# Chapter 15
# Artificial Intelligence and Robotics in the Nail Care Industry:
## Are Cyberattackers Sitting Pretty for a Zero-Day Attack?

**Laura Ann Jones**
https://orcid.org/0000-0002-0299-370X
*Capitol Technology University, USA*

## ABSTRACT

*This study investigates the cyber vulnerabilities of artificial intelligence (AI) and robotics in the nail care industry, mainly using nail-painting robot technology, and identifies other cybersecurity concerns. The wide use of evolving technologies across sectors is not a new phenomenon; however, the utilization of robotics in nail salons is a recent development, with its initial implementation less than three years ago. The possibility of unauthorized access to or control of the robots exists for industries that leverage these technological advancements. Despite limited public reporting on cyberattacks in nail salons, the increasing adoption of AI and robotics necessitates implementing proactive cybersecurity measures. Hackers exploit vulnerabilities before the weaknesses in technology are made known. Due to the human safety risks that robots can cause, financial implications, and the prospect of being targeted for malicious cyber activity, protecting the nail care industry through sound cybersecurity measures is imperative.*

## INTRODUCTION

More than 20 million individuals in the United States engaged in manicure services on four or more occasions throughout 2020, with the actual figure potentially surpassing this estimate due to the survey's exclusion of individuals who receive nail treatments less frequently than four times a year (Statista, 2020). The number of nail treatments is likely to continue to grow in the coming years (ReportLinker, 2023; Statista, 2020).

DOI: 10.4018/979-8-3693-1906-2.ch015

According to IBISWorld (2023), the number of nail salons in the United States in 2023 was estimated to be 111,350, with a total employment of 433,623 individuals. Fortune Business Insights (2023) indicates that the United States led the world in nail salon revenue in 2020, with a market value of $10.7 billion. Further, the global nail salon sector has a substantial market size of $11.00 billion in 2022 (Statista, 2020). These numbers indicate that a substantial proportion of individuals worldwide take part in nail care services yearly.

The beauty industry, which generated approximately $430 billion in revenue in 2022, is increasingly becoming a target for cyber threats due to its rapid digital transformation and the sensitive nature of customer data it handles (McKinsey, 2023). Integrating robots to provide customer service has been gradual, with the concept being developed and refined over several years (Grandey & Morris, 2023; Madhan; 2023).

Overall, the beauty industry's investment in AI, which includes nail care, was expected to reach $7.3 billion in 2022 (HomeConsumer Goods & Services, 2023). Moreover, the use of AI across the beauty enterprise is expected to significantly contribute to its projected growth of $580 billion by 2027 (McKinsey & Company, 2023). Recently, the beauty industry has witnessed a surge in the use of AI technology, with robots powered by AI reaching the nail care industry (Market Research Future, 2023; Valley et al., 2021). One of the most innovative applications of AI in the beauty industry is the development of manicure robots (Davis, 2022; Papadopoulos, 2023). These machines offer an express option for nail treatments (Prinzivalli, 2021) and could be available in corporate buildings, retail stores, and airports (McKinsey & Company, 2023).

Notably, this study did not locate prior research focusing specifically on successful cyber exploits in the nail industry; however, while the nail care sector may not be a primary focus for cybercriminals, it is nevertheless susceptible to cyberattacks. Any enterprise that utilizes computers, networks, software, or online services is susceptible to potential threats such as data breaches, ransomware, phishing, malware, or other assaults. The escalating apprehension regarding cybersecurity is particularly prominent in various sectors, particularly those heavily dependent on digital technologies and data.

Cybersecurity is an essential component for organizations that depend on technological systems and networks. Nevertheless, cyberattackers can undermine even the most sophisticated security measures by capitalizing on undisclosed weaknesses in software or hardware. Zero-day vulnerabilities refer to specific weaknesses unknown to the software vendor and have not been patched or fixed. A zero-day attacks are the malevolent activities that exploit these vulnerabilities.

Hence, nail care experts and enterprises must possess knowledge of the potential hazards and implement precautionary measures to safeguard their data and systems. The increasing demand for personalized and efficient services drives this growth. Integrating AI into services such as nail care is enhancing the customer experience and opening new avenues for revenue generation (Walch, 2020). Moreover, it is helping the industry adapt to unprecedented challenges and prepare for a more automated future (Walch, 2020).