ROCHESTER BUSINESS JOURNAL
JANUARY 12, 2024

SPECIAL REPORT

Cybersecurity

NEXT LEVEL ARTIFICIAL INTELLIGENCE

Generative AI is smarter, smoother and easily used by bad actors

BY CAURIE PUTNAM

Story begins on Page 8

Generative AI – What large and small businesses need to know

By CAURIE PUTNAM

In 2023 ProArch's most downloaded piece of content on their website was a free AI Policy Template, which helps businesses provide clear guidelines and expectations for the ethical use of AI tools, ensuring privacy, data security, transparency, and accountability in the organization's practices.

"Any business is susceptible to AI-generated threats, especially if they're not taking any measures to protect their data," said Ben Wilcox, the CTO of ProArch, a Fairportheadquartered, global team of multidisciplinary experts in cloud, infrastructure, data analytics, cybersecurity, compliance, and software development.

Wilcox explains that, like any cybersecurity threat, data is the ultimate prize for those using generative AI in malicious ways.

Generative AI is the type of deep learning AI utilizes in platforms like ChatGPT, Google Bard,

Wilcox

and Bing Chat. It became readily accessible to the public in October 2022 with the release of Chat GPT 3.0 and differs from traditional, general AI.

Whereas general AI mostly recognizes patterns and can provide canned answers to set questions and keywords, generative AI creates brand-new content, including text, images,

---

audio and more that appear human-like in origin.

One way cybercriminals use generative AI is by creating unique content — like phishing emails — that is sometimes of higher writing quality than the public has previously seen.

"Writing is hard for a lot of people," said Wilcox, who noted generative AI may make it easier for people with both good and bad intentions to write AI-generated content that's sometimes indistinguishable from that generated by humans.

Research published in the ScienceDirect journal Research Methods in Applied Linguistics in September 2023 revealed that "experts from the world's top linguistic journals could differentiate between AI- and humangenerated abstracts less than 39 percent of the time."

Wilcox says it's important for businesses to keep in mind that it's not only the attackers that could be a threat with generative AI but also unwitting employees via shadow AI.

GENERATIVE from page 8 to 10

Harnish

Travis

the information technology industry and says when it comes to generative AI and business, education is key. "There are companies that don't even know that they're using generative AI," Travis said. "There is a significant need for education and awareness of the risks and capabilities of AI."

Risks of generative AI go beyond security vulnerabilities, Travis explained, and can also include

“Shadow AI is when people use AI without the approval of the business they work for,” said Wilcox, noting that this behavior opens a new door for cybersecurity and data privacy threats. “Setting allowable use cases is important.”

Reg Harnish is the CEO of OrbitalFire, a leading cybersecurity services provider specifically for small businesses headquartered in the Capitol Region with clients in Rochester.

While he says 2023 was loud in terms of the chatter of generative AI, when it came down to boots on the ground, things were relatively quiet for small businesses.

“We’re not seeing a lot right now in terms of impact,” said Harnish about threats to small businesses from AI. “We’re also not seeing it show up as a defensive mechanism much either.”

Harnish is in wait-and-see mode — not overreacting or underreacting to the threats of AI on small businesses but looking for more data to emerge.

“Small businesses’ advantage is that they’re small, so they’re a much smaller target and have historically been less likely to be victimized because they’re flying under the radar,” said Harnish, about cybercrime. “But AI could change that because of the economics and start to neutralize the advantage small businesses have.”

Harnish does not believe the overall quality of the content of phishing emails has increased with generative AI, but he does believe generative AI is starting to make it cheaper and faster to conduct scams — opening the door to more solo operators with just a laptop and AI platform.

The extent to which these AI-driven frauds will target small businesses is yet to be seen, but on a broader level, Harnish said, “When you change the economics of cybercrime that is a huge advantage for our adversaries.”

Jeffery Travis is a director with the Fox-Pointe Solutions information risk management division of The Bonadio Group. He has over 25 years of experience in data privacy, bias and fairness, transparency, regulatory and compliance challenges and ethical concerns. On the flip side, the capabilities of generative AI can include improved security protocols, automated real-time threat protection, data analysis, and product development.

“It’s a double-edged sword,” said Travis about generative AI, calling it a “great technology, an advanced technology,” but also one that can be used nefariously and can be injected with misinformation and bias.

The first step a business considering the use of AI should take is to identify the goals and scope of AI implementation, Travis said, followed by an assessment of current capabilities and the development of an AI strategy. Other steps include but are not limited to, strong human oversight, stakeholder communication, knowledge sharing, monitoring and continuous improvement, and contingency planning.

“Plan for someone getting in,” Travis said. “Prepare for potential AI failure or breach. Every company should dust off their cyber incident response plans and inject AI in there.”

Regulatory and ethical considerations are also extremely important, though the United States does not have the overarching data privacy laws seen in the European Union yet. Some resources and agencies Travis recommends for companies looking to be proactive in this space include: -The White House’s Blueprint for an AI Bill of Rights https://www.whitehouse.gov/ostp/ ai-bill-of-rights/ - The National Institute of Standards and Technology (NIST) https://www.nist.gov/ -The National Conference of State Legislatures’ summary of Artificial Intelligence 2023 Legislation https://www.ncsl.org/technology-and-communication/ artificial-intelligence-2023-legislation Caurie Putnam is a Rochester-area freelance writer.