How-to

Alamy

SECURITY > VULNERABILITIES AND THREATS

How To Prevent Quiet Quitting in Cybersecurity

Quiet quitting continues to pose severe risks for cybersecurity efforts. Here are five ways to keep staff happy and engaged.

Karen D. Schwartz | Apr 12, 2023

1. Create clear expectations for remote work
2. Provide employees with opportunities for growth
3. Promote team culture and connections
4. Staff the cybersecurity team properly
5. Monitor and measure employee engagement

Quiet quitting, where an employee disengages from their role without formally resigning, remains a problem in today's job market, especially in the cybersecurity industry. Signs of quiet quitting include plummeting productivity, absenteeism and being AWOL during a crisis, and doing the bare minimum.

Related: Cybersecurity Skills Shortage: How a Focus on DEI Can Help

In cybersecurity, disengaged employees can have severe consequences. At the very least, work isn't being done, leaving more work for the rest of the cybersecurity team to do. But that's only the beginning: Cybersecurity employees who aren't on top of their game are more likely to miss critical alerts, make mistakes, or take too long to make decisions about security threats. And as we all know, it only takes seconds for a malicious threat like ransomware to make its way through the network.

"If a cybersecurity professional is disengaged or unavailable, the repercussions can be huge," said Maurice Stebila, a former CISO and founder of CxO InSyte, which runs cybersecurity networking events for CISOs. "These people are literally in a foxhole, and they have to be ready at all times."

When cybersecurity professional quietly quit their jobs, it can lead to retention problems and stretch the remaining staff thin, affecting security coverage for the organization, noted Tapan Shah, cybersecurity leader for EY Americas Consulting.

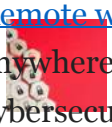
According to ISACA's State of Cybersecurity 2022 report, 69% of organizations that experienced more cyberattacks in the past year reported being understaffed. ISACA found that the top reasons why cybersecurity professionals leave their jobs include limited promotion and development opportunities, high stress at work, and lack of management support.

you prevent quiet quitting from becoming a problem.

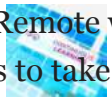
0 COMMENTS

#1. Create clear expectations for remote work

RECOMMENDED READING


Key Strategies for Tackling Third-party Software Vulnerabilities
MAY 22, 2023


Look Out – Get-Rich-Quick Schemes Are Coming to AI
MAY 17, 2023


Cisco U. VP Explains How Upskilling and Reskilling Drive Tech Careers
MAY 10, 2023


Generative AI: A Cybercriminal's New Best Friend
MAY 08, 2023

[Remote work](#) can be a double-edged sword. Employees appreciate the flexibility to work from anywhere and often work longer hours, which can be a plus for employers struggling to fill cybersecurity positions. However, it's hard for some remote workers to remain focused and engaged.

"Remote work can make it easier to be out of sight and out of mind. Some [employees] even go as far as to take a second job and work both at the same time," said Dan Lohrmann, field CISO for the public sector at Presidio, a digital services and solutions provider. "It only works if there is a good relationship and clear expectations about what constitutes good performance."

#2. Provide employees with opportunities for growth

In addition to providing social and well-being opportunities, organizations must ensure they provide employees with a clear path for progression.

"An employee may have been working in security operations for five years, and that's pretty mundane work," Stebila said. "If you're not cross-training those people yearly and giving them opportunities to learn something different, you're going to see plenty of quiet quitting."

About
Advertise
Contact Us
Sitemap
Ad Choices
CCPA: Do not sell my personal info
Privacy Policy
Terms of Service
Content Licensing/Reprints
Cookie Policy
Follow Us
© 2023 Informa USA, Inc., All rights reserved
Privacy Policy | Cookie Policy | Terms of Use

#3. Promote team culture and connections

Company leaders should have regular check-ins with the team and foster a healthy work culture with social events and activities.

"Organizations must encourage strong human capital management, especially as more companies continue operating in remote or hybrid settings," said Jon France, CISO of (ISC)², an organization for cybersecurity professionals. "Just because we are remote working doesn't mean we should lower connectedness within teams. We should still set goals, [do] check-ins, train, and support one another in the organization."

Stebila suggested that CISOs regularly take their employees to lunch, something he has done his entire career. At one company, Stebila had 44 people on his staff. He took each employee to lunch periodically. "I found that by taking someone out of the work environment and interacting with them one on one, there is more opportunity to share thoughts," he said. "Being heard and recognized goes a long way."

#4. Staff the cybersecurity team properly

Despite the cybersecurity talent shortage, don't skimp on staffing. Failing to staff up can lead to burnout, which often leads to quiet quitting (and real quitting).

#5. Monitor and measure employee engagement

"One of the best indicators that an organization has a problem with its workforce is by measuring happiness," said Sushila Nair, vice president of cybersecurity services at Capgemini and vice president of ISACA's Washington, D.C. chapter. "The best way to start is by using anonymous surveys to get a baseline."

Nair also recommended that organizations track attrition levels, engagement levels, response times to tickets and incidents, and attendance rates at all-hands calls. If any of these measures trend in the wrong direction, it may indicate unhappiness and dysfunction among employees.

Shah called these types of measurements "frequent listening." To the list of monitoring and measuring activities, he added focus groups. "These things can be leading indicators of a kind of quiet quitting, where they withdraw to focus only on their own tasks at a lesser level and care less about the team, the department, and the needs of the group."

If an employee is suspected of quiet quitting, it may be worth monitoring whether they are downloading and collecting intellectual property. Organizations can usually configure data loss prevention and endpoint monitoring tools to accomplish this.

About the author

Karen D. Schwartz is a technology and business writer with more than 20 years of experience. She has written on a broad range of technology topics for publications including CIO, InformationWeek, GCN, FCW, FedTech, BizTech, eWeek and Government Executive.