AXIS Insurance

Mitigating Breach of Contract Risks for Software Firms: Contractual, Operational, and Insurance Strategies

Introduction

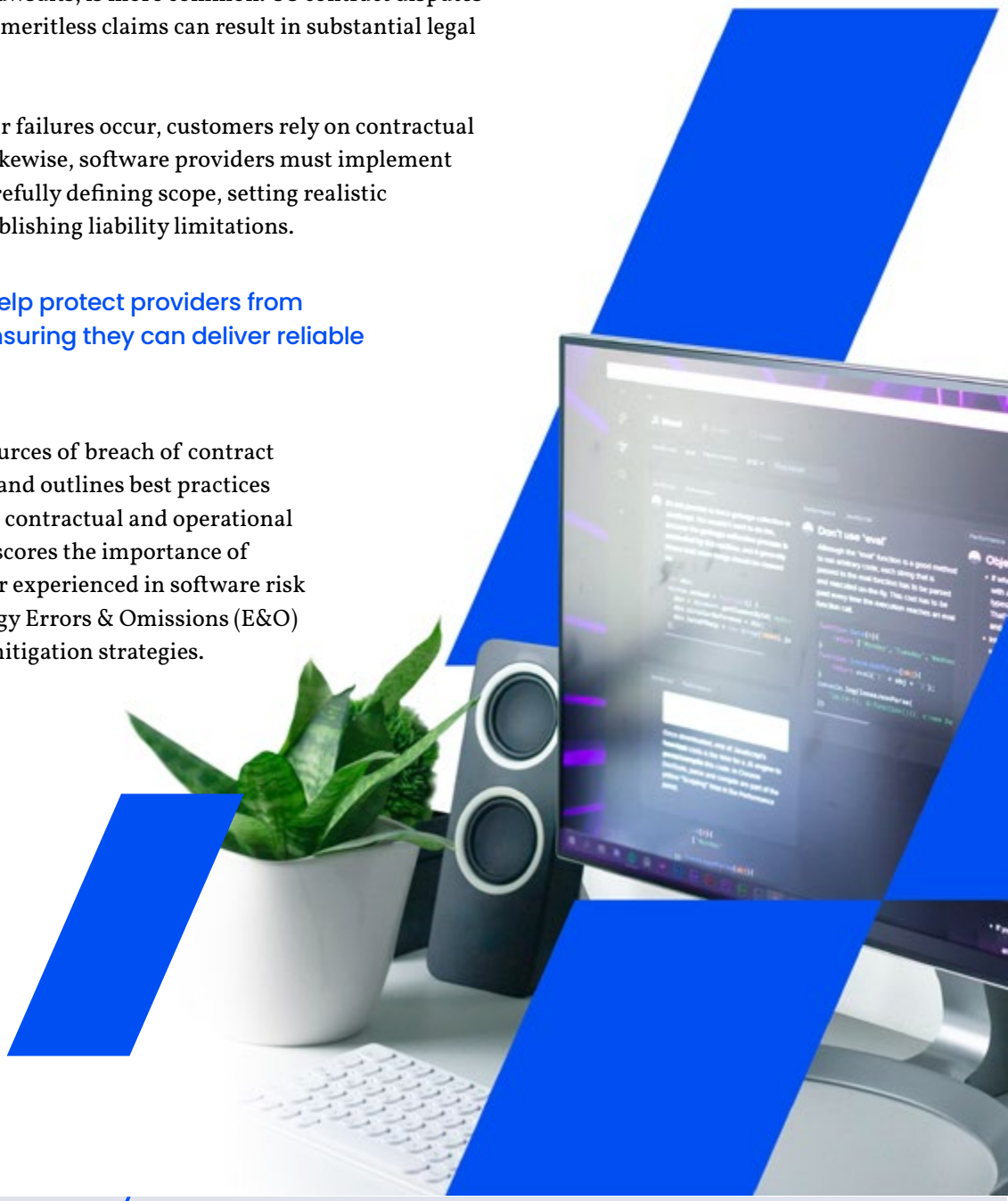
Whether operating as a cloud computing provider, SaaS company, or custom software developer, the main source of legal claims against software firms is breach of contract claims. Contracts often include explicit guarantees and warranties related to delivery timelines, software performance, and service level agreements (SLAs). While these commitments are essential for maintaining client trust and staying competitive in the market, they also create legal exposure if obligations are not fulfilled, leading to disputes and costly litigation.

The risk is even greater for software companies operating in the US market where litigation, particularly class action lawsuits, is more common. US contract disputes are often aggressively pursued, and meritless claims can result in substantial legal expenses.

When performance issues, delays, or failures occur, customers rely on contractual provisions to pursue legal action. Likewise, software providers must implement strong contractual protection by carefully defining scope, setting realistic performance expectations, and establishing liability limitations.

> Well-structured contracts help protect providers from excessive legal exposure, ensuring they can deliver reliable services without undue risk.

This paper explores the common sources of breach of contract claims against software companies and outlines best practices for mitigating these risks from both contractual and operational standpoints. Furthermore, it underscores the importance of partnering with an insurance broker experienced in software risk to advise and place robust Technology Errors & Omissions (E&O) insurance to support internal risk mitigation strategies.



Sources of Breach of Contract Claims Against Software Companies

Breach of contract claims in the software industry typically arise from the following key areas:

1 Failure to Meet Delivery Deadlines

Delivering on time and as promised is important in contracts, especially when businesses rely on software to support their operations. Delays in development, deployment, or feature rollouts can cause serious operational and financial disruptions for clients.

> Contracts typically stipulate specific delivery dates for initial software deployment, updates, and feature enhancements and any failure to meet these deadlines can be grounds for a breach of contract claim.

Many agreements include provisions that outline consequences for missed deadlines, such as financial penalties, service credits, or even termination rights for the client. If delays result from issues like resource misallocation, development bottlenecks, or project mismanagement, affected clients may seek compensation for lost revenue, productivity setbacks, or additional costs incurred due to the delay.

2 Failure to Meet Service Level Agreements (SLAs)

SLAs define key performance benchmarks, such as system uptime, response times, and processing speeds. These agreements ensure that customers receive a consistent and reliable service.

> If a software provider fails to meet the agreed-upon metrics, such as frequent system outages, sluggish performance, or delayed response times for support, clients may claim a breach of contract, especially if the disruptions lead to financial losses.

SLA breaches often trigger automatic remedies, such as service credits, refunds, or the right to terminate the contract without penalties. However, in severe cases where a business suffers financial harm due to prolonged or repeated SLA failures, clients may pursue legal claims seeking damages. Additionally, failure to provide adequate customer support, as defined in SLAs, can also constitute a breach if it results in unresolved technical issues affecting the software's usability.

3 Software Performance & Functionality Deficiencies

Delivering on time and as promised is important in contracts, especially when businesses rely on software to support their operations. Delays in development, deployment, or feature rollouts can cause serious operational and financial disruptions for clients.

> If the software does not meet the promised specifications, customers may claim a breach of contract on the basis that they did not receive the product they paid for.

A common issue arises when products are marketed as compatible with third-party applications, but integration is flawed or non-functional, causing operational inefficiencies. Similarly, unexpected downgrades, removal of key features, or failure to maintain promised functionalities in future updates can also trigger disputes.

4 Security & Data Breach Issues

Data security is a top priority for software providers, especially in industries that handle sensitive information, such as healthcare, finance, and e-commerce. Most software contracts include specific data protection requirements, often referencing industry standards like GDPR, HIPAA, or ISO 27001.

> If a provider fails to implement adequate security measures, resulting in data breaches, unauthorized access, or data loss, customers may allege a breach of contract for failing to uphold security obligations.

Security-related breaches can have significant financial and reputational consequences, including regulatory fines, customer lawsuits, and damage to brand trust. Clients affected by data breaches may seek compensation for business losses, legal costs, and regulatory penalties.

5 Misrepresentation or Misstatement in Sales & Marketing

Software providers must be cautious when promoting their products, as misleading statements about features, performance, or compatibility can lead to breach of contract claims. Overpromising capabilities, such as exaggerated AI automation, scalability, or security protections, can result in customer dissatisfaction and legal disputes when the product fails to meet expectations. Common claims arise when:

A provider assures customers that the software integrates seamlessly with specific platforms, but compatibility issues later surface.

Performance benchmarks (e.g., „99.99% uptime") are advertised but not contractually guaranteed or consistently met.

Features or customizations promised during sales negotiations are missing in the delivered product.

> If a customer can demonstrate that they entered the contract based on inaccurate representations, they may have grounds for a breach of contract claim.

Contractual Measures to Mitigate Breach of Contract Claims

Software companies can implement strong contractual controls to help mitigate potential breach of contract claims. These measures help set clear expectations, limit liability, and enhance service reliability.

1 Clearly Defined Scope & Deliverables

One of the primary causes of contractual disputes in the software industry is ambiguity regarding what the provider is obligated to deliver. To avoid misunderstandings:

- Clearly define the scope of services, including core features, functionality, and any additional modules or integrations.
- Outline deployment timelines, expected milestones, and potential variances.
- Specify support and maintenance commitments, including updating schedules and response times.
- Detail client responsibilities, such as necessary configurations, system requirements, or data migration steps.

By ensuring that deliverables are explicitly stated in the contract, software providers can limit disputes over unmet expectations.

2 Limitations of Liability & Disclaimers

To reduce financial exposure in the event of a breach of contract claim, agreements should include well-drafted limitation of liability provisions. Key components include:

- **Liability Caps** – Set a maximum limit on damages, often tied to a percentage of the total contract value or a fixed dollar amount.
- **Exclusion of Consequential Damages** – Exclude liability for indirect damages, such as lost profits, business interruption, or reputational harm.
- **Third-Party Dependency Disclaimers** – Limit responsibility for failures related to third-party vendors, cloud hosting services, or API integrations that are beyond the provider's control.

These provisions help software providers manage risk while ensuring they remain accountable for core service obligations.

3 Force Majeure Clauses

A force majeure clause protects software providers from liability if contract performance is disrupted due to unforeseen circumstances. This can include:

- Cyberattacks or system failures beyond the provider's reasonable control.
- Regulatory changes that impact compliance requirements.
- Global supply chain disruptions affecting cloud infrastructure or third-party services.
- Natural disasters, pandemics, or geopolitical events that prevent service delivery.

By explicitly listing potential force majeure events and defining how they impact contractual obligations, software companies can protect themselves from liability due to uncontrollable disruptions.

4 Performance-Based SLAs with Clear Remedies

Service Level Agreements (SLAs) should set realistic performance benchmarks and define appropriate remedies for non-performance. This includes:

- Uptime commitments (e.g., 99.9% availability) with exclusions for scheduled maintenance.
- Response and resolution times for customer support requests.
- Data processing speeds and storage reliability guarantees.

Rather than allowing SLA breaches to escalate into legal disputes, contracts should include remedies such as service credits or extended support periods instead of automatic refunds or termination rights. This approach incentivizes providers to maintain service quality while reducing financial and legal exposure.

5 Indemnification Clauses

Indemnification provisions clarify who is responsible for specific risks, helping prevent legal disputes over liability. These clauses should address:

- **Data Breaches** – If a security breach occurs due to provider negligence, they may be required to indemnify the client for regulatory penalties or legal costs.
- **Intellectual Property Infringement** – Providers should indemnify clients if their software infringes on third-party patents or copyrights.
- **Third-Party Software Failures** – If the software solution depends on third-party components (e.g., cloud hosting, payment processing APIs), responsibility for failures should be clearly allocated.

By structuring indemnification clauses carefully, software companies can limit liability and be better protected from unreasonable claims.

Operational Risk Mitigation Strategies

Beyond contractual protections, proactive operational strategies can help reduce the likelihood of breaches and enhance customer trust.

1 Robust Quality Assurance & Testing

To minimize software defects, providers should implement:

- Automated and manual testing before deployment, including security and stress testing.
- Beta testing and pilot programs to identify potential issues before full rollout.
- Continuous monitoring for bugs and vulnerabilities to ensure timely fixes.

By prioritizing software quality, providers can prevent disputes related to non-functional or underperforming solutions.

2 Continuous Monitoring & Incident Response Plans

Real-time system monitoring and proactive incident management helps prevent disruptions before they escalate into contractual disputes. Best practices include:

- 24/7 system health monitoring to detect performance degradation or potential outages.
- Automated alerts for security vulnerabilities, unauthorized access, or unusual activity.

3 Customer Support & Communication Transparency

Effective client communication is essential for managing expectations and preventing disputes. Software companies should:

- Provide proactive updates about software changes, upcoming maintenance, or potential service disruptions.
- Offer transparent escalation processes for unresolved technical issues.
- Document client interactions to ensure contractual commitments are met and avoid misunderstandings.

When clients feel informed and supported, they are less likely to pursue legal action over minor service disruptions.

4 Cybersecurity & Compliance Frameworks

Ensuring compliance with industry security standards not only reduces the risk of breaches but also strengthens contractual defenses. Software providers should:

- Implement security frameworks such as SOC 2, ISO 27001, or NIST to ensure data protection.
- Encrypt sensitive data to prevent unauthorized access.
- Regularly conduct security audits and penetration testing to identify vulnerabilities.
- Ensure compliance with data protection laws such as GDPR, CCPA, or HIPAA, depending on the industry and region.

By maintaining a strong security posture, software companies can reduce the likelihood of security-related breach of contract claims and regulatory penalties.

Partnering with an Experienced Insurance Broker

While robust contractual and operational risk mitigation measures reduce exposure, they do not eliminate the possibility of breach of contract claims. By working with an experienced insurance broker who understands the unique exposures software companies face, businesses can leverage their risk mitigation efforts to secure the most favorable insurance coverage terms.

A knowledgeable broker can:

- ✔ **Assess risk exposure and recommend risk mitigation measures**
- ✔ **Present tailored insurance coverage options**
- ✔ **Negotiate lower premiums based on strong internal safeguards**
- ✔ **Ensure policies address liability risks unique to the business operations of software companies**

Conclusion

Software companies operate in a high-risk environment where breach of contract claims are common, and particularly costly when brought in the US. While contractual clarity, operational resilience, and proactive customer engagement are essential in reducing these risks, they cannot fully prevent disputes.

Robust Technology E&O insurance is an important backstop to strong contractual and operational controls providing financial protection against breach of contract claims.

By working with an insurance broker experienced in software risk, providers can optimize their risk management approach and secure the best coverage terms, ensuring long-term operational stability and financial protection.

Contact us today to learn more.

AXIS Insurance

Chris Jones
Account Executive, Technology
chris.jones@axisinsurance.ca
(778) 788-2853

axisinsurance.ca