1Password

State of Access Report 2021

The Burnout Breach

How employee burnout is emerging as the next frontier in cybersecurity

Contents

Executive summary	2
The dangers of burnout	3
A threat from within	4
The "Great Resignation" risk	5-6
"Do as I say, not as I do" *The dangers posed by security professionals' lapses*	7
Emerging threats	8
The way forward	9
Conclusion	10
Methodology	10

Legend

Office worker

Security professional

Burned-out
office worker

Burned-out
security professional

"Ready to resign"
office worker

"Ready to resign"
security professional

Executive summary

When organizations around the world abruptly pivoted to remote work in the spring of 2020, cybersecurity threats skyrocketed. Suddenly, a proliferation of cloud-based workloads, home network usage and brand new tools and behaviors exposed dangerous security gaps, which companies struggled mightily to address.

Now, nearly two years into the pandemic, another urgent threat to technology security has emerged: employee burnout.

Workers in virtually every industry are reporting extraordinarily high levels of burnout, stemming from a bitter stew of pandemic-related stresses. This flagging enthusiasm can cause employees to drop their guard, posing data security risks.

To understand how the burnout phenomenon is impacting cybersecurity, 1Password surveyed 2,500 North American adults who work full-time and whose work is conducted primarily at a computer.

Our data, collected in October 2021, indicate that burnout presents a severe, pervasive and multifaceted cybersecurity risk.

Burned-out employees, we discovered, are often apathetic and lax about workplace security measures. For example, employees experiencing burnout were three times as likely as others to acknowledge thinking security rules and policies "aren't worth the hassle" (a view expressed by 20% of burned-out workers and 7% of others).

This apathy is especially pronounced, we found, among employees who are looking to switch jobs. This is particularly relevant because more Americans than ever fall into this category—so many that this period is being described as the "Great Resignation." Respondents who want to switch jobs were nearly 50% more likely to maintain that convenience is more important than security at work, compared to those who plan to stay (24% vs. 16%).

Perhaps most troubling, we found that cybersecurity professionals themselves report disproportionately high levels of burnout. In fact, security professionals were twice as likely as other workers to say that due to burnout, they are "completely checked out" and "doing the bare minimum at work" (10% vs. 5%).

The findings detailed in the following pages draw from 1Password's first annual "State of Access" study. As the modern workforce continues to evolve—with widespread remote and hybrid work, high turnover and a continued push toward the cloud—cybersecurity will be paramount. By tracking security-related attitudes and behaviors among North American workers on a yearly basis, we hope to identify emerging cybersecurity threats—and chart a path forward.

The dangers of burnout

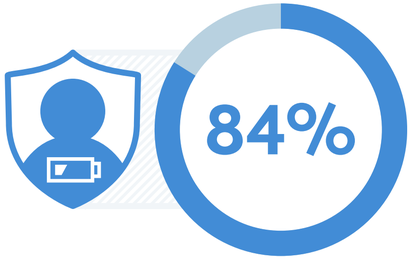
Despite the high level of automation in today's business world, workplaces still rely heavily on human beings—and technology security professionals in particular—to implement the protocols that safeguard their assets, data, information and, ultimately, reputations. When even a small number of people relax their vigilance, organizations are at grave risk. Pervasive burnout among security professionals and other employees presents a significant cybersecurity threat.

"The biggest threat is internal apathy. When people don't use security protocols properly, they leave our company vulnerable."

— Security Professional*

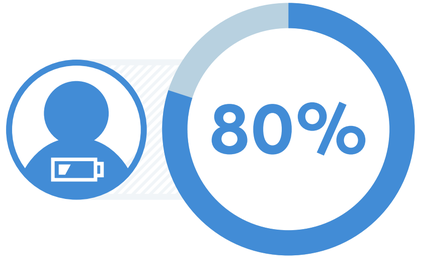
Security professional burnout

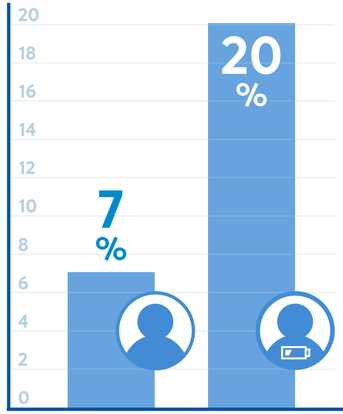
84% of security professionals report feeling burned out.



Office worker burnout

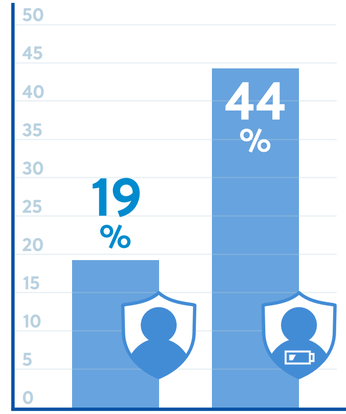
80% of office workers report feeling burned out.





Can't be bothered

3 times as many burned-out employees as non-burned-out employees maintain that security policies "aren't worth the hassle" (20% vs. 7%).



Breaking the rules

Twice as many significantly burned-out security professionals say security rules and policies "aren't worth the hassle," compared to those who are only somewhat burned out (44% vs. 19%).

Completely checked out

Security professionals were twice as likely as other workers to say that due to burnout, they are "completely checked out" and "doing the bare minimum at work" (10% vs. 5%).

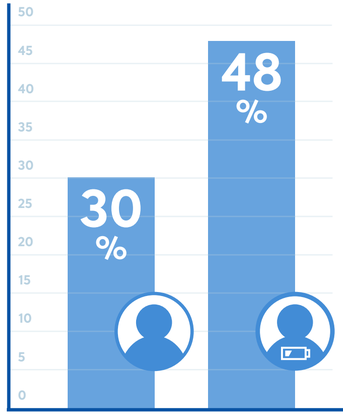
One foot out the door

Nearly a third of burned-out security professionals are currently looking for new jobs or on the verge of quitting—5 times the share of those without significant burnout (32% vs. 6%).

A threat from within

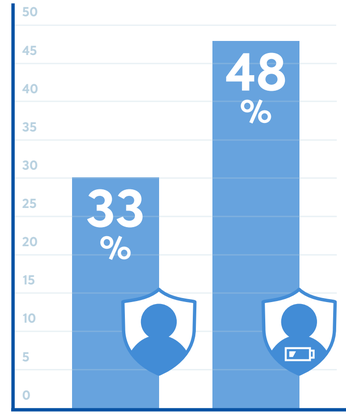
One in 3 workers say burnout is affecting their initiative and motivation levels. Burnout is reducing employees' adherence to security protocols, with a 21-point gap separating those who are burned out (59% of whom say they follow their companies' rules) from those who are not (80% of whom say they follow the rules).

Security professionals are especially prone to burnout, posing an even more critical threat.



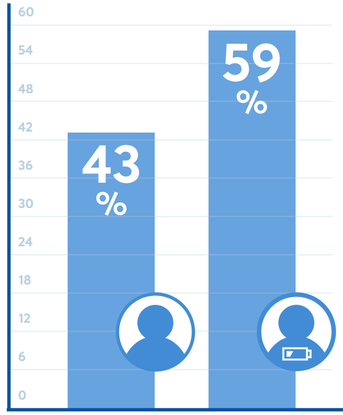
Without IT's permission

60% more burned-out employees than non-burned-out employees are creating, downloading or using software and apps at work without IT's permission (48% vs. 30%).



(Mis)managing apps

48% of burned-out security professionals, and 33% of non-burned-out security professionals, say it's unrealistic for companies to be aware of and manage all apps and devices used by employees at work.



Easy passwords

59% of burned-out employees have poor practices when setting up work passwords, compared to 43% of non-burned-out employees.

Easy breaches

Nearly twice as many burned-out employees pick easy passwords they won't forget (16% vs. 9%) and use the same password or just a few passwords for everything at work (12% vs. 7%), compared to those who are not burned out.

"Security is oftentimes not a technical problem, but an organizational and human problem."

—Adrian Ludwig, Chief Trust Officer, Atlassian

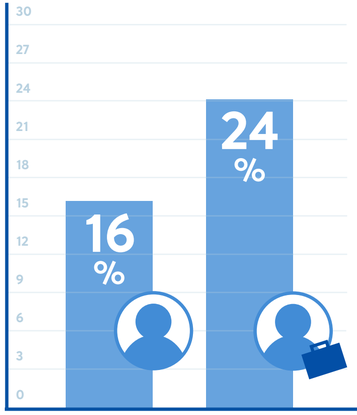
"Taking advantage of human emotions is always a risk to security."

— Security Professional*

The “Great Resignation” risk

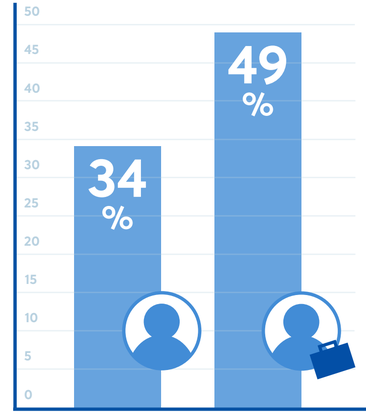
Burnout is a major force behind the “Great Resignation”: an unprecedented exodus of American workers, who are leaving their jobs in search of greater flexibility, satisfaction and salaries. Nearly two-thirds (64%) of our survey respondents said they were actively looking for a new job, on the verge of quitting or, at the very least, open to the idea of switching jobs.

Our findings show that “ready to resign” employees are a significantly greater security risk for companies.



Convenience over security

“Ready to resign” employees were 50% more likely to say convenience is more important than security at work (24% vs. 16% of those expressing loyalty to their current job).

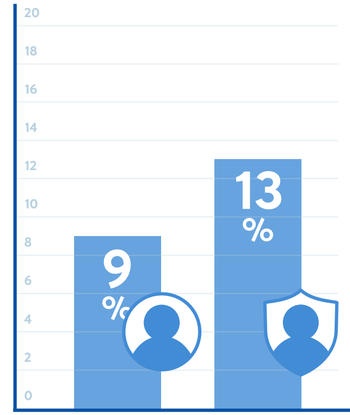


Surging shadow IT

Nearly 50% more employees looking to switch jobs are creating, downloading or using software and apps at work without IT’s permission (49%), compared to those with no interest in a job change (34%).

Imminent flight risks

Security professionals who are burned out were 5 times as likely as those who are not burned out to be considered “imminent flight risks” because they are looking for a new job or planning to quit (32% vs. 6%).



Security shuffle

Nearly 50% more security professionals than other workers are actively looking for a new job (13% vs. 9%).

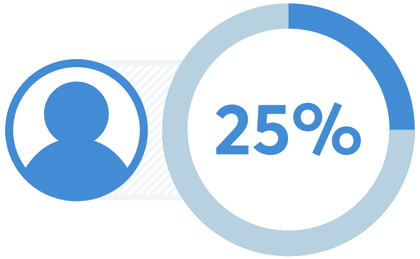
The "Great Resignation" risk continued

Workers who quit often present a security threat to their former employers.

A quarter of workers say they've tried to access a former work account after leaving a job, and over 80% of those say they were successful. These breaches involved targeting relationships, targeting money and targeting brand.

"Employees can be easily manipulated into giving up their security credentials, and much more, by attackers using human psychology."

—Security Professional*

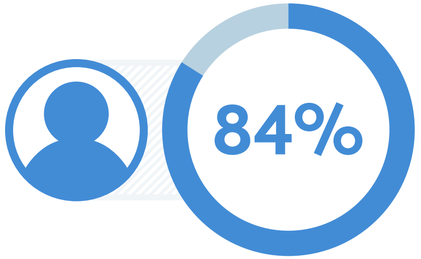


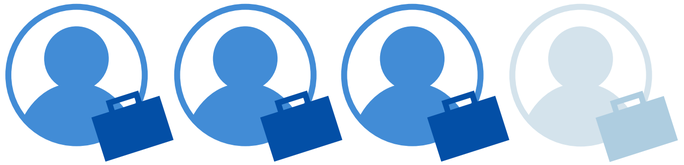
Post-exit access attempts

A quarter of workers say they've tried to access a former work account after leaving a job.

Unauthorized access

84% of those who have tried to access a former work account say they were successful.





Long-term unauthorized access

3 of 4 workers who successfully accessed former work accounts after leaving a job were able to maintain that access for weeks or longer.

Targeting brand

1 in 5 were trying to access company social media accounts.

Targeting money

1 in 4 were trying to access financial accounts.

Targeting relationships

1 in 3 were trying to access a database.

"Do as I say, not as I do" *The dangers posed by security professionals' lapses*

The vast majority of security professionals (89%) say they favor security over convenience. Nonetheless, many acknowledge they often take shortcuts.

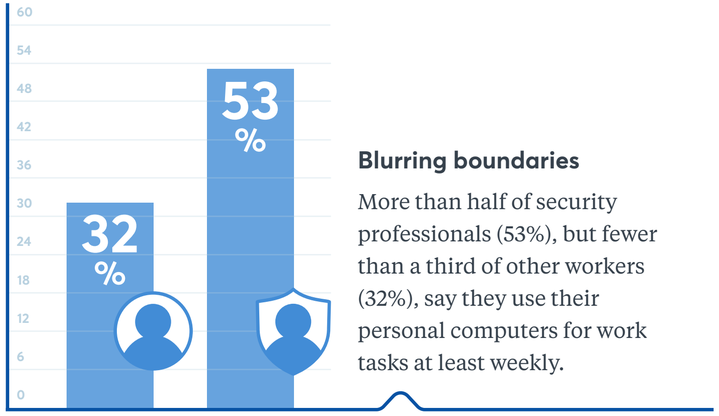
Security professionals were more likely than other types of workers to say they work around their company's policies because they are trying to solve their own IT problems themselves (37% vs. 25%) or because they hate the software their company provides (15% vs. 5%).

"Your best defense is your existing staff. These people know your organization's normal rhythms and will be in a position to say 'this looks odd' when social engineering is attempted. So invest in your staff's willingness to notice risks and raise them, and discourage bad processes that force your staff to take shortcuts and bypass safety checks to get their jobs done."

— Bron Gondwana, CEO, Fastmail

Sharing computers

Nearly 4 times as many security professionals as other workers say they let family members, roommates or friends use their work computers (22% vs. 6%).



Blurring boundaries

More than half of security professionals (53%), but fewer than a third of other workers (32%), say they use their personal computers for work tasks at least weekly.

Installing unapproved apps

4 times as many security professionals as other workers say they install apps or browser extensions the company hasn't recommended or approved (29% vs. 7%).

Emerging threats

We also asked survey respondents about their experience with emerging security threats. We found that security professionals are concerned about a wide range of threats, from the extremely high-tech (like targeted attacks using artificial intelligence) to the profoundly pedestrian (like inattentive, distracted workers).

The rapidly shifting workforce—shaped by remote and hybrid models, cloud-based workloads and tremendous flux and turnover—has dramatically expanded vulnerabilities. According to our survey, the threats that security professionals find most concerning relate to:

- rapidly advancing technology that can automate functions that formerly required human skill
- easily exploited vulnerabilities in human psychology and behavior

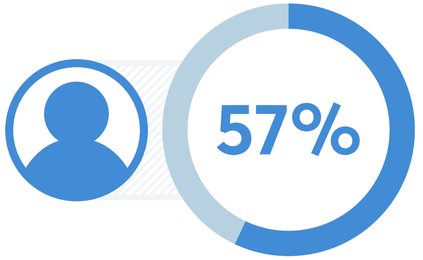
Ransomware is the top threat that security professionals have heard about (55%); of those, 42% list it among their top 3 worries. But just 20% of security professionals actually encountered ransomware at work last year.

Phishing is a top 3 concern for 1 in 4 security professionals knowledgeable on emerging security threats. Even as employees try to look for clues of phishing—by checking senders' email addresses, for example, and looking for typos and unprofessional formatting—many employees continue to fall victim.

Phishing is especially dangerous because it manipulates human psychology, by mimicking friends or coworkers in need of help—or companies or colleagues seeking to offer protection and assistance.

Encountering threats

6 in 10 security professionals say their company encountered an emerging security threat last year, with social media spoofing, sophisticated phishing and DDoS attacks being the most common.



Phishing confusion

Over half (57%) of employees say they've recently encountered an email which they weren't sure was phishing or not.

"With all of the heat on ransomware gangs right now, we may see a decline in sophisticated attacks against large organizations—and a focus on breaching the security of small to medium-sized businesses, as they tend to have fewer defenses."

— John Donovan, CISO, Malwarebytes

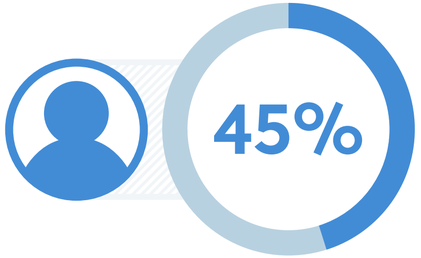
"I think it's too easy to overlook the benefits of simple software upgrades. Failure to keep software up-to-date is behind an appalling number of horror stories. The more you can build up-to-dateness into your values, the better."

— Ricardo Signes, CTO, Fastmail

The way forward

The impact of burnout on organizations' cybersecurity illustrates how human psychology and behavior can diminish technological solutions.

Burnout aside, our findings indicate that high-quality, user-friendly software that meets or exceeds employees' expectations can have an enormous impact on security.

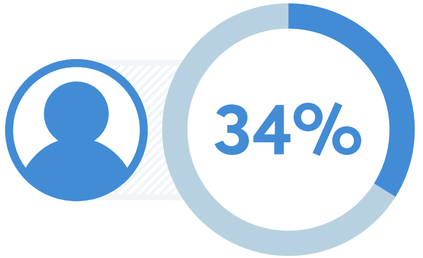


Improving automation

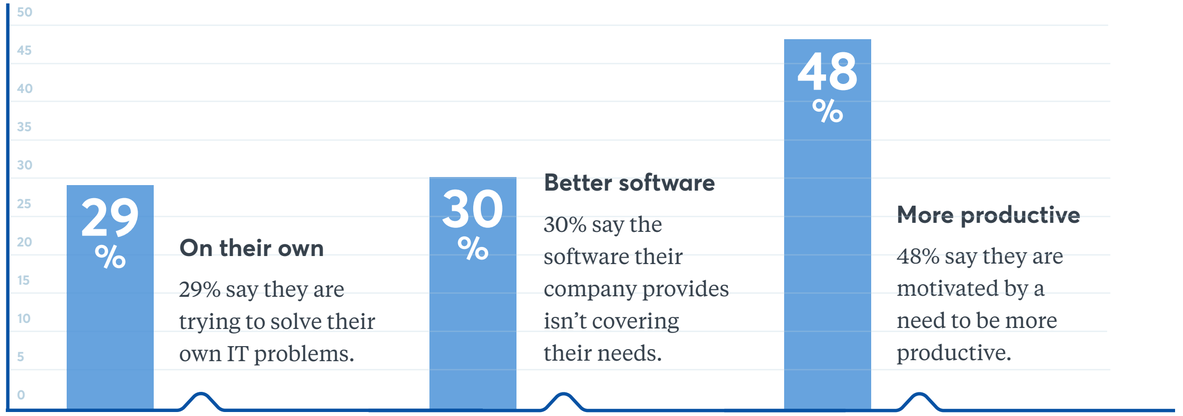
45% of remote and hybrid employees who aren't perfectly following their company's security rules and policies say they'd be more likely to follow them if they were automatically forced by technology to do so.

Forced by technology

34% of in-office workers who aren't consistently adhering to their company's security rules and policies say they'd be more likely to follow them if automatically forced by technology to do so.



Among respondents who acknowledge skirting their companies' policies on downloading apps and software:



On their own

29% say they are trying to solve their own IT problems.

Better software

30% say the software their company provides isn't covering their needs.

More productive

48% say they are motivated by a need to be more productive.

"I'd like to see organizations preparing better for data breaches—for example, practicing incident response in the same way as they've practiced disaster recovery for years now. I'd also like to see a much bigger focus on preemptively working to minimize the damage caused by breaches, through practicing data minimization. You cannot lose what you do not have."

— Troy Hunt, Founder, Have I Been Pwned

Conclusion

Widespread burnout among employees, and security professionals in particular, is leaving organizations dangerously vulnerable to cybersecurity attacks. While fast-evolving technologies and practices have enabled organizations to survive and thrive throughout the Covid-19 pandemic, their rapid escalation—coupled with the enormous toll the pandemic has taken on employees' lives and well-being—have created new opportunities for bad actors.

Remote and hybrid work is here to stay. Two-thirds of respondents to our study, in fact, are currently working at companies that still have everyone working remotely or in a hybrid setup. As even more data, applications and workloads move to the cloud to accommodate a geographically dispersed workforce, employers who develop airtight security protocols tailored to a "work-from-anywhere" model will benefit.

Moving forward, companies will need to focus on unintended threats from within as well as highly targeted threats from outside their organizations. When it comes to cybersecurity, the employee burnout conversation should be front and center.

"Human error causes data breaches more than anything else. We need to better protect the individual wherever they venture. This is what I call human-centric security."

— Akshay Bhargava, Chief Product Officer, 1Password

Methodology

1Password conducted this research using an online survey prepared by Method Research and distributed by Dynata among n=2,500 adults ages 18+ in North America (US + Canada) who work full-time primarily at a computer. The sample consisted of 2,000 respondents from any department and title within their company, while n=500 respondents were security practitioners working in IT departments with a manager title or above. The sample was roughly equally split between gender groups. Data was collected from October 6 to October 18, 2021.

*The quotes attributed to anonymous security professionals throughout this report draw from survey participants' responses to open-ended questions.

About 1Password

1Password provides human-centric security for everyone, everywhere. The company's password management and credentials security platform is trusted by more than 100,000 business customers including IBM, Slack, Shopify, Under Armour and many more. 1Password also protects the most sensitive information of millions of individuals and families across the globe, and is committed to helping consumers and businesses get more done in less time and with security and privacy as a given. Learn more at 1Password.com.