

## Title

Cybersecurity Clauses: Why Contracts Are Becoming Companies' First Line of Defence

## Brief Overview

In today's digital economy, cybersecurity is no longer just an IT issue—it is a strategic and legal priority. Well-crafted contracts play a pivotal role in mitigating cyber risk, ensuring incident response, defining liability, and enforcing supplier standards, helping companies safeguard operations, reputation, and regulatory compliance.

## Practice Group

IP, IT, and Data Protection

Compliance & Regulatory Advisory

## Full Article:

In the modern digital economy, **cybersecurity** is no longer solely an IT issue. It has become a matter of **legal strategy, risk management**, and long-term business stability. A growing number of cyber incidents do not end with the technical remediation of systems but continue through **regulatory proceedings, damage claims**, and complex **contractual disputes** between business partners.

In such an environment, **contracts** are becoming one of the most important instruments for protecting a company. A properly structured contract can prevent a **cyber incident** from escalating into a multi-year dispute or regulatory problem, whereas a poorly defined contractual framework often means that a company bears the consequences even when it is not technically responsible for the incident.

## Why Contracts Are a Key Tool for Managing Cyber Risk

Modern business models rely on **cloud infrastructure, SaaS platforms**, outsourced IT support, and integrated digital ecosystems. This means that a company's security no longer depends solely on its internal systems but also on the **security maturity of suppliers** that have access to its data or infrastructure.

For this reason, **cybersecurity clauses** today play an equally important role as traditional clauses on liability, confidentiality, or intellectual property protection.

## Formal Compliance Versus Real Cybersecurity

One of the key challenges in practice is the distinction between formal and actual security. Many IT providers formally apply certain **security standards**, but without a clear **contractual obligation**, a company has limited ability to react if an incident occurs.

In modern contracts, **security standards** are increasingly defined through specific technical and organizational measures, with the possibility of verifying their implementation through **cyber audits** or other forms of control.

## Contractual Management of Cyber Incidents

Particularly important are provisions regulating actions in the event of a **cyber incident**. In practice, delays in reporting an incident often cause more damage than the incident itself.

Companies that do not have contractually defined obligations for **incident notification** and **cooperation during an incident** often lack critical information at the moment they need it most, which further increases **regulatory** and **reputational risk**.

### **Cooperation During an Incident as a Key to Business Continuity**

Cooperation during an incident becomes especially important in complex digital environments. Forensic analysis, access to logs, communication with regulators, and user notification can rarely be carried out without active cooperation from IT providers.

Contracts that do not foresee such situations often lead to disputes precisely at the moment when the company needs operational support the most.

### **Allocation of Liability and Cyber Insurance**

**The allocation of liability for cyber incidents** is one of the most sensitive issues in contractual practice. The boundary between direct damages, **indirect damages**, **liability limitations**, and compensation obligations often becomes the central point of dispute after an incident.

Therefore, modern contracts increasingly include an obligation to maintain **cyber insurance**, providing an additional layer of financial protection in the event of serious security breaches.

### **Cyber Risk in the Supply Chain**

A particular challenge is managing **cyber risk in the supply chain**. A significant number of serious incidents arise precisely from vulnerabilities within subcontractors or partners in the digital ecosystem.

For this reason, companies increasingly require suppliers contractually to apply the same **cybersecurity standards** to their own subcontractors, thereby reducing systemic risk.

### **Cybersecurity as Part of Corporate Governance and Reputation**

Although **cybersecurity** is often viewed through a technical lens, practice clearly shows that the **legal framework** is frequently a decisive factor in managing the consequences of a cyber incident.

Companies that proactively define obligations, procedures, and responsibilities through contracts demonstrate significantly greater resilience to cyber incidents and regulatory pressure.

### **Three Key Cybersecurity Clauses That Determine the Legal Outcome of a Cyber Incident**

Modern contracts may contain numerous cybersecurity provisions; however, practice shows that three groups of clauses most often determine the legal and financial outcome of a cyber incident:

- The first is the clause defining the supplier's **minimum security standards**, as it establishes the basis for assessing whether the supplier acted in accordance with professional and regulatory expectations.
- The second key area consists of provisions governing the **obligation to report a cyber incident and cooperate during the incident**, since the speed and transparency of information exchange often directly affect regulatory consequences and the ability to mitigate damage.
- The third most important group comprises clauses regulating the **allocation of liability and compensation for cyber incidents**, including liability limitations, indemnity mechanisms, and cyber insurance obligations.

In practice, it is usually the combination of these three types of clauses that determines whether a cyber incident remains an operational issue or escalates into a serious legal and financial dispute.

### **Cyber Contracts as a Strategic Business Protection Tool**

Today, the question is no longer whether a cyber incident will occur, but when. The difference between companies that successfully overcome such situations and those that suffer long-term consequences often comes down to the level of **legal preparedness** and the quality of the **contractual framework** governing digital relationships with partners.

In the modern business environment, **cybersecurity contracts** are becoming a key instrument for protecting business operations, reputation, and long-term market stability.

*This article is for informational purposes only and does not constitute legal advice. Should you require additional information, please feel free to contact us.*

**Author:**

Ivan Todorović  
Partner