft coverage.

Send Positive Messages

Communication and training on cyber security risks can feel ponderous and threatening, but it doesn't always need to be. Communication messages often work best when they incorporate humor. A series of cartoons may do more to help employees remember best practices than simply relying on text.

Training can be made more fun by using games and quizzes. Getting teams to compete in a game about their cyber security knowledge or practices will often positively grab the attention of employees.

Finally, you may find entertaining guest speakers who can share memorable stories that will bring home the value of following the organization's security guidelines.

Fifth, Offer the Right Set of Benefits

Our study showed that 71% view digital wellness benefits as important for employees. So, what do these benefits look like? They can be anything from device protection from suspicious attacks to identity theft protection and recovery coverage. Here we discuss four elements of digital benefits that were most widely cited in our study.

- **Real-time protection:** As an example of real-time protection, we cited "anti-virus software" in our survey, but this can allude to a variety of protections such as password managers so employees know when it is time to update their passwords.
- **Personal data clean-up:** Personal data clean-up involves reviewing social media and other accounts to ensure the employee's information is accurate, ensuring personal information is secure, and removing any unused or unwanted profiles.
- **Virtual Private Networks:** Through encryption, a VPN creates a secure connection between a digital device and a computer network, or between two networks, even while using insecure communication mediums such as the public Internet. A VPN can also protect employees from various online threats and risks that they might encounter while working remotely.
- **Identity monitoring and Identity theft coverage:** Identity monitoring, which is an element of identity theft protection, gives employees access to a service that checks the dark web to see if their personal information has been subject to a security breach. Other features related to identity theft protection could include ID restoration. In a related area, sometimes there is insurance to cover some of the expenses incurred in the case of identity theft.

Conclusion

There are, of course, various ways of boosting the digital wellness of employees, but we think that leveraging the right technologies, policies, communications, training, and benefits is especially important. Of course, each of them must be managed well to be effective, but if they are, then they tend to reinforce one another in a virtuous cycle of employee well-being.

McAfee™ Digital Wellness

Complete Digital Peace of Mind.

For Employees. For You.

All-in-One Digital Wellness Benefits from McAfee

Identity, privacy and award-winning device protection during work time and play-around time.

Keeping your employees safe online is our full time job.

Learn more

McAfee
Digital
Wellness™