From Burnout to Balance: How AI Supports Cybersecurity Professionals

By Jason Lamar, SVP of Product at Cobalt

As technology advances, cyber threats are becoming more complex and harder to combat. According to Cobalt's State of Pentesting Report, this past year, the number of security vulnerabilities increased by 21%, putting organizations at greater risk than ever before. Because some of these vulnerabilities carry a high probability of exploitation, cybersecurity professionals are working overtime to reduce their exposure and give their organizations a fighting chance against cyber threats. Cyber professionals' day-to-day lives have always been plagued by long hours and high stress levels, but coupled with the growing number of cyber risks, industry leaders continue on the path to burnout.

While artificial intelligence (AI) has a reputation for contributing to the growing number of cybersecurity incidents, when used appropriately, this technology may provide cybersecurity professionals with some hope of relief from their immense workloads. Over the past 12 months, 75% of cybersecurity professionals have adopted new AI tools into their organization. With the growing accessibility of this technology, cybersecurity professionals have the opportunity to leverage these tools to speed up a multitude of tasks and better manage the always-on approach needed to stay secure in today's threat landscape.

Burnout From the Top Down

2024 has already set a new record for ransomware attacks as the number of new leak sites reached an all-time high for a single quarter. So far this year, the world has seen a number of high-profile ransomware attacks, including the Ascension Healthcare network and Change Healthcare attacks. These nationwide incidents forced cybersecurity teams nationwide into overdrive to protect their systems from similar vulnerabilities. On top of this, organizations are dealing with unsurmountable stress internally.

What's more, a recent SEC regulation now requires public companies to disclose cybersecurity incidents within four days of the incident being determined material, thrusting CISOs into the hot seat, nervously awaiting a cybersecurity blunder that could derail their careers. The mental and physical health of C-suite executives is dwindling, leaving some looking towards the exit. While C-suite professionals in the cybersecurity industry are 34% more likely than average respondents to say they currently want to quit their jobs, almost half of cybersecurity professionals at all levels are currently experiencing burnout.

Over the past six years, a third of cybersecurity teams have faced layoffs, with more internal shifts on the horizon. When layoffs occur, the uncertainty can have negative implications across the board. 67% of cybersecurity professionals agree that layoffs and resignations cause noticeable disruptions to their ability to maintain high-security standards. This is a 10% increase from 2023, demonstrating how cyber professionals are noticing these issues compound each year. The cybersecurity industry must find new ways to alleviate the burdensome workload currently on their plates or else they risk losing more talented professionals with each year to burnout.

Where AI Can Help

When put in the right hands, AI may provide immense benefits within the workplace. Our annual report found that 73% of cybersecurity professionals already view AI as a valuable tool rather than a threat to the organization. AI can help companies stay competitive by appealing to new generations of talent expecting the next tech, streamlining administrative tasks like reports, and monitoring data for irregularities.

From network traffic monitoring to checking for vulnerabilities, cybersecurity professionals have a multitude of items on their plate that could be alleviated by AI. Of course, that’s not to say this technology can fully take on the role of a trained cybersecurity professional or that it doesn’t cost something to begin to adopt AI. A new and ongoing learning burden exists for all who want the benefits. In fact, AI should be viewed as a new intern at the company. Colleagues should check its work for accuracy and jump in should issues arise, but ultimately, it can be trusted with a variety of lower-stake projects.

At Cobalt, for instance, we’re seeing an increased demand for pentests as companies incorporate offensive security strategies into their defense plans. Pentests can effectively uncover known and new vulnerabilities in various systems, making them a significant asset for cybersecurity teams. These tests are thorough, and with that, they’re also time-consuming. Our pentesters have found ways to leverage AI to automate report generation, free up time to address vulnerabilities and implement new security measures.

The cybersecurity industry is showing no signs of slowing down, and neither is AI's role in our society. Cybersecurity professionals have been asked to battle large-scale cyber threats, internal disruption, and changing industry standards, forcing them to be on alert constantly. AI is no silver bullet, but it has the potential to provide much-needed relief for industry leaders who are desperate for more sustainable operations. If this past year has shown us anything, it's that 2024 is shaping up to be a challenge like never before. Industry leaders should equip their teams today with emerging technologies to ensure they're prepared for whatever this year throws their way and can better balance their workload.

About the Author

Jason Lamar is Cobalt's SVP of Product. In this role, Jason is responsible for product, product operations, and design teams pioneering Pentest as a Service (PtaaS) and building out the Offensive Security solution portfolio. Jason has made a career of building and launching innovative cybersecurity products, supporting from ideation to release to adoption success. With more than two decades of experience in the cybersecurity industry, Jason has worked with companies of all sizes to provide customers with the technology and knowledge to defend themselves in today's dynamic risk landscape.

Jason can be reached on LinkedIn and at Cobalt's website: https://www.cobalt.io/.