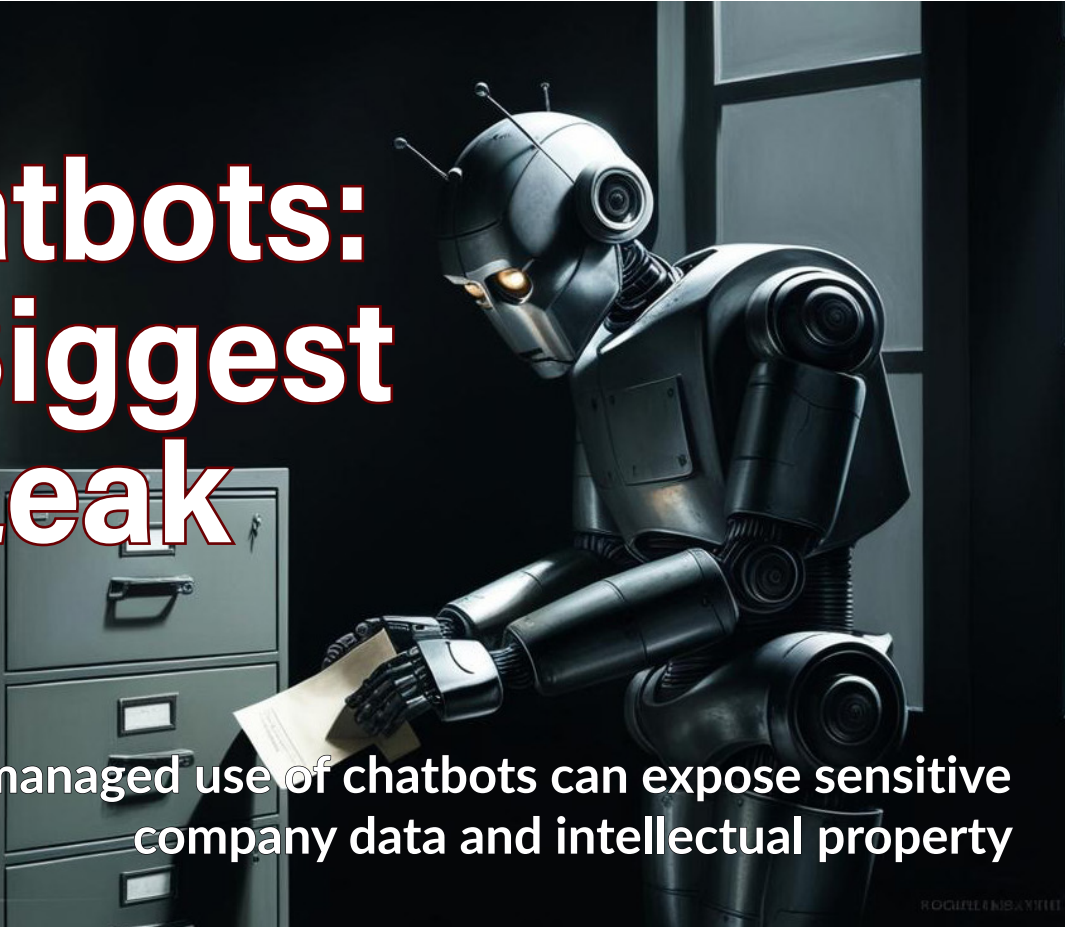


AI Chatbots: Your Biggest Data Leak



Unmanaged use of chatbots can expose sensitive company data and intellectual property

Business System Solutions is your IT Service Partner who provides peace of mind through guidance, education, and responsive support. We are the Caretakers of Your Productivity.



With Offices in:

North Central Indiana
(765) 742-3440

Middle Tennessee
(615) 819-0600

West Michigan
(616) 776-0400



info@bssconsulting.com

"Jesus replied: 'Love the Lord your God with all your heart and with all your soul and with all your mind.' And the second is like it: 'Love your neighbor as yourself.'"
Matthew 22:37,39

by Anisa Williams, BSS Staff

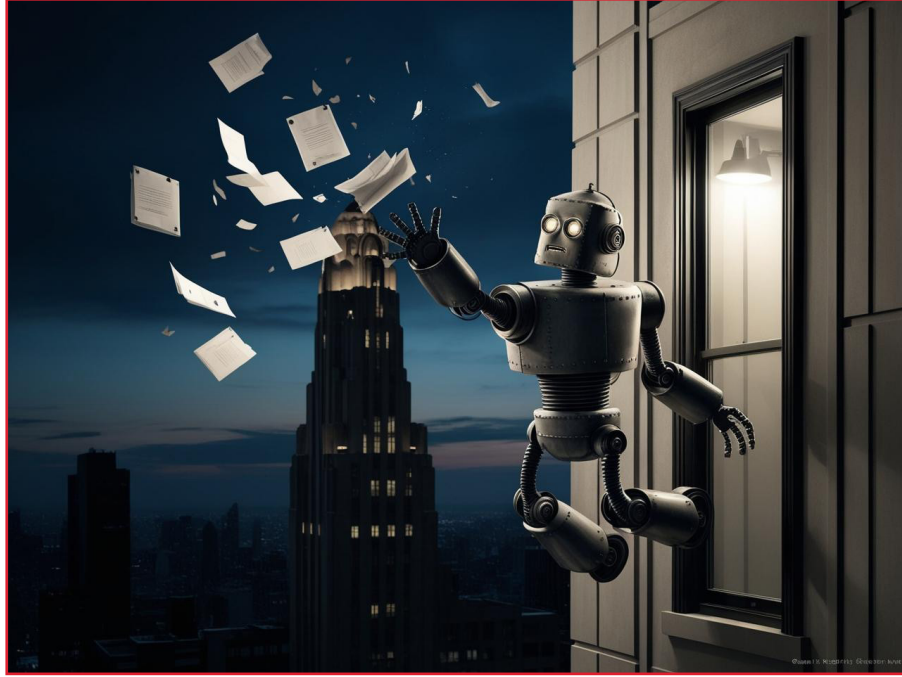
Generative Artificial Intelligence (AI) is rapidly transforming workplaces, offering many new tools and ways to be more efficient. However, this revolution also brings new risks, particularly when it comes to sensitive data and intellectual property.

A 2024 report by ISACA, a global association of IT professionals, reveals the extent of the AI problem. It states that while many organizations are eager to adopt AI, they may not be fully prepared to address the potential dangers. The crux of the issue is that most businesses who use AI are not thinking of the security or implications of sharing sensitive company data with third party chatbots.

Data Privacy and Security Risks

One of the primary risks is the exposure of sensitive or confidential data. Some employees don't think twice about firing up Midjourney, Gemini, or ChatGPT to help them create a slide deck or turn a meeting transcription into usable notes. However, their sharing data with unvetted, third parties means that your company's data may be shared with other people and companies using the same platform.

Additionally, should a threat actor use those platforms for research or hacking, there is nothing stopping the chatbot from sharing your uploaded data. The AI can't know if the files that your employee uploaded are considered confidential or sensitive. Threat actors research their targets to exploit weaknesses in both the chatbot systems or to find vulnerabilities and valuable information on their target.



Intellectual Property Concerns

Another significant concern is the protection of intellectual property. If your employees are not entirely familiar with what data qualifies as intellectual property, you could be opening your company to a major loss in both money and ownership.

Dr. Keegan Caldwell of the Caldwell Law firm said “Once your intellectual property is available online, it becomes part of the extensive dataset from which AI systems draw their knowledge. This could potentially lead to unintended use or replication of your ideas.”

AI-generated content can blur the lines of ownership and copyright. If a third-party AI system is trained on your proprietary data, the resulting output may raise questions about who owns the rights to that content, especially if your competitors are using the same chatbot.

Brands, Trademarks, and Copyrights

Additionally, there's the risk of AI being used to infringe on existing trademarks, copyrights, and other branded materials. Since AI is often trained on copyrighted and social media materials, it can't help but generate content that closely resembles that copyrighted content. For example, when searching for “super hero metal man,” many of the image results show a hero that is eerily similar to Marvel's Iron Man[™]; lawsuits are currently pending for that issue.

Caldwell mentions that differentiating between original, human-created works and AI-derived works will increasingly become more difficult to parse, leaving companies open to legal ambiguity and increased legal fees while companies attempt to prove their original work.

There is another insidious aspect of copyright that companies are not considering: many of the design-based applications that use AI generators explicitly state in their terms that any design or image made in their app cannot be copyrighted and/or is creative commons usage. So, if you're using Canva or Adobe Express to create a company or brand logo, you won't be able to register that mark or brand as the platform owns the copyright.

Company-Driven Policy

To mitigate these risks, organizations must immediately adopt a multi-pronged approach to the implementation and use of AI by its employees. This includes:

- **Selection of AI programs:** Like any software, AI tools must be vetted and reviewed by stakeholders before implementation on an enterprise level.

- **Data Privacy and Security:** Some AI systems, such as Microsoft's Co-Pilot, store uploaded files and conversations within a company's own SharePoint or other fileshare system. Review where AI chats are inevitably stored and the security, encryption, deletion rights, and access controls available to you. Regularly review the AI terms and conditions regularly.
- **AI Security:** Perform regular audits to make sure your policies and security access controls are still relevant, especially after major software updates. Also review the questions and files that your employees are sharing with the program to ensure your IP or copyrighted materials are not being uploaded.
- **Intellectual Property & Copyright Protection:** Train your employees at every level how to recognize your company IP, brands, copyrights, and trademarks. Set clear policies about not creating, sharing, or uploading that data with unauthorized AI programs.
- **Employee Training & Policies:** Educate your employees about the risks and responsible use of AI, especially as it pertains to sensitive or confidential information. Create strong policies and documentation of appropriate employee use and limitations.

By taking these steps, your company can harness the power of AI while minimizing the risks. Begin having the conversations now about how to minimize sensitive data leaks since it looks like AI is here to stay. □

Sources: <https://www.isaca.org/about-us/newsroom/press-releases/2024/the-ai-reality-new-research-from-isaca-identifies-gaps-in-ai-knowledge-training-and-policies>
<https://www.forbes.com/councils/forbesbusinesscouncil/2024/08/20/how-ai-can-affect-intellectual-property-and-what-it-means-for-leaders/>
<https://www.morganlewis.com/pubs/2024/07/ai-in-the-workplace-the-new-legal-landscape-facing-us-employers>
<https://www.tripwire.com/state-of-security/brief-look-ai-workplace-risks-uses-and-job-market>

The End of Windows 10 Looms Large for Small Biz Owners

Are you ready for the October 2025 deadline?

Business owners are reeling with the unexpected costs of having to replace or upgrade nearly all of their staff computers before the dreaded October 2025 End of Support for any computer running Windows 10 operating systems.

Windows 10 computers will still work after October 1, however important security features will stop being supported, making the device more vulnerable. If the computer has specifications that allows an upgrade, owners should work with IT Support to upgrade. However, if the computer is too old, the computer will require replacement.

Supply Chain Challenges: Supply levels around the world are holding steady for now, but our Procurement Department is expecting a run on desktops and laptops as we get closer to the October 1 deadline. Prices are expected to rise on computers. Deliveries may be delayed as budgets are renewed January 1 prompting orders, as well as the challenges of chip manufacturing in recent years.

It's time to start thinking about how to get your employees upgraded computers before your company becomes more vulnerable to threats and hacking. Your BSS Account Manager can put a game plan together while computers are still available. □



Return Address:
601 3-Mile Road NW, Suite C
Grand Rapids, MI 49544

The BSS ADVISOR

info@bssconsulting.com

North-Central Indiana Office
1211 Cumberland Avenue
West Lafayette, IN 47906
(765) 742-3440

Middle Tennessee Office
1026 West College Street
Murfreesboro, TN 37129
(615) 819-0600

West Michigan Office
601 3-Mile Road NW, Suite C
Grand Rapids, MI 49544
(616) 776-0400



Holiday Closures

Christmas

12/24 - CHRISTMAS EVE

12/25 - CHRISTMAS DAY

OnCall Support is available 24/7 during holidays. For emergencies, please call our main office numbers.

New Years

1/1 - NEW YEAR'S DAY

Emails sent to Support will be handled the next business day.