Eighty two percent of security professionals fear artificial intelligence attacks against their organization

Oct 24, 2018

Neustar's International Cyber Benchmark Index™ reveals the top cybersecurity concerns

???

Neustar®, Inc., a trusted, neutral provider of real-time information services, today released the most recent International Cyber Benchmarks Index, which highlights the increased year-over-year concern around security vulnerabilities, including significant fears around the impact of artificial intelligence (AI) on company security defenses.

According to the report, security professionals recognize the potential of AI in cybersecurity – with 87 percent of respondents agreeing that it will make a difference to their company's defenses. However, the majority (82 percent) of security professionals are concerned about the possibility of attackers using AI against their company, with stolen data (50 percent) being of the highest concern, followed by the loss of customer trust (19 percent). Business performance and cost implications were also weighted equally (16 percent). As a result, nearly 60 percent of security leaders are apprehensive about adopting AI technology within their organizations.

??The International Cyber Benchmarks Index is an initiative of the Neustar International Security Council (NISC) , an elite group of select cybersecurity leaders across key industries that assesses the international cybersecurity landscape from the vantage point of security professionals across the EMEA and U.S. regions. Other key findings from the most recent survey include:

- **DDoS leading the way:** DDoS was most likely to be perceived as an increasing threat to organizations, followed by social engineering, email and generalized phishing.
- **Rising threats:** 46 percent of enterprises have been on the receiving end of a DDoS attack in Q3, a higher proportion than in previous reporting periods.
- **IPv6 adoption:** Just under half (48 percent) of organizations have already begun to adopt IPv6, and 16 percent have not started. Lack of IPv6 enterprise adoption and security considerations is presenting new opportunities for cyber criminals.
- **Threat from outside:** Organizations have perceived the most likely increase in threats to be from criminals and unknown actors. These threats are also perceived to be increasing the most from the world at large and the least from within their own company.

"Artificial intelligence has been a major topic of discussion in recent times – with good reason," said Rodney

Joffe, Head of NISC and Neustar Senior Vice President and Fellow. “There is immense opportunity available, but as we’ve seen today with this data, we’re at a crossroads. Organizations know the benefits, but they are also aware that today’s attackers have unique capabilities to cause destruction with that same technology. As a result, they’ve come to a point where they’re unsure if AI is a friend or foe.”

“What we do know is that IT leaders are confident in AI’s ability to make a significant difference in their defenses,” said Rodney Joffe. “So what’s needed now is for security teams to prioritize education around AI, not only to ensure that the most efficient security strategies have been implemented, but to give organizations the opportunity to embrace - and not fear - this technology.”

About Neustar, Inc.

Neustar, Inc. is a leading global information services provider driving the connected world forward with responsible identity resolution. As a company built on a foundation of Privacy by Design, Neustar is depended upon by the world’s largest corporations to help grow, guard and guide their businesses with the most complete understanding of how to connect people, places and things. Neustar’s unique, accurate and real-time identity system, continuously corroborated through billions of transactions, empowers critical decisions across our clients’ enterprise needs. More information is available at https://www.home.neustar.

??