Our Approach

Technology

All Guidewire applications share a commitment to quality and performance

Three principal goals govern how we design and develop all Guidewire products.

Flexible software that must keep evolving

Flexibility means that our customers can change the system according to their specific needs and that they can support a wide spectrum of business operations. This also means flexibility for deployment—by region, line of business, and functional area. “Evolving” refers to the responsibility we have to continually update our technology to deliver value in future versions and ensure that customers have new opportunities for value.

Defining and supporting specific user journeys

We design for the holistic experience that users want to have on their journeys. We ensure that we design to enable this kind of experience, rather than accepting the limits of the status quo and the “the way things have always been done.”

One-mind design

Our development teams work together to address specific user journeys across our products and to ensure that those products work together in a connected way.
The Guidewire technology platform

Guidewire core systems are built on a shared technology platform providing unparalleled performance, reliability, flexibility, and openness. Our platform was designed and built on a completely modern architecture to meet the specific needs of the property and casualty insurance industry.

Guidewire applications are built in Java and conform to the Java EE standard—the preferred technology of the insurance industry.

A 100% web client ensures that no software needs to be installed on end-user desktops.

Web service APIs enable Guidewire applications to integrate seamlessly into a service-oriented architecture and interact with any other applications in any technology.

Clustering, caching, and never-ending performance tuning ensure that Guidewire applications can support thousands of concurrent users.

Guidewire applications run on the insurance industry's preferred application servers, operating systems, and databases.

An unmatched commitment to quality—embodied by more than 120,000 tests that run continuously throughout the development cycle—makes Guidewire applications the most reliable and trustworthy in the industry.

Features and Benefits

The Guidewire platform provides a set of core technology components that provide critical building blocks and services to all Guidewire applications, including the following features:

Rules engine: Combines easy-to-understand, hierarchical rule execution with a rich library of methods specifically developed to meet the needs of modern insurance companies

Business process management: Gives insurers the ability to define long-running insurance processes involving multiple activities and actors, with exceptions and escalations as appropriate

Configuration: Enables insurers to extend the application data model and screens using logical, easily understandable XML files

Integration: Provides a variety of integration mechanisms, including a web services API, event-based messaging, and the ability to add integration adapters at any point in the application; enables the exchange of data in any format, including ACORD XML or IAA

Security: Provides mechanisms for controlling which users have access to an application, what functionality they can use, and what data (accounts, policies, claims, and so on) they can view or edit

Guidewire's technology platform enables insurers to reduce long-term cost of ownership by consolidating on a single suite of applications, resulting in these benefits:

Insurers gain complete control over their core applications due to the extensive configurability of the Guidewire platform, coupled with an insurance-specific rules engine.

Users benefit from responsive, easy-to-use applications, and growing companies can support larger populations simply by adding more servers.

The robust integration layer means that insurers can integrate their core applications with any other systems inside or outside the enterprise.

Insurers can share a common set of skills and knowledge across their core systems portfolio. Business and IT team members who know how to configure, write business rules for, or integrate with one Guidewire application can immediately work with any other of our applications.

Because our automated tests protect our applications against regression, we can add new functionality rapidly. As a result, critical new functionality can be delivered in a few months rather than requiring a year or more of planning and development.

Guidewire Cyence Risk Analytics

Measuring the financial impact of cyber risk for the insurance industry through data science and economic modelling

Guidewire Cyence™ Risk Analytics is a cloud-native economic cyber risk modelling solution built to help the insurance industry quantify cyber risk exposures. Leaders across the insurance industry use Cyence Risk Analytics to prospect, underwrite, and price risks. It enables insurers to manage portfolio exposure accumulations and develop new products with confidence.

Cyber risk is evolving. This presents unique challenges for the insurance industry. Without the benefit of substantial loss history to build traditional actuarial pricing models, insurers have to rely on subjective information from the insured—like high-level questionnaires and brief discussions about what security technologies and protocols are in place—to manage cyber underwriting and accumulation.

Unlike traditional catastrophe risks, cyber has no authoritative data source on which to rely. Cyber risk accumulations are stealthy, and they change often. Companies that might otherwise be completely unrelated may share common internet infrastructure and risks: a cloud outage or zero-day vulnerability can cause correlated losses to companies on opposite sides of the globe.

Unlike most P&C insurance lines, cyber risk involves active adversaries who deliberately seek high-value and opportunistic targets. Cyber risk can be modelled using game theory and behavioural economic frameworks. Our models measure company and portfolio risk by examining company posture and comparing it to bad actor motivations and capabilities.

In short, cyber risks call for better tools for underwriting, pricing, and management. These tools need to account for the shifting threat landscape and measure cyber catastrophe exposures in terms of dollars and probabilities.
How We Do It

Through a process called data listening, we collect vast amounts of technical and behavioural data from a variety of sources at internet scale, including public data, open-source data, proprietary data, and third-party data. We curate the data and apply sophisticated machine-learning techniques to find the signal through all the noise.

The result is a comprehensive and unparalleled economic cyber risk modelling solution that adjusts as the cyber landscape shifts, continuously gathering data and updating economic models based on changing circumstances. Our risk models include a dynamic cost benefit analysis to keep up with bad actors as they choose targets, and with companies as they shift their mitigation strategies.

Our team dedicates deep talent from the cyber risk, data science, and insurance domains to provide a state-of-the-art economic modelling solution and expert-led operational support. This combination gives insurance clients deep insights into their business and enables growth through data-driven product development, underwriting, pricing, and risk management strategies.

Individual and Accumulated Risk Selection

Cyence can be used to assess the risk level of a potential insured at an individual level, but the solution is vital for insurers that need a comprehensive view of their aggregate portfolio exposure. This includes the ability to measure the likelihood and financial impact of a comprehensive set of customizable scenarios.

Cyence examines the correlation of cyber risk within a portfolio and the potential losses that disaster scenarios can have on that portfolio. Understanding the shared attributes and correlation of risk enables realistic, fact-based measures of probable maximum loss. This detailed and continually updated understanding of risk accumulation is crucial for an insurer managing the long-term stability and soundness of their portfolio.

Cyence Risk Analytics Benefits

Improved risk selection

Augments underwriting information with 40+ additional risk factors based on externally collected data to better enable underwriter validation and targeted inquiry

Advanced risk assessment and stress testing

Enables insurers to monitor portfolio health through EP curves, a scenario library, and scenario customization

Improved growth opportunities

Delivers the insight needed to design new insurance products and go-to-market strategies

Rethinking Cyber Risk for Insurance

The cyber security technology industry is full of scores, ratings, and scorecards, but each tool measures technologies and technical metrics in a vacuum. While important, technology itself is not an adequate predictor of cyber risk—many companies with state-of-the-art technology are breached while others with legacy technology are not.

To assess cyber threat, Cyence Risk Analytics leverages a variety of econometric risk models and uses real breach data aggregated from multiple sources. However, technology assessment is just the beginning.

We also:

- Measure companies' cyber posture from the perspective of people and process
- Assess adversary motivation
- Examine attack capabilities
- Consider the impact of a well-timed attack

In addition to using the broadest and deepest collection of technology assessments on companies, we constantly train and refine our predictive risk capabilities to provide customers with the best understanding of cyber security risk.

KEY BENEFITS

- Improved risk selection
- Augments underwriting information with 40+ additional risk factors based on externally collected data Protected profitability
- Addresses pricing adequacy at the individual risk and portfolio level
- Ability to monitor portfolio health
- Evaluate and track portfolio health through portfolio loss analyses and accumulation risks
- Fuel for growth
- Enables you to design new insurance products and go-to-market strategies that drive increased revenues

PRODUCT HIGHLIGHTS

Data listening engine

• Continuous collection and curation of real exposure data across a broad spectrum of people, processes, and technology risk factors

Advanced modelling

• Frequency and severity modelling for cyber-specific aggregation and scenarios

•Stochastic and deterministic outputs at portfolio and event level for improved insurance risk modelling

Robust scenario library

• Out-of-the-box scenario library that includes common regulatory scenarios and scenarios curated by Cyence

• Ability to customize and create scenarios to test hypotheses and manage accumulation risk

Cloud-based

•Browser-based cloud platform

•Quick and easy to get up and running

•Easy-to-use interface

Designed for the insurance industry

•Tailored for underwriting, actuarial, product management, and enterprise risk management users

Stand-alone

•You can take advantage of Cyence insights even if you do not use other Guidewire products

Data Collection

Most actuarial models use easily accessible authoritative sources of attribute and loss data. These risk models are relatively simple to create because the data is abundant and it hardly changes.

In cyber however, there is no authoritative source of data. That's because of a complex regulatory environment, inaccessible data, and the challenge of identifying the cause of an event or even whether an event has occurred.

Furthermore, there are a wide variety of vectors for cybercrime, each of which must be considered to determine a company's cyber risk. Add to this the fact that cyber risk is so dynamic that loss data and models must be regularly updated, and you have a sector desperate for reliable data and models.

Assessment at scale

Many elements must be considered to determine a company's cyber risk profile. These include its user profiles; web traffic; technology stack; malware protection; processes for protecting sensitive information and responding to cybercrime; and employee behaviour, expertise, and training.

While some of this information is accessible through surveys, the data may be unreliable because of reporting accuracy and scale issues. That's why Cyence created a diverse and scalable data factory to accurately and non-invasively collect human and machine data. This behavioural and technical data drives the Cyence risk models

The Challenge

The world's companies are increasingly realizing that cybersecurity is not just a technical problem but a business risk. It has to be managed like other business risks, not only through a combination of risk prevention and mitigation (technology products and services), but also through risk transfer (insurance). According to Marsh, the world's leading insurance broker, the market for cyber insurance covering network security incidents and privacy breaches is over $3 billion and expected to double in the next few years.

But building a cyber risk model involves three different challenges.

The Data Collection Challenge

The first challenge in building a cyber risk model is data. The insurance industry has traditionally built risk models that rely on authoritative providers of data, such as the United States Geological Society (USGS) for earthquake risk, or the National Oceanic and Atmospheric Administration (NOAA) for hurricanes and tropical storms. For such natural events, the hazards are relatively stable, and the same risk models can be used over a span of a few years.

The difficulty with cyber risk is that there is no authoritative source of data that can supply a large, rich dataset for model creation. The Internet is distributed by nature and is increasingly becoming more complex as new technologies emerge. The threat landscape is continuously changing and evolving. So not only does data need to be collected, but it needs to be collected in a dynamic, near real-time fashion to appropriately keep pace with ever-changing threat vectors.

Data collection and risk modelling are closely intertwined, as they iteratively inform and feed into each other. Given the rapidly changing environment, a cyber risk model requires a continuous loop between the two, which is a challenge when the data collection and the risk modelling are performed in silos.

The People/Process Challenge

The second challenge in building a cyber risk model is analysing people and processes in addition to technology. In cybersecurity, there is an obvious and immediate focus on technology and technical indicators. However, most cyber events have a human element associated with them.

A good percentage of all cyber events are caused or aided by insiders, such as the disgruntled employee or contractor, people who often have legitimate access to the data being affected. Another major source of cyber events are accidents or errors - someone leaving a laptop unattended, clicking on a malicious link, or naively providing information that can lead to unauthorized access. Technology itself is not the main culprit in any of these.

A cyber risk model needs to look beyond pure technology and extend the problem to people and processes as well - a holistic data-driven approach is necessary to get a complete view of the multi-faceted cyber risk of companies.

The Economic Modelling Challenge

The cybersecurity industry is awash in a variety of metrics, benchmarks, scores and ratings based on all sorts of technical indicators, including botnets, spam, vulnerabilities and misconfigurations, to name a few. However, these are somewhat orthogonal to the critical question: what is the probability of a cyber event?

The insurance industry requires an economic model around cyber risk, which not only addresses the question on frequency (probability), but also answers questions on severity (how bad is the event going to be?), financial loss (how much is it going to cost?), and recurrence (if a company had an event, what is their probability of having a follow-on event?).

In addition, since the insurance industry is focused on the performance across their portfolio instead of just any one company, a cyber risk model also needs to cover the economic impact of risk accumulations, aggregate events, disaster scenarios and translate all this into probabilistic loss curves - enabling insurers to deploy capital and to economically justify their decisions to shareholders, regulators, and rating agencies.

Approach

What We Do

Cyence combines data science, cybersecurity, and economics into a unique analytics platform that quantifies the financial impact of cyber risk. Cyence is used by leaders across the financial services industry to prospect and select risks, assess and price risks, manage portfolio risk accumulations, and bring new insurance products to market.

The Cyence Approach to Cyber Risk

The Cyber Risk Modeling Challenge

Business leaders worldwide recognize that cybersecurity is not just a technical problem but a business risk-according to Marsh, the world's leading insurance broker, the $3 billion market for cyber insurance is expected to double in the next few years.

Cybersecurity is managed with risk prevention and mitigation (through technology products and services) and risk transfer (through insurance). Building an effective cyber risk model means addressing three challenges:

<https://www.cyence.net/challenge.html> LEARN MORE

The People/Process Challenge

The second challenge in building a cyber risk model is understanding how people and processes influence technology. In cybersecurity, it makes sense to focus on technology and technical indicators. But most cyber events also involve humans and what they do.

An example of human involvement might be a disgruntled employee who embezzles through his company's internal systems. This person is intentionally exploiting their legitimate access to their company data.

Other human sources of cyber events are mistakes-someone leaves a laptop unattended, clicks on a malicious link, or naively provides information that can lead to unauthorized access. Technology itself is not the main culprit in any of these.

A cyber risk model therefore must involve data on both technology and human behaviour to understand the client's holistic risk.

<https://www.cyence.net/process.html> LEARN MORE

The Economic Modeling Challenge

The cybersecurity industry is awash in metrics, benchmarks, scores, and ratings. But these are somewhat tangential to the critical question: how much damage could a cyber event do?
To answer this question, insurers consider not only overall probability but also severity (how bad could the event be?), financial loss (how much could it cost?), and recurrence (what is the chance a company could have more than one event?).

Additionally, since insurers are focused on performance across their portfolio, a cyber risk model must also address widespread systemic events.

This requires considering risk accumulations, aggregate events, and disaster scenarios to quantify exposures. These calculations enable insurers to deploy capital in an informed manner and justify their decisions to shareholders, regulators, and rating agencies.

<https://www.cyence.net/modeling.html> LEARN MORE

The Data Collection Challenge

The first challenge in building a cyber risk model is gathering good data.

For natural catastrophe events, the hazards are relatively unchanging and the same risk models can be used for years. But this is not the case with cyber risk because the internet is so dynamic.

Because the threat landscape for cyber risk is constantly changing, data must be collected in real-time and constantly integrated into an updated risk model. This is a challenge when data gathering and risk-modelling are kept in their traditional silos.

<https://www.cyence.net/data.html> LEARN MORE

Economic Cyber Modelling

Cyber risk is an economic concept, not a technical one, and it is important to view it through that lens. Even with an unlimited budget, no security professional could guarantee that their company will not suffer from a cyber event. Since the cyber risk problem cannot be fixed, much the way a natural disaster cannot be avoided, we must take a risk-based approach, and develop risk mitigation and transfer strategies based on robust models for the frequency and severity of events including potentially systemic disaster scenarios.

The past does not predict the future

Technology and the threat landscape change so rapidly that simple models based on past cyber events don't adequately predict those of the future. This includes both the probability of a cyber event and the type of event that might occur.

Cyber criminals are active adversaries

Cyber events are often not chance occurrences. Bad actors are deliberate. They will escalate their efforts in direct response to a company's attempts to mitigate their risk and exposure.

Many cybercriminal groups have sophisticated attack strategies to circumvent standard protections, especially for attractive targets. That's why cyber risk models must evaluate both the company's defence and attacker's offense.

The active and intentional nature of events makes game theory and behavioural economics the best lens to model cyber risk.

Cyber risk events have many causes

Why does one company fall victim to a cyber event while another is spared? In many cases, an "unintentional insider" neglects to safeguard company information or uses weak authentication procedures that allow a criminal to infiltrate the system. Or a "hacktivist" group targets an organization because it disagrees with its politics. State actors may even launch an attack motivated by espionage or cyber warfare.

The reasons why an organization becomes a cyber-attack casualty are extremely varied. That's why responses and losses cannot be tied to a simple formula. Instead, risk models must include the dynamic cost benefit analysis that bad actors and companies are continuously calculating when choosing targets and risk mitigation strategies.

Cybercrimes can occur in the aggregate

If a cybercriminal breaks into a company's network, he could harm hundreds or even thousands of associated companies and individuals. Additionally, if there are shared paths of aggregation across these companies, a single event can cause a string of related events.

Considering this, the insurance industry is working to define the limits of its exposure so it can make responsible capital decisions and protect itself, its policyholders, and the market at large if catastrophic events occur.

Only a comprehensive economic model can accurately predict cyber risk

Before committing capital, insurers need to understand the organization's many possible threats and their impact in dollars and probabilities. But traditional cyber risk metrics and assessments do not adequately provide this insight.

Instead, insurers need dynamic analytics that tap into technical and non-technical data sources to continually monitor the cyber risk of a portfolio of companies. This kind of cyber risk model integrates in-depth data analysis and sophisticated economic modelling. It provides an agile platform to make confident business decisions based on probability, impact, severity, and accumulation.

Process

Most cyber events are driven by human and behavioural factors - it's often easier for bad actors to trick an employee to hand over their legitimate credentials or click on a bad link in a phishing email than to break into the network vi technical means only. So when an organization's cyber risk is calculated only according to technical indicators, as is often the case, the results can be inadequate at identifying the relevant risk factors.

To accurately model cyber risk, three crucial aspects of a cyber event's human-computer interplay must be considered: people, processes, and, of course, technology.

People

The people behind cyber-attacks often dictate their frequency and severity. For example, a large corporation may be targeted by a number of outside aggressors-rivals, criminals, rogue insiders, activist groups, even state actors-each of whom has a unique motivation, level of sophistication, and resources. These differences will determine how often their attacks happen and how damaging they are.

But the human element of a cyber-attack is not limited to intentional aggressors. According to a 2014 study by IBM, 95% of all cybercrime involves human error-an employee loses a device or leaves it unattended, creates weak passwords, or clicks on malicious links.

Or the insider could intend to attack the company. Insiders include a past or present employee, a contractor, or a vendor or other individual with privileged information about the company or its security protocols.

Intentional insider attacks can be extremely damaging, partly because they may go unnoticed for a long time. That's why keeping an eye on insiders is critical. According to a 2015 AT&T survey, 32% of respondents said inside threats were more destructive to their organizations than outside threats.

Processes

Any company's security profile is only as strong as its weakest link. The problem is, many organizations employ or contract with individuals who do not follow security protocol.

Most companies have corporate guidelines for protecting their technology, but it is still impossible to monitor their entire network completely. This reality is exacerbated by employees and contractors connecting private devices to the company's intranet due to the rising popularity of BYOD programs. If the oversight of an organization's network connections is too narrow or too simple, it can create dangerous security blind spots.

It is therefore as important to consider how a company protects itself as whom it employs and what technology it uses. Does the organization teach and enforce proper protocols and industry standards across the company and among third parties? The quality of an organization's mitigation and incident-response processes suggest how severe a cyber-attack could be, should one occur.

Technology

Finally, the organization's technology posture and technical indicators are important to understanding cyber risk. For example, what firewall protection is present, and how are personal devices on the company network monitored?

It is also necessary to evaluate the organization's established cybersecurity software, and whether any of it is missing security patches. A detailed audit of this technology stack and its history of cyber events will show how prepared the company is for future attack.

A holistic approach

Cyber risk models have traditionally considered only an organization's technology. But that's like betting on your favourite football team based only on the quality of its defence. The

match's outcome will be dictated by much more-like your team's offense, which players are on the disabled list, and the relative strength of your team's defence and your opponent's offense.

As we learn more about cyber events, we know that technology, like the defensive line, is only one part of the whole. Technology must also be analysed alongside people and processes for an accurate assessment of risk.

<https://www.cyence.net/index.html#services> BACK