JUL 01
Jacob Bourne

Millions of hacking attempts daily as cybersecurity industry bleeds workers

Article

The news: The cybersecurity field is burning out as mounting attacks take their toll.

- **45% of senior cybersecurity professionals are considering quitting the industry due to stress from unrelenting ransomware attacks**, according to Deep Instinct's annual Voice of the SecOps report.
- **4 in 10 UK cybersecurity leaders say they might quit due to stress within the year**, according to a Bridewell Cyber Security in Critical National Infrastructure Organizations 2022 report.
- The US House Subcommittee on Intelligence and Counterterrorism warned on Tuesday of considerable risks small businesses and local governments face from cyberattacks.
- Chairwoman **Elissa Slotkin**, D-Mich., said **Michigan state services get targeted by hackers 90 million times a day**.
- Meanwhile, top cybersecurity expert **Kevin Fu** said the healthcare industry is ripe for a disastrous medical device attack that could harm patients.

Layoffs: A litany of cybersecurity layoffs this year follows an increase in the sector's number of unfilled positions by **350%** in 2021, per TechCrunch.

- Virginia-based **IronNet**, which helps large corporations and government agencies protect critical infrastructure, announced plans to lay off **17%** of its workforce.
- In April, San Jose-based **Lacework** laid off **20%** of its workforce.

Just last month, layoffs hit the industry particularly hard:

- Atlanta-based startup **OneTrust** cut **25%** of its workforce.
- US-Israeli startup **Cybereason** laid off **10%** of staff.
- Deep Instinct laid off 10% of its workforce.
- **Automox** laid off **18%** of workers.

Why it's worth watching: Russia's war in Ukraine has raised the risk of attacks globally.

- The emergence of tech like no-code and low-code tools could exacerbate the problem.
- Although AI can be used as a cybersecurity tool, its unrestrained proliferation across society also creates vulnerabilities.
- We should expect long-term risks to rise as quantum computing poses the potential for breaking cryptographic algorithms.

The big takeaway: As workers hit their stress threshold and quit and firms enact layoffs, remaining staff become even more overburdened than before.

- Although organizations can take steps to beef up security with multifactor authentication and encryption, more cybersecurity specialists are needed.
- **Higher education institutions could hire more cybersecurity educators**, create related degree pathways, and work with industry recruiters to link recent graduates with jobs.
- As cyberattacks threaten to wreak havoc on all sectors of society including critical infrastructure, the case is strong to bolster incentives for people to enter the field with more robust pay and benefits, not layoffs.