

The Hidden Cybersecurity Risks of Workplace AI:

How Businesses Can Protect Sensitive Data While Taking Advantage of Artificial Intelligence

By Richard Preston, Preston Office Solutions

Artificial intelligence (AI) is becoming an increasingly common tool in today's workplace. Employees use it to draft emails, summarize reports, analyze spreadsheets, write marketing materials, troubleshoot technical problems, and automate repetitive tasks. Many businesses are exploring AI because it can help employees complete certain tasks more efficiently.

For business owners who haven't explored AI, think of it as an intelligent digital assistant. You ask it questions or give it a task, and within seconds it can generate written content, organize information, analyze data, brainstorm ideas, or even write computer code.

It's important to remember, however, that AI is not a person, nor does it "know" information the way humans do. It generates responses by recognizing patterns in enormous amounts of data. While it can be remarkably helpful, it can also make mistakes, misunderstand instructions, or produce inaccurate information. For that reason, AI-generated work should always be reviewed by a knowledgeable person before it is relied upon or shared.

At the same time, many people don't realize that using public AI tools can create cybersecurity risks if confidential business information is entered into them.

According to a January 2026 report from BlackFog, 86 percent of employees use AI at least weekly for work-related tasks, and nearly half admit using AI without employer approval. Those numbers suggest that AI adoption is happening faster than many workplace policies can keep pace.

Businesses have spent years strengthening their cybersecurity defenses through firewalls, multifactor authentication, endpoint protection, email security, encrypted backups, and continuous network monitoring. However, even the strongest cybersecurity defenses can be undermined if employees enter confidential customer information, financial records, legal documents, proprietary business processes, or other sensitive data into public AI platforms.

"Organizations have worked incredibly hard to secure their networks and protect financial records, employee information, and customer data," says Richard Preston, president and CEO of Preston Office Solutions. "The challenge now is that employees are using AI tools independently, often without realizing the potential consequences of where that information may be going."

Not all AI systems are designed the same way. Many people are familiar with public AI tools that are freely available online. Some organizations, however, choose AI platforms designed specifically for business use because they offer additional administrative controls and privacy features, such as encryption, user permissions, audit logs, and security settings that help protect confidential information.

"The majority of your staff are already utilizing AI in some form, whether employers officially approve it or not," Preston says. "That means they need to understand the liabilities they can inadvertently expose the business to when using these tools."

Practical Steps Every Business Can Take

Whether your organization has five employees or five hundred, developing guidelines for AI use is becoming an important part of protecting your business.

Consider these best practices:

- Develop a written policy outlining appropriate AI use.
- Train employees on what information should never be entered into public AI tools.
- Avoid entering confidential customer, financial, legal, medical, or proprietary business information into public AI platforms.
- Review AI-generated work before sharing it or using it to make important business decisions.
- Consider using AI platforms designed for business when handling sensitive information.
- Review cybersecurity policies regularly as AI technology continues to evolve.

"AI has quickly become one of the most powerful productivity tools ever created," Preston says. "But the organizations that succeed long term won't necessarily be the ones using the most AI. They'll be the ones using it securely, responsibly, and strategically."

Whether an organization chooses to adopt AI today or in the future, business leaders should understand both its capabilities and its risks. Like any technology, AI requires thoughtful policies, employee training, and appropriate safeguards. Organizations that take the time to establish clear expectations will be better prepared to protect sensitive information while making informed decisions about how AI fits into their operations.

For more information about how to protect your business, visit prestonoffice.com, call (435) 628-2997, or email admin@prestonoffice.com.



Prosperity & Purpose

ABOUT THE AUTHOR

Richard Preston, owner and CEO of Preston Office Solutions in St. George, Utah, has been a trusted name in business technology for over forty years. Under his leadership, Preston Office Solutions has earned a solid reputation for exceptional sales, service, and support of office multifunction printers and large-format printing products across Southern Utah and southern Nevada. Preston Office Solutions is more than just a print solutions provider. As a dependable IT partner, the company delivers a comprehensive suite of technology products and services—all designed to support the success and growth of every client. To learn more, contact Preston Office Solutions at 435-628-2997 or visit www.prestonoffice.com.