The Emergence of AI In the Enterprise: Know the Security Risks

By John Anthony Smith, CEO Conversant Group, and Eli Nussbaum, Managing Director, Conversant Group

As businesses strive to keep up with the rapid pace of technological advancement, many are turning to artificial intelligence (AI) tools as an increasingly vital component of their strategies. One such tool is ChatGPT, an OpenAI language model being leveraged by cross-departmental employees in customer service, marketing, research, and more. However, as is often the case with any new, emerging technology, using AI comes with security risks, and it's essential to understand them and impose the proper guardrails around them to protect company, customer, and employee data.

While we could delve into some of the defensive cybersecurity concerns AI presents—such as its use to create more realistic and compelling phishing emails and social engineering tactics as well as broader "Skynet" type concerns—we will confine our discussion to the risks inherent in leveraging ChatGPT and other Artificial Generative Intelligence (AGI) as productivity tools. There are real, tangible risks businesses must address today, as AI/AGI is a relatively immature technology actively making its way

into the corporate environment. Specific to ChatGPT, there are many unknowns regarding its ongoing evolution and how it impacts data and information security. From an infosec perspective, managing "unknowns" is not anyone's view of ideal. Cybersecurity is the art and science of attempting to achieve full transparency to risk and then mitigating and controlling that risk.

Even if an organization secures its connectivity to OpenAI, it is challenging to ensure data protection, particularly granting the tremendous data troves gathered by ChatGPT. In late March, OpenAI disclosed a data breach that exposed portions of user chat history as well as personal user information including names, email/payment addresses, and portions of credit card data over a nine-hour window. That same week, threat intelligence company Grey Noise issued a warning regarding a new ChatGPT feature that enabled expanded data collection features using a plugin, which they believed had been exploited in the wild. Samsung employees also leaked sensitive data into the ChatGPT program; as a result, Samsung lost control of some of its intellectual property. Since there are little to no legal precedents for this activity, these types of leaks have the potential to cost organizations billions in lost opportunity and revenue. There is also little evidence of how the large tech companies that control these platforms may leverage this newly found treasure trove of previously undisclosed intellectual property.

These issues highlight the vulnerability of the product and raise serious concerns about the security of sensitive information that businesses, knowingly or unknowingly, entrust to ChatGPT. As with all third parties, these platforms must be vetted and their vendors contractually bound to protect the data to your organization's standards before being permitted access to it.

The security issues also underscore the legal obligations of organizations to secure their own and their clients' data. Law firms with attorney-client privilege and those subject to regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the EU's General Data Protection Regulation (GDPR) are particularly affected. Organizations must ensure the security and privacy of their information. Using a third-party service like ChatGPT creates challenges to these obligations.

Importantly, OpenAI's ChatGPT and Google's Bard learn from and store information from many sources. Organizations should never place corporate and client information into these platforms, as it must be assumed it can be viewed by those unauthorized to do so (intentionally or otherwise). The lack of clarity and transparency around how data is being handled creates a real risk for businesses using ChatGPT. Yet, lacking direct action by IT or security teams to impose controls, users can easily copy and paste data of any level of corporate sensitivity into the platform, without their organization's knowledge or consent. Thus, these platforms should be blocked by default, despite their current attraction and whirling popularity. For organizations that require research and development in these platforms, access should only be permitted for those groups.

Today, it is quite difficult to block these platforms by default because they are popping up quickly (as well as their related scams). Fortinet, Palo Alto Networks, Cisco, and other security vendors have not yet created holistic lists that include all the OpenAI and ChatGPT options available. Thus, IT is left to compile manual lists of these tools for blocking.

To mitigate the risks of AI tools, organizations need to take a proactive approach. They should conduct thorough risk assessments to understand their exposure and ensure that appropriate security measures are in place, such as encryption, access controls, data leakage protection, and active monitoring. Proper policies must be defined and approved. Until such policies and controls are in place, the use of ChatGPT and similar tools must be blocked—just as they would (or should) any other non-approved IT system.

Though powerful and seemingly useful, organizations must not allow ChatGPT and similar tools access to their systems and data until they can clearly understand the risk inherent in them and can control against or accept those risks. And, as AI and technologies like ChatGPT and Bard are evolving at a lightning pace, continuously securing these iterations will certainly provide new challenges for both organizational IT and security researchers.

There continues to be much debate about the risk vs. reward of AI/AGI in enterprise settings. Clearly, a tool that produces instant data, content, and analysis provides value; whether the risks can be contained, controlled, and managed to a sufficient degree to justify these rewards will be tested over time. Just like any other tool, AI's effectiveness and impact must be weighed. Organizations need to separate hype from reality before even considering the use of these tools. After all, an OpenAI spokesperson recently commented on its product's ability to "hallucinate" and "make up information that's incorrect but sounds plausible."

While the fear of AI evolving into Terminator or Skynet is certainly fun to hypothesize, the immediate risk is to today's data and customers' networks. Therefore, it is essential to prioritize data security to protect our organizations and the clients we serve.

About the Authors

John A. Smith is CEO of Conversant Group and its family of IT infrastructure and cybersecurity services businesses. He is the founder of three technology companies and, over a 30-year career, has overseen the secure infrastructure design, build, and/or management for over 400 organizations. He is currently serving as vCIO and trusted advisor to multiple firms.

A passionate expert and advocate for cybersecurity nationally and globally who began his IT career at age 14, John Anthony is a sought-after thought leader, with dozens of publications and speaking engagements. In 2022, he led the design and implementation of the International Legal Technology Association's (ILTA's) first annual cybersecurity benchmarking survey.

John Anthony studied Computer Science at the University of Tennessee at Chattanooga and holds a degree in Organizational Management from Covenant College, Lookout Mountain, Georgia.

John can be reached at @ConversantGroup on Twitter and at Conversant's website: https://conversantgroup.com/