The Impact of AI on Cybersecurity Operations and Employee Well-being

Jeremy Schoenick

University of the People

ENGL 1102: English Composition 2

Jason Kahler

January 7, 2026

Abstract

Integrating Artificial Intelligence (AI) into cybersecurity operations is readily transforming the industry. While most of today's focus is on financial and the operational benefits AI provides–such as quicker incident response times and cost savings–less attention has been paid to how these tools impact the human element of cyber defense. Due to "alert fatigue" and burnout, cybersecurity professionals face high turnover rates, creating a "hidden" or lesser known vulnerability in the security posture. This paper analyzes data from recent sources, 2024 and 2025, to evaluate the impact AI has on both operational efficiency and employee job satisfaction. The findings indicated that while AI significantly reduced response time which also lowered breach costs, its ability to automate repetitive tasks also plays a vital role in mitigating burnout. This paper argues that it is in an organization's best interests to adopt a balanced security strategy that views employees well-being not just as an HR concern, but as a long-term piece of the security infrastructure.

Introduction

Cybersecurity is easily comparable to being a soccer goalie. A goalie can block the ball from entering the net 1,000 times, but missing just that one block that loses the game, that error is usually the only thing remembered. Attackers only need to be successful once, whereas the defenders must be successful 100% of the time. "Success" usually results in nothing happening, making the victory seem less or invisible. Consequently, cybersecurity professionals often will find themselves in a burnout loop, defending against an overwhelming volume of threats. This

dynamic leads to a high turnover rate, which ends up costing companies even more in recruitment and retraining on systems that just keep evolving.

In today's rapidly evolving digital world, there is a concern that human intelligence is being wasted on repetitive tasks, slowing down even the most advanced professionals with unwanted tasks. Utilizing AI tools in high-stress cybersecurity operations helps offload these repetitive tasks, such as threat monitoring, and enhances productivity and job satisfaction. This paper examines the utilization of machine efficiency and the impact on human well-being, positing that the true value of AI lies in its ability to stabilize the human workforce.

Background

In today's world, the current cybersecurity landscape is defined by volume and velocity. Security Operation Centers (SOCs) are plagued with thousands of alerts a day. This sheer volume leads to "alert fatigue". Analysts become desensitized to alarms due to sensory adaptation. When they experience this desensitized state, they are more likely to overlook critical security alerts, leading to potential breaches.

Historically, the industry has hired more analysts in an attempt to solve this issue, but the gap in talent and high turnover rates make this strategy unsustainable. The introduction of automation tools and Generative AI offer a technological solution. Implementing these tools is usually solely justified though financial metrics, overlooking the positive impacts it may have on the cognitive load of the analysts operating them.

Problem Statement

In today's evolving digital landscape, integrating AI into cybersecurity operations is becoming a more dominant trend. While this is a benefit, it currently lacks a unified framework that connects the operational efficiency with the human factors. Most research today focuses primarily on cost savings and speed, treating the mental well-being of the employees as a secondary factor rather than an important component in the security infrastructure. Neglecting the mental well-being of humans and focusing on speed creates a critical gap; which may lead to compounding security risks through error and turnover.

Research Objectives and Questions

The main goal of this paper is to bridge the gap between operational efficiency and human factors in the field of cybersecurity. The specific objectives are:

1. Analyzing the impact AI has on burnout and job satisfaction by reducing the volume of repetitive tasks.
2. Evaluating the negative impacts that ignoring the analysts mental well-being may have on the company's security posture.
3. To determine if a balanced approach of speed and mental well-being yields a greater long-term financial and security benefit

To achieve these objectives, this paper will address the following research questions

- How does the utilization of AI for completing low-value repetitive tasks influence the cognitive load and job satisfaction of cybersecurity professionals?
- What is the correlation between unaddressed burnout and a company's security posture, specifically regarding turnover rates and human error?

- Where is the line that a balanced security strategy yields a long-term financial benefit compared to just speed alone?

Literature Review

Current literature evaluates the integration of AI into the cybersecurity field through two distinct lenses: productivity and job satisfaction.

Operational Efficiency and Cost: Recent studies demonstrate a clear correlation between adopting AI and financial savings. In a study evaluating Microsoft's Copilot, which is a generative AI tool, Bono et al. (2024) analyzed data from live security operations. They determined that adopting this technology reduced the time to resolve incidents by 30.13% within just three months. Similarly, a report from 2024 by IBM highlights that AI-enabled teams contain breaches up to five days faster than previous benchmarks. The financial savings resulting from this are significant; according to Bonderud (2025), organizations using AI and automation saved an average of $1.9 million USD in breach costs compared to those that did not.

The Human Factor and Job Satisfaction: There are multiple reports that highlight the potential for improved job satisfaction. An ISC2 workforce study found that roughly 75% of professionals use AI specifically to automate repetitive tasks (ISC2, 2024). This report also notes that AI impacts the areas where companies would rather not have skilled laborers tied up which is time-consuming and lower-value functions (ISC2, 2024)

Furthermore, Lamar (2024) reported that 73% of cybersecurity professionals now view AI as a valuable asset rather than a threat, stating that it offers a balance in an environment where cybersecurity professionals are "forced to be on alert consistently." Edmondson and Bromiley (2024) emphasized that the benefits extend beyond operational speed and help enhance employee morale. The survey pointed out that among the organizations reporting high job satisfaction, 71% of these companies attributed this boost to AI handling repetitive tasks, and allowing them to focus on more rewarding work.

Methodology

This research uses a secondary qualitative analysis methodology. It utilizes the data and findings from five key industry reports and peer-reviewed studies that were published between 2024 and 2025. These sources were chosen due to their relevance to high-level security operations, the integrity of their data (making sure it reflects the post-generative AI boom), and their authority (stemming from some of the major industry bodies such as IBM, SANS, and ISC2). This analysis focuses on cross-referencing the quantitative data regarding incident response times against the qualitative survey data regarding the burnout rates and "alert fatigue" to assist in identifying the correlations between automation and workforce stability.

Results

Reviewing the collected data revealed two primary findings:

1. **Inverse Correlation between AI and Incident Time:** The data from the literature confirms that adopting AI leads to immediate, and measurable reductions in operational friction. The reduction of incident resolution time by roughly 30% (Bono et al., 2024)

and the containment of breaches five days faster (Bonderud, 2025) validates the "efficiency" argument for AI.

2. **Positive Correlation between Automation and Job Satisfaction:** AI acts as a relief mechanism, contrary to the belief that AI would displace jobs. With 71% of satisfied professionals attributing their sentiment to AI's ability to handle the repetitive tasks (Edmondson & Bromiley, 2024), the results were indicative that automation is directly providing positive impacts on "alert fatigue" described in this paper.

Discussion

The evidence provided in this research paper demonstrates that financial and human benefits of AI are not two separate metrics, but they are linked. While the IBM and Bono et al. study highlights the "hard" metrics of time and money, the SANS and ISC2 study reveals the "soft" metrics of morale.

This paper argues that the "soft" metric here is actually the financial one. If companies solely focus on efficiency, they risk creating a high-pressure environment akin to the "goalie" analogy scenario mentioned earlier–high stakes and no relief. Having AI handle the overwhelming amount of repetitive tasks, organizations achieve consistent threat monitoring that humans cannot possibly recreate without drastic ways and helps break them out of this burnout loop.

Because AI lowers the cognitive load, we get the positive result that burnout decreases. When burnout decreases, the high turnover rates stabilize. Due to higher turnover rates resulting in companies to spend more resources in retraining new employees on complex systems, preserving the mental well-being of current employees translates into a measure that ends up

saving companies money. Therefore, the $1.9 million savings cited by Bonderud (2025) is likely the aggregate of both technical efficiency (faster breach containment) and organizational efficiency (retained talent)

Conclusion

Integrating AI into the cybersecurity field offers benefits other than just speed; it offers sustainability. AI tools, such as Microsoft Copilot and automated threat detection systems, drastically reduce incident response time and breach costs, their value is equally significant in protecting the mental well-being of security professionals. By automating the "time-consuming and lower-value functions" (ISC2, 2024), AI allows analysts to escape the burnout loop and focus on high-value, and rewarding work.

In conclusion, this paper addresses the human factor not just being a human resources concern, but as a major and critical metric of a company's security posture. A security strategy that focuses on the mental well-being of its employees through the use of automation will yield greater long-term financial and operational benefits than a strategy based on just speed alone.

References

Bonderud, D. (2025, November 18). *Cost of a data breach 2024: Financial industry*. IBM. https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry

Bono, J., Grana, J., & Xu, A. (2024, November). *Generative AI and security operations center productivity: Evidence from live operations*. arXiv. https://arxiv.org/html/2411.03116v2

Edmondson, M., & Bromiley, M. (September, 2024). *SANS 2024 AI Survey*. SANS Institute. https://services.google.com/fh/files/misc/sans-2024-ai-security-survey-gcs.pdf

ISC2. (2024, February 22). *The Real-World Impact of AI on Cybersecurity Professionals*. ISC2 Insights. https://www.isc2.org/Insights/2024/02/The-Real-World-Impact-of-AI-on-Cybersecurity-Professionals

Lamar, J. (2024, September 29). *From burnout to balance: How AI supports cybersecurity professionals*. Cyber Defense Magazine. https://www.cyberdefensemagazine.com/from-burnout-to-balance-how-ai-supports-cybersecurity-professionals-2/