# Contents

1. A year later—key statistics  3
2. Pandemic-induced IT and security changes  5
3. Cybersecurity improvements in the time of COVID-19  7
4. The problem with fear fatigue  10
5. Fortifying cybersecurity remotely presents challenges  12
6. Will employees return to the office?  17
7. How to create a “new normal” for cybersecurity  19
A YEAR LATER

Key statistics

After the world moved to remote working conditions in the spring of 2020, Malwarebytes surveyed 200 IT decision makers (ITDMs) through the C-suite about how the COVID-19 pandemic lockdowns affected their businesses and changed the face of work environments forever. Now that companies have been working in a hybrid or remote environment for over a year and a half, we checked back in to see what—if anything—had changed.

Our research shows that organizations have embraced many cybersecurity best practices as employees become more aware and vigilant of constant threats, both from cybercriminals and COVID-19. However, organizations must also learn to balance cybersecurity education while avoiding fear fatigue.

Fear fatigue is defined as the “demotivation to follow recommended protective behaviors, emerging gradually over time and affected by a number of emotions, experiences, and perceptions.” In the context of cybersecurity, fear fatigue refers to a complacency that leads to careless behaviors, such as opening an email attachment without properly scrutinizing the sender or neglecting to turn on a VPN while using public WiFi.
Organizations must learn to balance cybersecurity education while avoiding fear fatigue.

IT managers surveyed on cybersecurity posture and employee experiences

- 55% Revealed that their organizations have made some improvements in their cybersecurity posture since the beginning of the pandemic
- 71% Implemented new cybersecurity trainings
- 74% Implemented new tools
- 61% Reported employees experiencing fear fatigue, with 27 percent feeling particularly overwhelmed by fear
- 69% Expressed that employees needed more IT support than their businesses had IT resources available
- 62% of IT Managers’ most significant concern was employees accidentally exposing data, such as by using “shadow IT” tools
HOW THE PANDEMIC CHANGED IT AND SECURITY

As organizations adapted to remote working, their spending habits also changed. More than 70 percent of respondents said they now spend more on cybersecurity tools, cloud-based software tools, and IT support and management staff. A significant number (60 percent) also reported spending more on hardware, which is consistent with increased hardware spending in our original report (62 percent) at the beginning of the pandemic, when many organizations provided hardware for remote work environments.
Remote work has changed the way we work and significantly increased the use of tools across cloud collaboration, cybersecurity, backup, and other solutions.

We have beefed up our security controls as well as security tools as we expand to support an ever increasing remote work force. Our goal is security controls protecting the users and users being smarter about security. We have one gauge that we consistently measure - a monthly/quarterly phishing awareness campaign - that indicates our employees are getting more vigilant about security.”

— TC, manufacturing company
Despite the challenges of remote work, ITDMs continued to be confident in employees following security best practices.

A majority of respondents (61 percent) said they think their employees are “very aware” or “acutely aware” of cybersecurity best practices, which is only a slight decrease from our initial report of 64 percent.

ITDMs also perceived their employees as being committed to cybersecurity practices at home. Most respondents (82 percent) felt that their employees care about maintaining good cybersecurity practices.
Despite the challenges of remote work, ITDMs continued to be confident in employees following security best practices.

<table>
<thead>
<tr>
<th>Awareness Level</th>
<th>Percentage</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oblivious and risky</td>
<td>11%</td>
<td>(21/200)</td>
</tr>
<tr>
<td>Slightly aware</td>
<td>13%</td>
<td>(26/200)</td>
</tr>
<tr>
<td>Aware but not a priority</td>
<td>15%</td>
<td>(30/200)</td>
</tr>
<tr>
<td>Very aware</td>
<td>44%</td>
<td>(87/200)</td>
</tr>
<tr>
<td>Acutely aware and mindful to avoid risk</td>
<td>18%</td>
<td>(36/200)</td>
</tr>
</tbody>
</table>

Conversely, a small group reported that their employees “don’t care enough” about cybersecurity best practices (3 percent) and some reported a few employees who are considered “reckless” (1.5 percent).

While few ITDMs were concerned about employee recklessness, even one employee can represent a significant risk: An organization’s cybersecurity posture is only as strong as its weakest link.
An organization’s cybersecurity posture is only as strong as its weakest link.

How would you say that the employees in your organization feel about cybersecurity practices at home? Select one.

200 total respondents

- **Our employees care deeply about maintaining good cybersecurity practices**: 51% (101/200)
- **Our employees care somewhat about maintaining good cybersecurity practices**: 32% (63/200)
- **Our employees are ambivalent about cybersecurity practices**: 14% (27/200)
- **Our employees don’t care about cybersecurity practices enough**: 3% (6/200)
- **Our employees are reckless about cybersecurity practices**: 1.5% (3/200)
THE PROBLEM WITH FEAR FATIGUE

With the increase in velocity and damage from cyberattacks, many organizations have invested in new tools, processes, and staff training programs to stay safe.

However, remaining ever vigilant comes at a cost, with almost 80 percent of survey respondents reporting some level of jadedness or “fear fatigue” within their organization.

ITDMs reported that more than one in four employees (27 percent) were overwhelmed by threats and jaded by cybersecurity procedures.

Organizations must continue to design cybersecurity programs that take the burden off of employees and counter inadvertent actions that put data at risk.
The best approach here is to continually practice radical empathy — for others in the workplace and for yourself. You have to be willing to forgive and willing to be flexible. You can’t be too hard on yourself right now as we are all still collectively healing. In moments of extreme exhaustion, I think it’s important to take time to reflect and to practice mindfulness. Remind yourself of things you’re still grateful for and let go of outdated mindsets, routines, and the things that don’t truly matter.”

— Tanya Barlow, PROCON, Inc.

Are your employees facing “fear fatigue?”
Does that impact cybersecurity threats?

200 total respondents

- Yes, employees seem overwhelmed by threats and jaded by cybersecurity procedures: 27% (54/200)
- Yes, employees overall seem to have reached a point of fear fatigue during the pandemic beyond just cybersecurity: 22% (43/200)
- My employees seem somewhat overwhelmed by threats and jaded by cybersecurity procedures: 13% (26/200)
- My employees seem to be experiencing some level of fear fatigue during the pandemic beyond just cybersecurity: 18% (35/200)
- There is no clear impact of fear fatigue within my organization: 21% (42/200)
FORTIFYING CYBERSECURITY REMOTELY STILL PRESENTS CHALLENGES

Despite increasing cybersecurity fortification in the remote work environment, another set of challenges have come to life.

Almost three in four ITDMs (74 percent) said they have implemented new tools to enhance security. They also reported enforcing new cybersecurity trainings (70 percent); requiring employees to use additional security measures (51 percent), such as two-factor authentication (2FA); and updating their crisis management protocol (48 percent).
After being home for up to 18 months, what would you say has changed about your organization’s security posture? Select all that apply. 200 total respondents

However, many businesses are still struggling to find the right cybersecurity tools (62 percent) to support employees at home. Another challenge ITDMs reported was how to remotely train their employees (54 percent) on working securely and meeting compliance requirements from home.

To compound matters, ITDMs’ biggest cybersecurity concerns were exacerbated by remote work: 62 percent were concerned about accidentally exposing data, while 51 percent harbored concerns that cloud-based collaboration tools may not offer adequate security, especially as use increased significantly.

62% of businesses are still struggling to find the right cybersecurity tools to support employees at home.
After being home for up to 18 months, what would you say has changed about your organization’s security posture? Select all that apply.

200 total respondents

- 63% Finding the right cybersecurity tools to support employees at home
- 54% Training employees how to most securely and compliantly work at home
- 69% Serving employee needs through limited IT resources
- 54% Shifting to a new, remote model of communication and/or collaboration amongst employees
- 41% Ensuring work/life balance
- 43% Setting up work or personal devices with new software to continue responsibilities/roles

ITDMs’ biggest cybersecurity concerns were exacerbated by remote work.

Many ITDMs who were not fully prepared for the added security measures needed at the beginning of the pandemic have since improved their remote cybersecurity posture.

In our first report, IT decision makers scored their organization over 7 out of 10 in readiness to work from home. Although, at the time, 44 percent did not provide cybersecurity training that focused on the potential threats of working from home, and 65 percent did not deploy a new antivirus solution for new devices issued to employees working remotely for the first time.
Many ITDMs who were not fully prepared for the added security measures needed at the beginning of the pandemic have since improved their remote cybersecurity posture.

What are your biggest cybersecurity concerns currently? Select all that apply.

200 total respondents

- **26%** Bossware monitoring employee performance | 52
- **39%** Phishing/clicking on a malicious link | 78
- **63%** Exposing data or information accidentally, (possibly by using shadow IT tools or software/tool...) | 125
- **34%** Ransomeware | 67
- **32%** Hackers gaining access to proprietary information | 63
- **34%** Losing access to immediate, physical IT support in the office | 68
- **31%** Purposful insider data exfiltration from company employees | 61
- **52%** Cloud collaboration tools may not provide adequate cybersecurity (Concerns of Zoom) | 103
- **15%** Difficulty in offboarding remote employees when necessary to prevent unauthorized future access | 29
### How has your organization’s level of security changed from the start of hybrid work environments due to the pandemic versus now? Select one.

**200 total respondents**

- **We’re significantly less secure than at the beginning of the shift to remote work**: 8% (16/200)
- **We’re slightly less secure than at the beginning of the shift to remote work**: 18% (36/200)
- **We’re equally secure than at the beginning of the shift to remote work**: 19% (38/200)
- **We’re slightly more secure than at the beginning of the shift to remote work**: 29% (57/200)
- **We’re significantly more secure than at the beginning of the shift to remote work**: 27% (53/200)

### How has your use of devices changed in today’s working environment, when compared to the beginning of the pandemic? Select one.

**200 total respondents**

- **I now only use my work-issued devices for work**: 42% (84/200)
- **I now sometimes use my personal devices for work**: 28% (55/200)
- **I now use my personal and work devices to the same degree**: 21% (41/200)
- **I now use my personal devices for work more than my work-issued devices**: 10% (20/200)
- **My organization did not offer me a work-issued device**: 0% (0/200)
WILL EMPLOYEES RETURN TO THE OFFICE?

As lockdowns continue to ease and people return to the "new normal," many businesses have an eye towards reopening. However, not all employees feel the same. According to a survey by FlexJobs, an online employment agency, 58 percent of most remote workers would "absolutely" look for a new job if they were not allowed to work out of the office.²

While many employers may worry that employees are less productive outside the office, 65 percent of ITDMs report that productivity has actually stayed the same or improved in remote environments.

When asked to rank their concerns for returning to the office, ITDMs top concern was health matters, followed by being unable to focus in open office environments, or losing valuable time commuting to the office. Concerns about pets being left home alone ranked last.
65% of ITDMs report that productivity has actually stayed the same or improved in remote environments.

Top return to work concerns

- Health concerns: 71%
- Trouble focusing/distractions in-office: 35%
- Not being present due to relocating: 32%
- Childcare concerns: 29%
- Commuting time lost: 27%
- Pets not adjusting to owner’s absence: 6%
HOW TO CREATE A “NEW NORMAL” FOR CYBERSECURITY

According to the Verizon 2021 Data Breach Investigations Report, 85 percent of breaches are caused by people. Employees are an organization’s biggest asset, but they also break the rules and make mistakes—sometimes, costly ones. Mistakes can happen due to distractions (57 percent), stress (52 percent), and general fatigue (44 percent), and employees need protecting, supporting, and keeping safe.

Fear fatigue inspires complacency, and complacency leads to risky cybersecurity behavior. Scammers are primed and ready to take advantage of reduced focus.

Stronger awareness and overall protection are essential to keeping threats at bay. However, maintaining low risk factors by addressing fear fatigue will better serve organizations in the long run. As the pandemic drags on, with no real end in sight, there’s no better time to confront complacency.

Any organization that requests, processes, accesses, or stores customer data should prioritize securing employees against inadvertent errors. In fact, organizations should consider “human-proofing” an essential layer of their cybersecurity approach.

Leveraging technology, for example, to automatically and readily block site visits from employees clicking potentially malicious links, or detecting and binning spear phishing email attempts before a targeted employee gets to see them, are some of the ways organizations can help keep their employees—and, in turn, company data—safe.
But technology can’t do it all. Organizations should start looking into implementing effective fatigue mitigation programs\(^6\). Employers must collaborate with employees to figure out general strategies\(^7\), which could include ways of developing strong social networks and regularly practicing healthy routines, to manage fatigue. It’s recommended that employees be given ample chance to unplug and refresh themselves.

To further help employees stay secure, cybersecurity-wise, Malwarebytes suggests the following tips for organizations: “Reinforce security measures often and in a fun way. Phish your own employees. Gamify security trainings. You can get fatigue from communications, too, so balance the right amount of communication. Know how to provide folks with guardrails, so they don’t drive off the road by mistake. Proper endpoint protection must be in place. Use a corporate VPN when you are on unsecured networks.”

The sudden change to work in response to the COVID-19 pandemic has illustrated that focusing solely on the security of data and systems, while ignoring the people using them, is not a holistic cybersecurity strategy. Innovative organizations are realizing that to improve overall cybersecurity posture, we need to secure everything and everyone.

Cyberattacks and threats to businesses will never go away. What organizations need is technology that automatically negates human error and provides the confidence needed for employees to work securely and productively from anywhere. Remote work may be here to stay, but fear fatigue shouldn’t be.

Sources


4 Tessian Research & Hancock, Jeff (Stanford University). “Understanding the mistakes that compromise your company’s security” (July 2020) https://www.tessian.com/research/the-psychology-of-human-error/


65% of ITDMs report that productivity has actually stayed the same or improved in remote environments.