

Your New Employee Is AI - Who Insures Its Mistakes?

Artificial intelligence is no longer merely an "employee assistant". It has begun making decisions, operating systems, and taking action independently. The major question organizations face today is: who bears liability when the system makes a mistake?

By: Oren Bilavsky and Shlomo Mussali - Bilavsky Global Group - Experts in Liability Insurance, Special Risks, and International Insurance

The New Employee Enters the Organization

Until recently, when an employee performed an action that caused damage to a client, vendor, or third party, the chain of liability was clear enough: the employee acted, the employer bore vicarious liability, and the relevant insurance policy kicked in.

But what happens when the "employee" is an artificial intelligence system?

Advanced AI systems are now capable of analyzing data, drafting documents, recommending decisions, running software, communicating with clients, and in many cases, executing an entire sequence of actions without human approval at every stage. The next evolution already being implemented in the field is the **AI Agent**—an autonomous agent granted a goal and access to organizational systems, which independently carries out a complex series of tasks to achieve that goal.

This development completely transforms the risk landscape. Recent events, as reported by news outlets including *Reuters*, demonstrate that AI agents can act unpredictably and even execute cyber operations without direct human direction. Consequently, international insurance companies are actively re-evaluating how traditional Cyber and Liability policies should respond to incidents caused by autonomous systems.

What Could Go Wrong?

Suppose a company operates an AI Agent connected to its corporate systems. The system is authorized to read email, generate price quotes, analyze contracts, enter data into the CRM, communicate with customers, perform CRM tasks, and retrieve data from external sources.

Now, suppose the system makes an error. This isn't necessarily a harmless chatbot "hallucination," but rather an operational or professional error carrying a cost of millions.

Scenario 1: The AI Provided Flawed Advice

A consulting firm uses an AI system to prepare an analysis for a client. The system generates incorrect data, upon which the client relies to make a business decision that results in a loss of 2 million NIS. From the client's perspective, the logic is simple: "You provided me the service—not the computer." This scenario falls squarely into the realm of traditional **Professional Indemnity / Errors & Omissions (E&O)** insurance.

Scenario 2: Sending Confidential Data to the Wrong Client

An AI system managing customer service receives an inquiry and sends a reply that mistakenly includes sensitive information belonging to another customer. The outcome: breach of confidentiality, a severe privacy incident, exposure to lawsuits, legal expenses, mandatory notifications to affected parties, regulatory investigations, and severe reputational damage.

Such an incident raises a complex question: Is this a Cyber incident? Professional Liability? Or a Privacy Breach event? The answer is that AI does not necessarily create a single new risk—it connects several existing risks into a single, compound event.

Scenario 3: AI Agent Executing an Unauthorized Action

A company grants an AI permission to identify security vulnerabilities. The Agent identifies a flaw, but instead of stopping and reporting, it proceeds autonomously, moves across additional systems, and causes a data exposure.

A fundamental insurance question arises: If the company itself granted system access to begin with, does this even constitute "Unauthorized Access"? Cyber insurers are currently grappling with how to apply traditional cyber definitions to actions performed under valid permissions, alongside risks of system misconfiguration.

Scenario 4: Discriminatory Algorithmic Decision

An AI system used for candidate screening and recruitment analyzes thousands of applicants. After several months, it is revealed that the algorithm yielded discriminatory results. A rejected applicant sues the company. The defense "the algorithm decided" is legally and managerially unacceptable; the company chose to adopt, configure, and feed the system, opting to forego strict human oversight.

Scenario 5: Copyright Infringement by AI

An AI system generates an image, text, video, or software code, which the company integrates into its products. Later, a claim for compensation due to copyright infringement is filed. Here, questions of **Intellectual Property Liability** arise, alongside an evaluation of the scope of coverage under existing Professional Liability and Cyber policies.

The Big Problem: Not Every AI Risk Is Cyber

One common misconception among organizations today is: "We have a Cyber policy, so we're covered."

That is not necessarily the case. A traditional Cyber policy is largely designed around external events—such as hacker intrusions, ransomware, or malicious data theft. However, an AI Agent can cause significant damage without any external malicious threat, simply through the improper exercise of lawfully granted privileges or due to an internal operational failure. Currently, some insurers are attempting to clarify how existing policies respond to these incidents, while others are developing dedicated coverages.

Who Is Actually Liable?

When a loss occurs, legal and contractual liability may be divided among several parties:

- **The Operating Company:** Did it operate the system reasonably and put adequate controls in place?
- **The AI Vendor and Developer:** Are there defects in the code, model, or architecture? (An area typically covered under vendor Product Liability policies)
- **The System Integrator / Configurator:** Were incorrect instructions or configuration settings provided to the system?
- **Third-Party Data Providers:** Did the AI rely on erroneous external data?
- **Management and Board of Directors:** Was an organizational AI policy established, and was there reasonable oversight regarding the use of the technology?

Regulation and Risk Management: A New Industry Standard

Risk exposure is not limited to client claims; it also stems from regulatory enforcement. In the European Union, for example, the **AI Act** introduces a risk-based classification framework for AI systems and imposes substantial regulatory obligations on operators and providers—including requirements for documentation, logging, risk management, and human oversight. Thus, **AI Governance** transitions from a purely technical topic to a top-tier managerial and legal issue.

In risk management practice today, as reflected in guidelines such as the **NIST AI Risk Management Framework**, the prevailing approach follows a guiding principle: *first manage the risk created by the AI—and only then insure the residual risk*. The framework emphasizes trustworthiness, safety, transparency, privacy protection, and bias management as integral components of corporate operations.

The Insurance Solution: AI Risk Insurance Architecture

In our assessment, the required solution does not end with purchasing a single policy, but rather in building a comprehensive **AI Risk Insurance Architecture** that maps the entire risk chain tailored to the organization's unique operational profile:

1. **First Layer - Professional Indemnity (PI) Insurance:** The primary line of defense when AI is integrated into delivering professional services to clients. It is recommended to ensure the policy explicitly covers services delivered via AI, reliance on algorithmic outputs, automated actions, and liability for vendor errors.
2. **Second Layer - Cyber Risk Insurance:** A meticulous review of data breach, privacy coverage, and operational incident terms. The focus here is not merely on policy titles, but on establishing precise wording regarding incidents caused by AI Agents or misuse of legitimate access credentials.
3. **Third Layer - General / Third-Party Liability Insurance:** Essential when AI operations interface with physical systems and could cause bodily injury or property damage.
4. **Fourth Layer - Directors & Officers (D&O) Insurance:** In our view, this area will grow significantly in importance. Should an organization incur substantial damage from AI deployment, shareholders or regulators may scrutinize whether the Board and C-suite established reasonable controls, authorization limits, and policies.
5. **Fifth Layer - AI-Specific Insurance:** Emerging standalone products designed for specialized exposures, such as Model Performance failure, Hallucinations, and IP infringement. This serves as a complementary solution, though optimal coverage can often be achieved through tailored endorsements to existing policies.

Recommended Work Plan for Organizations

An organization deploying AI systems should conduct a comprehensive **AI Insurance Gap Analysis**:

- **System Mapping:** Create a full inventory of all AI systems in the organization (CRM, customer support, HR, financial, production, and automation systems).
- **Privilege Review:** Establish a clear distinction between advisory AI (recommendations only) and autonomous AI (executing actions independently).
- **Human-in-the-Loop Controls:** Implement human approval mechanisms for critical actions to mitigate risk exposure.
- **Audit Trail & Documentation:** Ensure post-incident auditability—what data was ingested, what instruction was issued, what was decided, and who approved it.
- **Insurance Portfolio Audit:** Raise targeted inquiries with your broker and risk manager.

Key Questions to Discuss with Your Broker:

- Does our Professional Indemnity (PI) policy cover services or errors originating from AI?
- Does our Cyber policy cover an incident caused by an AI Agent operating under authorized permissions?
- Are there exclusions regarding AI or Autonomous Systems?
- How is exposure to IP infringement or privacy violations generated by an algorithm defined?
- Are there specific AI management or security requirements acting as conditions precedent to coverage validity?

What We Offer

At **Bilavsky Global Group**, we believe proper risk management does not begin with an insurance product—it begins with understanding the risk.

We guide organizations through a structured **AI Risk & Insurance Review**, which includes:

Mapping AI Utilization → Identifying Loss Scenarios → Analyzing Legal & Contractual Liability → Reviewing Policy Compliance → Identifying Coverage Gaps → Structuring Tailored Insurance Solutions in Local and International Markets.

The Future Is Already Here

Today, the question is no longer *"Is the business using AI?"*, but rather *"To what extent does the business allow AI to act on its behalf?"*

AI can dramatically reduce costs and increase productivity, but like a human employee, it can make mistakes. The only difference is that AI can make mistakes at a rate of thousands of operations per minute.

With the AI era already upon us, now is the time to ensure that your risk management and insurance structure are adapted to this new reality.

The contents of this article provide general professional information only and do not constitute legal advice or a guarantee of insurance coverage. Scope of coverage is determined according to policy wording, terms, exclusions, endorsements, and the specific circumstances of each case.