expert.ai

Managing and Mitigating

Silent Cyber Risk with NLP





Cyber insurance is undoubtedly the fastest growing sector of the insurance industry. According to FitchRatings, standalone cyber coverage, which represents approximately two-thirds of industry premiums, increased by 92% in 2021, as the frequency and severity of cyberattacks led more insurance clients to view cyber coverage as a necessity than a luxury.

However, the challenge of cyber insurance extends beyond market demand. There's also the claims side of the insurance equation and the "silent cyber" issue — the risk that insurers have absorbed in claims due to ambiguous cyber policy coverage terms or no cyber coverage at all.

Silent cyber risk is growing at an alarming rate. The Allianz Risk Barometer survey ranked cyber incidents as the most significant risk for businesses. A recent study by cyber risk analytics firm Cyber Cube projects losses from silent cyber to reach $12.5 billion in the United States market alone.

For insurers to move from a cyber silent to cyber affirmative position at the portfolio level, proper risk assessment is crucial and requires facing two core challenges:

- **Understanding as-is cyber exposure**
- **Evaluating the contract certainty of all new and existing policies**

The question is, how? That's where natural language processing (NLP) solutions come in.

Four Pillars of a Successful Cyber Solution

What does every successful cyber solution have in common? They each factor in the following four variables:

- **Technology**
- **Data**
- **People**
- **Process**

In a sense, each variable represents a pillar of the final solution because any weakness in one, or complete lack of presence, will render the solution useless. However, with careful consideration of the whole, immense value can be realized.

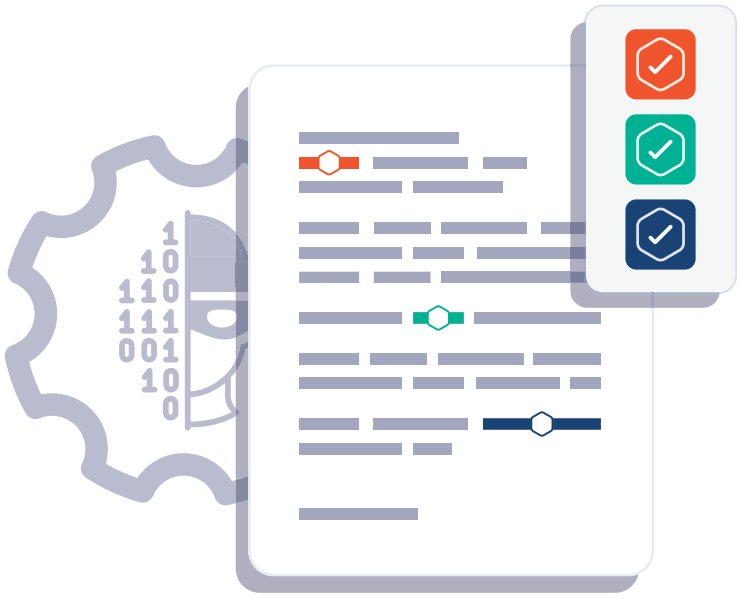
Technology

Policy review is a tedious and time-consuming process. Not only are policies lined with complex and nuanced language, but each one is often unique from the next. If you add new and unfamiliar cyber terminology to the equation, the process becomes that much more challenging.

Core to the issue here is that policy review is typically a manual process. It can take an underwriter hours to complete a single review due to the document complexity and length. That is not a scalable process, and it highlights the need for an automated technological solution. However, for technology to add any real value, **it must be able to understand the language within these policy documents**.

Natural language processing technology is core to any worthwhile policy review solution. It enables you to read and analyze complex policy documents and extract the information you need to understand your cyber exposure.

By extracting these elements, you have the information you need to evaluate contract readiness, identify potential red flags and make timely adjustments. In addition, this information enables you to clearly classify your contracts to better organize them for future use. This is beneficial for both comparison and search capabilities (more on these to come) as it enhances the information you know and can leverage for current analysis.



Data

The accuracy and quality of your data plays a key role in the success of your claims automation process. One of the most common reasons for data issues stems from poor version control. If you are processing outdated policies in large volumes, you leave yourself vulnerable to significant risk. This makes data governance critically important to the success of your model.

Key to effective data governance is making data accessible across your organization. You can accomplish this by creating a central repository for all current documents to live. This not only helps to eliminate data silos, but it ensures data quality across your organization. As a result, when you re-evaluate existing policies, you can be sure your model extracts the correct information.

Applying meaning-based understanding allows for more accurate interpretation of concepts. For example, date references like "no more than seven business days after deposit date" can be correctly interpreted. The same goes for payment terms like "early payment, within 60 days, will receive a 3% vendor discount."

By locating important information with a high level of accuracy, you can quickly align new contracts to internal standards. This enables you to **close contracts faster with a high degree of certainty** that core language is addressed.

This capability extends beyond just your gold standard policy as well, as you can compare any number of contracts including a new customer contract to their previous contract or an incoming contract to those archived in your contract database.



People

Policy review has always been dependent on the domain expertise of underwriters. Their expertise enables them to understand the insurance-specific terminology in every policy they review. To successfully automate this process, that expertise needs to be scalable. This can only be achieved with the help of human subject matter experts.

Unfortunately, **subject matter expertise is a scarce commodity**, especially when you factor in the uniqueness of cyber. Thus, it is imperative that you maximize the expertise you have throughout the process from training your model to testing and validating the results. This is even more important when you consider that their help comes at the expense of their day-to-day work**.**



Process

You can have the technology, data and people to effectively automate the claims process, but that can easily be derailed without effective process in place. A good place to start is defining your success criteria. What metrics will you use to evaluate each claim? What elements of cyber need to be monitored?

Once you have established your success metrics, you can set realistic expectations for model performance. **Given the nuance of policy coverages, expecting perfection would only set you up for failure.** To find a more realistic

number, perform a reality check of the whole system with full-volume testing to test the expected outputs. And as time goes on, build ongoing processes to ensure the quality of your model remains at your desired level.



Building Your Cyber Solution with Expert.ai

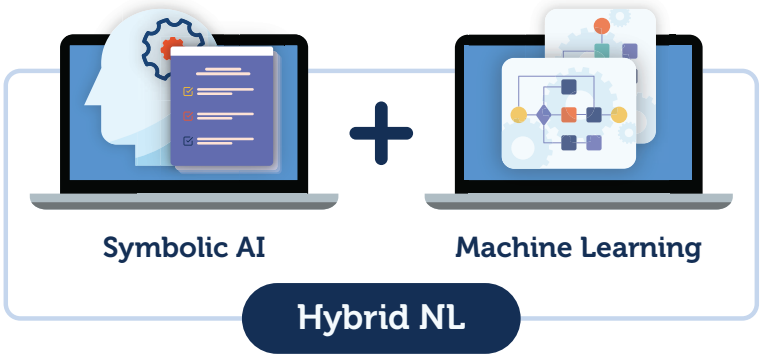
Now that you understand what goes into a viable cyber solution, it is time to put all the pieces together. While you may be capable of doing that yourself, this is a uniquely complex situation that is best left to the experts...or in this case, expert.ai.

Expert.ai built its cyber solution with each of the four pillars in mind. Together, the solution enables insurers to address their cyber challenges with confidence and limit their exposure to legal and financial risk. So, what makes this solution different from the others? Follow along as we break it down for you.

Technology

Artificial intelligence is key to automating cyber challenges such as policy review and claims processing. The key difference for expert.ai is it **relies upon a hybrid approach of symbolic AI and machine learning (ML) to understand the text in language-intensive documents**, rather than pure ML. Therefore, when companies are reviewing existing policies to understand their cyber position, they can do so using context rather than keywords.

Not only does expert.ai automate the most difficult and time-consuming part of policy review, but it enables insurers to compare the extracted information to their established cyber position and categorize the policies accordingly. In distinguishing cyber affirmative policies from those that are not, insurers can more quickly amend policies to their standards.



Data

Insurers need access to specific data points in policies, and they need to easily navigate through that data to accelerate policy reviews. **Expert.ai technology enables insurers to extract those specific data points and use them to accurately label and categorize documents.** This makes it easy for insurers to navigate through policies based on attributes such as the inclusion of specific implicit or explicit coverages, exclusions or endorsements.

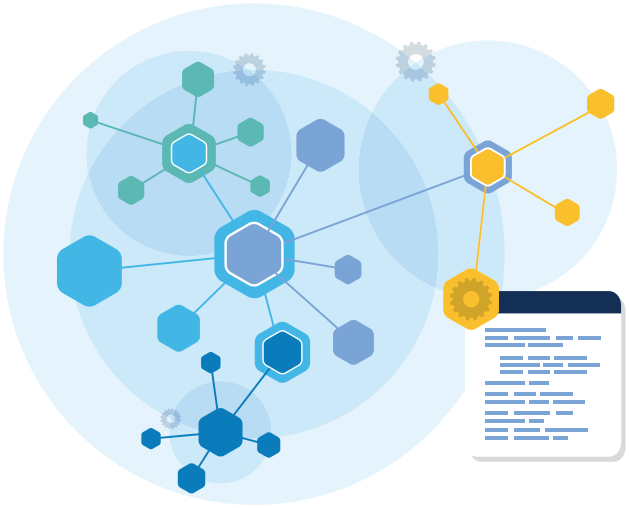
Data organization is key, but it depends heavily on your data governance processes. If your organization cannot maintain proper version control of your policies, any model you use will have significant issues. This is true regardless of the solution you select.

People

Without people, NLP technology cannot attain the knowledge and expertise it needs to truly understand a given topic; especially one as complex as cyber. Expert.ai leverages subject matter experts from the outset to extract their knowledge into knowledge bases that can then be used to train ML models. Given how new cyber risk is to insurers and how little historical data they have to train their model with, **insurers can avoid the data scarcity issue by training their model with the extracted domain knowledge**.

What makes this symbolic, rule-based approach particularly effective is the ability to expand upon knowledge bases as expertise grows. Considering the nascency of cyber to the insurance industry, there are sure to be new terms and

relationships between concepts that a model will need to learn. In being able to make those specific additions to your knowledge base and knowledge graph, you can avoid retraining your model during every instance.



Process

While implementation of specific processes is largely dependent on the insurer, expert.ai can help facilitate many processes due to its experience and technological capabilities. For instance, the selection and measurement of core performance metrics is often challenging because there are no universal benchmarks or best practices in place.

Expert.ai is steeped in knowledge when it comes to policy review and understands exactly what metrics provide the best insight, as well as how to measure them. For instance, accuracy is not as straightforward to measure as it appears. Beyond the binary choice of right or wrong, there are also measurements for recall and precision (together they form the F-score). These are all metrics that expert.ai can both measure for insurers and advise them on regarding benchmarking.

Cyber is extremely nuanced and evolving at a rapid pace. The longer it takes your organization to address the hidden cyber risk in your portfolio, the harder it will be to catch up. Break the silence of cyber with a solution that can stand on its own. Expert.ai is here to help.

Get Started

Unlock the potential of your natural language assets.

See how expert.ai can help!



expert.ai

About us

Expert.ai (EXAI:IM) is a leading company in AI-based natural language software. Organizations in insurance, banking and finance, publishing, media and defense all rely on expert.ai to turn language into data, analyze and understand complex documents, accelerate intelligent process automation and improve decision making. Expert.ai's purpose-built natural language platform pairs simple and powerful tools with a proven hybrid AI approach that combines symbolic and machine learning to solve real-world problems and enhance business operations at speed and scale. With offices in Europe and North America, expert.ai serves global businesses such as AXA XL, Zurich Insurance Group, Generali, The Associated Press, Bloomberg INDG, BNP Paribas, Rabobank, Gannett and EBSCO.

www.expert.ai **info@expert.ai**

©expert.ai 2022