Combat cybercrime by fortifying your contracts

Offenses committed in the digital environment are numerous: unauthorized access to information systems, fraudulent transfer orders, website alterations, denial of service, ransomware, identity theft, fraud, and issues related to e-reputation, affecting both individuals, businesses, and states.
The number of cyberattacks is growing exponentially, and the resulting damages, which take various forms, can be highly significant.

While the fight against cybercrime is primarily a technical matter, it must also be addressed proactively and preventively in the contracts entered into between businesses and their suppliers. It is also essential to raise employee awareness regarding the risks associated with the use of computers, smartphones, and internet connections provided by the company.

Assessment of the company's exposure to cyber risk

At the contractual level, the first step in protecting against cybercrime is to trace the relationships between the company and each of its service providers (ISP, hosting provider, developer, maintenance, etc.) to verify the existence of a contract and its terms.
The contractual obligations will also be reviewed in light of the technical audit, which may reveal vulnerabilities.
Digital security professionals and legal experts will work hand-in-hand to assess the nature of the commitments, with the following key obligations: (i) to document and verify the commitments, (ii) to communicate the test results to the client, (iii) to implement the recommendations of the ANSSI (French National Cybersecurity Agency), and most importantly, (iv) to formalize their technical obligations in a contract.
For their part, service providers have every interest in ensuring transparency and promoting mutual understanding of the technical measures being applied and their limitations.

Internal Cyber Governance: The Digital Responsibility of the Company

Cyberattacks often originate from internal negligence or human error (e.g., opening a suspicious email), which could have been avoided through employee awareness and the dissemination of proper preventive measures.

In addition to the establishment of a cross-functional team, several legal tools are available to formalize internal measures for combating cybercrime, including:

- The internal regulations that render the protective measures defined by the company enforceable;
- The policy governing the use of information and communication resources provided to employees, including traceability, filtering, and synchronization, which must be binding in nature ; addressing technical and legal threats, and enhancing the protection of high-value data, personal data, sensitive information, and trade secrets through the development of a coherent action plan.

Contractual Cyber Governance: Strengthening your contracts with suppliers

A number of contracts are impacted by cyber risk. For example:

- **Integration Contract**: The delivery of a new version may contain malware. The testing phases must include specific security measures related to the testing and production environments. It is recommended to conduct tests using fictitious data.
- **Hosting Contract**: The hosting of servers, websites, applications, and sensitive data entails specific security conditions and approvals.

- **SaaS Contract**: All data is accessible and hosted by the service provider, which presents a high risk.
- **Maintenance Contracts (TMA)**: In these contracts, service providers deliver patches and connect to the company's information system, making them potential targets for cyberattacks.

To address these risks, new contractual requirements must be incorporated into the contracts to compel service providers[1] to comply with, in particular, the best standards of the art, which should include:

- The Information Security Policy (PSSI), which serves to outline the company's information security policy.
- Employee training, which is essential to ensure understanding and compliance with the defined measures and to promote accountability among all staff.
- Internal audits and action plans.

As with contracts with service providers, documents must be enhanced with new specific requirements that complement those established under the GDPR, along with the appropriate best practices to adopt in order to contain a cyberattack and preserve evidence.

With remote work being a contributing factor to increased cyber risk, the implementation of internal cyber governance is particularly timely.

Our recommendations: Strengthen contracts with your service providers, supplement internal best practices, and integrate, if not already done, a legal professional (in-house or outsourced) into a cross-functional team.

Isabelle BOUVIER
BOUVIER AVOCATS *(This is a straightforward translation, as names and titles typically remain unchanged)*

[1] *CNIL Decision of October 4, 2021, Francetest: In addition to a failure to configure the website properly, the company Francetest, which provides pharmacists with a website to collect personal data and transmit it to a national Covid screening information system, entrusted the hosting of health data to a company that was not authorized, along with other identified deficiencies.*

n°84 I Journal of Legal Management I 45

(This is a Journal name translation; however, names typically remain unchanged)