RISK SPOTLIGHT

# Beyond Firewalls:

## Safeguarding Your Business Against AI-Driven Attacks



**Discover:**

+ The New Wave of AI-Driven Cyber Risks
+ How Cybercriminals Use Your Technology Against You
+ The Business Impact of AI-Powered Threats
+ Are You Overconfident in Your Cybersecurity?
+ How Businesses Can Control AI-Powered Cyber Risks
+ Cyber Insurance as a Strategic Safeguard

WATKINS
INSURANCE GROUP




AI has unleashed a new wave of cyber risks. While businesses are becoming increasingly reliant on technology systems, bad actors are using AI to launch more sophisticated attacks in less time. We've reached an inflection point, and to prevent this from turning into disaster, businesses need to protect themselves against the growing risk.

## The New Wave of AI-Driven Cyber Risks

Cyberattacks have been making news for years now, but AI agents have upped the ante.

AI agents, like all other technologies, are inherently neither good nor bad. Legitimate businesses can use AI agents to automate processes, free up resources, and increase operational efficiency. Unfortunately, hackers can do the same. Bad actors can use AI agents to write and distribute highly convincing social engineering and to carry on conversations with anyone who replies, allowing them to scale their attacks in ways that were not previously possible.

Verizon's 2025 Data Breach Investigations Report found that AI-assisted malicious emails have doubled over a period of just two years as generative AI tools became widely available.

The implications go beyond phishing and business email compromise. Cybercriminals can also use AI agents to search for and exploit vulnerabilities and to create and carry out cyberattacks. According to Gartner, AI agents can automate credential theft, and they are poised to reduce the time it takes to exploit account exposures by 50% by 2027.

## How Cybercriminals Use Your Technology Against You

Businesses are investing in AI, and cybercriminals are investing in ways to exploit these efforts. Here are four tactics being used now:

+ **Adversarial Machine Learning.** In machine learning, computer systems are capable of learning on their own from the training data with explicit programming. In adversarial machine learning, bad actors manipulate this process to corrupt the system.
+ **Data Poisoning.** AI models are capable of incredible feats, but the results are only as good as the data used to train them. In data poisoning attacks, bad actors inject inaccurate or misleading data into a model's training set to sabotage it.
+ **Prompt Injection.** AI chatbots can be tricked into providing outputs that should be prohibited using prompt injection techniques. With prompt injection tactics, bad actors create deceptive prompts designed to manipulate AI programs into revealing sensitive information or other off-limits outputs.
+ **Data Seepage Exploitation.** In a data breach, thousands or even millions of records may be exposed in a single cyberattack. However, not all data vulnerabilities occur this way. Sometimes, data is exposed inadvertently and over an extended period before the issue is caught. This is known as data leakage, and the term data seepage may be used for gradual leaks.

## The Business Impact of AI-Powered Threats

In the wake of a cyberattack, businesses often face costs associated with data loss, computer system damage, forensic investigation, and consumer notification. They may also incur significant business disruption, IP theft and reputational harm.

Cyber incidents can be tremendously expensive.

+ The average cost of a ransomware attack has increased from $705,000 in 2024 to more than **$1.18 million** in 2025, according to Resilience's 2025 Midyear Risk Report.
+ The average cost of a data breach has reached **$4.88 million,** according to IBM.
+ The average business email compromise claim has reached **$35,000,** according to Coalition's 2025 Cyber Claims Report.

## Are You Overconfident in Your Cybersecurity?

Three vulnerabilities can make businesses more vulnerable to cyber incidents than they realize.

+ **Third-Party Vendors.** If your cybersecurity is excellent but your vendors' cybersecurity is subpar, you're still vulnerable to attacks, breaches and outages.
+ **Open-Source Models.** Many businesses rely on open-source models. While these tools can be sophisticated and cost-efficient, they can also be vulnerable to data poisoning and other types of cyberattacks.
+ **Employees.** CalypsoAI's Insider AI Threat Report found that 52% of U.S. workers say they are willing to use AI to make their jobs easier, even if they have to violate company policy to do so.

## How Businesses Can Control AI-Powered Cyber Risks

The cyber threat landscape is evolving, and cybersecurity practices need to keep up. Many businesses are fighting fire with fire by using AI in cybersecurity.

Here are three more actions that can help:

+ **Map AI use across the organization.** The rapid adoption of AI has been chaotic for many companies. If you don't know exactly how your organization is using AI, you can't control the associated risks.
+ **Vet vendors and implement stronger supply chain oversight.** You are only as strong as your weakest link. Choose your vendors carefully, use strong contracts that spell out cyber and liability issues, and have backup plans.
+ **Create and enforce workable AI policies.** Many workers are using AI tools, sometimes without their employer's knowledge. Businesses need to get ahead of this by creating clear policies on AI usage.

# Cyber Insurance as a Strategic Safeguard

Cyber insurance for businesses provides a final line of defense against cyberattacks. As threats increase, so does the need for coverage. In addition to helping businesses respond to cyberattacks, insurers can also provide resources to help businesses prevent attacks and minimize damages.

However, cyber coverage can vary, and some insurers are introducing terms that limit or exclude coverage for AI-related losses. Review your coverage to see how it handles adversarial machine learning, AI agent errors, data seepage and other emerging AI risks.

An insurance advisor who understands the intersection of AI and insurance can guide you through this process and help you understand your coverage.

Don't wait for a cyberattack to hit your business. Take control of your business risk management and AI risks now.

+ Review AI use within your business.
+ Establish governance frameworks to minimize emerging risks.
+ Partner with a broker to evaluate cyber coverage in light of AI exposures.

Watkins Insurance Group can help you understand your risks, coverage needs and insurance options. Contact us for a review of your cyber insurance coverage.



WATKINS
INSURANCE GROUP