

Shadow AI and the Risks of Employees Using Unapproved AI Tools

Artificial intelligence (AI) can help employees summarize documents, analyze data and complete other routine tasks. However, workers may adopt AI tools before their employers can properly evaluate and govern them. This can lead to shadow AI—the use of AI tools or accounts that an organization has not approved. Although employees typically turn to these tools to save time or meet productivity demands, unapproved AI use can create serious cybersecurity, privacy, regulatory and intellectual property risks.

Understanding Shadow AI Risks

Employees may enter source code, customer information, contracts, financial records or HR files into public AI platforms without knowing how the providers store, process or reuse that data. Some platforms retain prompts or rely on third-party infrastructure, placing sensitive information outside the organization's control.

Shadow AI may expose organizations to the following risks:

- **Data breaches**—Sensitive information entered into an unapproved tool could be improperly accessed, retained or disclosed.
- **Privacy and compliance violations**—Sharing personal or protected information may violate privacy laws, industry requirements or internal policies.
- **Contractual breaches**—Customer contracts, confidentiality agreements and other arrangements may restrict the disclosure of information to third parties, including AI providers.
- **Intellectual property loss**—Uploading proprietary data, source code or trade secrets could compromise ownership or confidentiality.
- **Financial and reputational harm**—An incident may trigger forensic investigations, legal expenses,

regulatory inquiries, customer notifications and remediation costs. It may also erode customer trust.

Insurance Considerations

AI-related losses may create coverage uncertainty. Although cyber insurance has historically responded to some AI-enabled data breaches, insurers are increasingly adding AI-specific language and exclusions to various policies. Organizations should review their entire insurance program—not only cyber coverage—for AI-related limitations or gaps.

Reducing Shadow AI Exposures

Organizations can take these steps to manage unapproved AI use:

1. **Inventory AI tools.** Identify the tools employees use and the business needs they address.
2. **Establish a written policy.** Specify approved tools, acceptable uses and the types of information employees may share.
3. **Offer approved alternatives.** Providing secure tools that meet legitimate business needs may reduce employees' incentive to seek unauthorized options.
4. **Vet vendors.** Review vendors' security controls, privacy practices, retention policies and contract terms, including whether prompts are used to train models.
5. **Implement safeguards.** Use access controls, network monitoring and data loss prevention tools to detect and limit unauthorized activity.
6. **Train employees.** Explain AI's risks and limitations and employees' responsibilities for safeguarding organizational data.

Your Risk Transfer Resource

Shadow AI can turn a seemingly routine shortcut into a costly cyber incident. For more information about managing AI-related risks and reviewing applicable insurance coverage, contact us today.

Managing Lithium-ion Battery Storage Systems

Lithium-ion battery energy storage systems can help businesses manage peak demand, maintain backup power, reduce utility costs and support solar power or electric vehicle charging. These installations may range from modular indoor racks to large outdoor enclosures.

Although battery storage systems offer significant benefits, they can also create serious fire and explosion hazards. Improper installation, insufficient maintenance or damaged components may result in extensive property damage, injuries and prolonged business interruptions.

Understanding Thermal Runaway

The primary hazard associated with lithium-ion battery storage systems is thermal runaway. This chemical reaction often begins when overcharging, short-circuiting or another failure causes a battery cell to generate heat rapidly. As the cell fails, it may release heat and toxic gases faster than they can dissipate.

The reaction can spread to nearby cells, creating extremely hot fires and combustible gas buildup. Conventional water-based fire suppression systems may not fully extinguish these fires, which can reignite hours or days later. In some cases, accumulated gases may contribute to an explosion.

Thermal runaway can occur in indoor mechanical rooms or outdoor installations and may affect connected equipment, including solar panels, electric vehicle charging stations, forklifts and other material-handling equipment.

These incidents can destroy buildings, equipment and inventory while exposing employees, emergency responders and nearby occupants to heat, smoke and toxic gases. Cleanup, investigation, repairs and system replacement may also suspend operations for an extended period and increase the total cost of a loss.

Reducing Battery Storage Risks

Businesses should consider the following safeguards:

- **Follow applicable codes and standards.** Confirm that system components comply with Underwriters Laboratories Standard 9540 and that configurations have passed UL 9540A thermal runaway testing.

Follow National Fire Protection Association Standard 855 and all locally adopted building and fire codes regarding system design, installation, spacing, maintenance and decommissioning.

- **Install supporting safety systems.** Use ventilation, gas detection and fire suppression systems appropriate for the batteries' chemistry, size and configuration. A dedicated battery management system should monitor temperature, voltage and charge levels so personnel can address abnormal conditions promptly.
- **Schedule inspections and maintenance.** Follow manufacturers' recommendations and document all inspections, maintenance and repairs. Trained personnel should perform inspections, while qualified contractors should complete repairs. Establish relationships with contractors before an emergency to help ensure timely service.
- **Coordinate with the fire department.** Invite local fire officials to review the installation and its hazards. Incorporate their recommendations into an emergency action plan that addresses thermal runaway, evacuation and specialized fire suppression tactics.
- **Train employees.** Teach employees who work near the system to recognize warning signs, such as bulging components, unusual hissing sounds, odors or excessive heat. Workers should also understand alarm procedures, evacuation routes and emergency response expectations.
- **Consult insurance professionals.** Review battery storage safeguards and commercial property coverage with a trusted insurance professional. Hazard analyses, code compliance reports, maintenance records, safety policies and emergency action plans can support more productive insurance discussions.

Lithium-ion battery storage systems can improve energy resilience, but their hazards require careful planning and ongoing oversight. For more risk management guidance and information about commercial property coverage for battery-related losses, contact us today.