CYBER SECURITY CLAUSES IN COMMERCIAL CONTRACTS: A GROWING NECESSITY IN THE DIGITAL ECONOMY

Vaishnobi Kumari*

ABSTRACT

The rapid growth of the digital economy has significantly changed the commercial dealings, mode of operations, and the degree of risks of organisations in the world. Firms are all relying on digital infrastructure, cloud computing, superior data analytics, and networked supply chains, thus making cybersecurity not just a technical matter but a fundamental business and legal matter to question. Cyber incidents, including data breaches and ransomware attacks, system downtime and intellectual-property theft, may cause irreparable financial losses, regulatory fines, disruption in business operations, as well as reputational damage.[1] This means that the traditional contractual terms, like confidentiality agreements and force majeure, are inadequate to address the issues of cyber risk.[2] Cyber security provisions have become an imperative contractual tool in sharing risk, setting responsibilities, and accountability amongst contracting parties. This paper provides a detailed discussion of cybersecurity provisions in commercial contracts and contends that they must be included in the modern online economy. It examines the economic, technological and regulatory forces behind their increasing acceptance, such as increasing cyber risks, tougher data-protection policies, and more demanding regulatory, customer and insurer demand.[3] It goes on to discuss the design of and the key elements of such clauses, such as security standards, data-protection obligations, breach-notification requirements, audit rights, cooperation on incident-response, allocation of liability, and indemnities, as well as the drafting and negotiation issues associated with proportionality, technological change, cross-border compliance and bargaining imbalances. Besides, the paper has covered industry-specific issues, the interaction between cyber security provisions and coverage, and new trends, including continuous compliance,

*BBA LLB, SYMBIOSIS LAW SCHOOL, HYDERABAD.

[1] IBM Security, *Cost of a Data Breach Report 2024*.

[2] Reed C and Angel J, *Computer Law* (7th edn, OUP).

[3] World Economic Forum, *Global Cybersecurity Outlook 2024* (WEF 2024).

artificial-intelligence risk, and supply-chain security. Combining law with practice, the article argues that the provision on cybersecurity is no longer a peripheral boilerplate but a tool that should be used to reduce the risk associated with digital interactions and maintain faith in business relationships. In a data-centric economy where connection is unavoidable, the tenacity of cybersecurity clauses is the building block of contractual toughness and business sustainability over the long term.[4]

Keywords: Cyber Security, Cyber Risks, Data Protection.

INTRODUCTION

The digital economy is marked by a massive penetration of information and communication technologies in virtually all spheres of business activity. Contemporary businesses are run through interconnected digital platforms, use data-driven decision-making, and heavily depend on third-party technology providers in delivering mission-critical services to the enterprise, such as cloud computing, payment gateways, customer-relationship management applications, data analytics and logistics coordination.[5] There are significant operational, scalability and innovation gains realised in this digital ecosystem. But at the same time, it expands the area of computer danger, exposing businesses to sophisticated and dynamic threats. Cyber risks in the digital economy have ceased to be local phenomena, that is, the failure of individual systems; they are endemic. Even one weakness in a vendor's software, a cloud system of a service provider, along with a data-processing procedure of a partner, can spread through the entire supply chain, leading to downtime, data theft, non-compliance with regulations, financial losses and long-term reputational losses. The number of digital dependencies also grows, and with the risks of cascading failures, which move beyond organisations, increases. Conventionally, business contracts were based on material goods, delivery channels and financial risks that can be easily measured. Cyber security considerations were traditionally handled as technical or operational in nature and dealt with internally by the IT departments, and seldom discussed directly as a contractual issue. This method is no longer relevant. The high-profile cyberattacks, increased regulatory and regulatory oversight, and increased litigation regarding data protection and service outages have heightened the direct contractual consequences of cyber incidents.[6] Consequently, cybersecurity has taken a strategic and legal

[4] Schneier B, *Click Here to Kill Everybody* (W W Norton 2018).
[5] OECD, *Digital Security Risk Management for Economic and Social Prosperity* (2015).
[6] World Economic Forum, *Global Cybersecurity Outlook 2024.*

priority as opposed to a technical issue.[7] The modern business agreements are becoming more elaborate in terms of cybersecurity provisions, assigning responsibility, establishing compliance principles, and determining liability in the case of an attack. This change indicates a wider understanding that the cyber risk in the digital economy should be actively addressed in the form of cooperation, regulation, and the clear definition of a contract.

CYBER SECURITY CLAUSE KNOWLEDGE

There are cybersecurity clauses that are contractual provisions that identify the obligations, rights, and liabilities of the parties involved in the contracts in terms of information systems, data, and digital property protection.[8] In contrast to the traditional confidentiality provisions, where the main limitation is described as the unauthorised disclosure, the cybersecurity provisions assume a proactive approach.[9] They include technical, organisational and procedural security measures that are needed to stop, identify, control and react to cyber threats during the contractual relationship. These provisions may be used in relation to a broad category of assets, such as personal data, trade secrets, business secrets, and essential systems of operations.

Cybersecurity clauses are significant in the current environment of increasing digital interdependence in the way they reduce the risks linked to outsourcing, cloud computing, and third-party services. They tend to make references to adherence to established security frameworks, regulatory requirements, and industry best practices and align contractual requirements with external legal and governance requirements.[10] Such clauses can also include a requirement related to employee training, access controls, incident-response planning and regular security assessments or audits. In the most basic definition, cybersecurity clauses perform three main functions. First, they define minimum security requirements and criteria and can make sure that all involved parties have a reasonable amount of cyber resilience. Second, they divide risk and responsibility through the clear delineation of liability, indemnity, and remediation liability in the occurrence of a cyber incident. Third, they establish transparency, collaboration, and enforcement mechanisms, e.g., breach-notification timelines

[7] Reed C and Angel J, Computer Law (7th edn, OUP).
[8] ENISA, Contractual Obligations and Cybersecurity in Supply Chains (2023).
[9] Solove DJ, Understanding Privacy (Harvard University Press 2008).
[10] ISO/IEC 27001:2022.

and audit rights.[11] Cybersecurity clauses via these functions enable the transformation of cyber risk as an abstract and technical issue into a well-defined and enforceable contractual duty.

MOTIVATIONS OF CYBER SECURITY PROVISIONS IN BUSINESS CONTRACTS

Escalating Cyber Threat Landscape: Cyber-attacks have increased drastically in terms of frequency and sophistication, which have posed a lot of operational as well as financial threats to businesses. Hackers, organised cybercriminal groups, and state-sponsored groups with high technical capabilities have now become a threat actor. Hackings of ransomware, phishing, and supply-chain are especially widespread, and usually involve third-party service providers to obtain unauthorised access to various organisations via a single vulnerable location.[12] Such is the linked threat landscape where vulnerability in the systems of one contractual partner can compromise the activities of another. Thus, it is the case that businesses are becoming more and more obliged to incorporate cybersecurity requirements into business contracts in order to make all the parties implement the right preventive and defensive strategies.

Competitive Regulatory and Legal Force: Data protection and cybersecurity regulatory frameworks have grown at a fast rate and currently have strict compliance provisions for organisations.[13] A large percentage of these laws hold other parties liable in addition to internal systems, making it the duty of businesses to make sure that other vendors, subcontractors and partners have taken appropriate precautions.[14] The obligations are further increased by sector-specific controls, critical-infrastructure controls and data-breach notification requirements. The inability to embed enforceable cybersecurity provisions in business agreements can trigger regulatory fines, financial fines or liability, especially in cases where the third-party failures have been the cause of data breaches or slowdowns.[15]

Commercial and Reputational Analysis: An attack on the cyber may significantly undermine consumer confidence and harm the brand recognition of an organisation.[16] Trust has become an important commercial weapon in competitive markets. Clients and partners in business demand contractual guarantees regarding their information, systems, and processes being safeguarded against cyber terrorists. As a result, cybersecurity provisions serve as a form of

[11] NIST, Cybersecurity Framework (v 2.0).
[12] World Economic Forum, Global Cybersecurity Outlook 2024.
[13] GDPR, Regulation (EU) 2016/679.
[14] Information Technology Act 2000 (India) ss 43A, 72A.
[15] IT Rules 2011.
[16] IBM Security, Cost of a Data Breach Report 2024.

trust, which is a show of an active engagement to secure data, robustness, and a responsible approach to risk management.

Insurance and Risk Transfer: Cyber insurance is now becoming a significant risk-reduction tool, but in many cases, coverage depends on a sound cybersecurity program. The insurance companies usually request policyholders to adopt and enforce cybersecurity provisions in their vendor contracts. In insuring and assessing claims, insurers can examine the risk distribution in the contract and adherence. Therefore, the presence of cybersecurity clauses is critical to the efficient transfer of risk and claims insurance.[17]

FUNDAMENTAL ELEMENTS IN CYBER SECURITY CLAUSES

The standards on information security aim to guarantee the protection of data in information systems.

Information Security Standards: The purpose of information security standards is to ensure the protection of information in information systems. Contracts may require adherence to established information security frameworks or industry standards that may be international, industry-specific guidelines or internal security policies.[18] The problem is how to be specific and flexible at the same time, ensuring that standards are not obsolete due to changing technology.

Technical and Organisational Measures: As a standard in cyber security provisions, it is necessary to establish the necessary technical and organisational controls, which may include access control, encryption, network monitoring, employee training and incident detection systems.[19] These requirements can be risk-based as opposed to prescriptive to suit different operating environments. Data Classification and Handling: The research engaged in data classification and handling through the classification of data into three categories.

Data Classification and Handling: The study involved data classification and handling by categorising data into three groups.[20] The effective clauses differentiate various types of information such as personal data, confidential information and publicly available information.

[17] OECD, Digital Security Risk Management (2015).
[18] ISO/IEC 27001:2022.
[19] Cavoukian A, Privacy by Design.
[20] UNCTAD, Data Protection and Privacy Legislation Worldwide (2023).

All categories can have individual handling and security requirements which describe their sensitivity and worth.

Incident Response and Breach Notification: Some of the most important aspects of cyber security provisions are breach notification.[21] They outline the definition of a security incident, the necessary time to notify about it, and the information to be published. The promptness of the notification allows the parties concerned to prevent the damage, to meet the law requirements and to handle the communications.

Cooperation and Remediation: Contracts often mandate the parties to assist in investigating and fixing cyber incidents. This can include access to logs, systems and people, and also being involved in combined response operations. This type of cooperation is critical in multi-party, multi-faceted, and digital setups.

AUDIT, MONITORING AND COMPLIANCE RIGHTS

In order to make sure that cybersecurity commitments are not only formal but also workable, commercial contracts are becoming more and more reflective of audit, monitoring, and compliance rights. Under these clauses, one of these parties, in most cases, the data owner or a service recipient, can ensure that the other party adheres to the agreed cybersecurity standards and contractual duties. Some rights can be to perform periodical security tests, to examine independent third-party certifications, or even to inspect systems, processes and controls related to cyber risk management on site. Audit and monitoring procedures are important in the improvement of transparency and responsibility, especially in long-term or high-risk contractual relations. They can help organizations undermine the shortcomings, keep up-to-date with the emerging regulatory demands, and implement corrective measures before a cyber-attack. Contracts, in most cases, provide details on what, how and the frequency of audits, and qualifications of auditors, to make audits consistent and objective. Timelines of reporting and remediation are usually part of formalising follow-up measures.

Nevertheless, audit rights should be well-designed to balance control and practicality in operations. Unnecessary or invasive audits may interfere with the running of the business, raise expenses, and reveal confidential commercial or security data. In order to deal with these issues, contracts usually restrict audits to reasonable notice, access to relevant systems

[21] GDPR arts 33–34.

exclusively, and have confidentiality guarantees.[22] Risk based approach would be proportionate in providing audit and compliance privileges to strengthen cybersecurity requirements without diminishing trust and business effectiveness.

SHARING OF LIABILITY AND RISK

Liability in Cyber Cases Websafe.co.uk is Liable in Cases of Cyber Incidents: The clauses related to cybersecurity are at the centre of deciding the distribution of liability in case of a cyber-attack. Commercial contracts can take the form of fault-based liability, where negligence or failure to comply with contractual obligation is the basis of liability, or strict liability, where the liability is independent of fault. The nature of the loss to be covered by contracts is usually specified, including direct financial loss, business interruption costs, data restoration costs, or third-party claims. The allocation of liability usually shows the relative level of control that the parties have over the systems, information and security protocols that were impacted. An example of this is that a service provider with responsibility over cloud infrastructure might have more liability for vulnerabilities of the system, whereas a customer might have the liability for misuse of data due to its own access controls.

Indemnities: The use of indemnity is also a major risk-sharing tool in a cyber-related incident. Such provisions can indicate that one of them must indemnify and hold the other harmless against losses, damages, claims, litigation expenses, and regulatory fines due to a cyber breach. The indemnities are especially important in the cases of personal data breaches when the regulatory penalties and claims of third parties can be very substantial.[23] Since indemnities may transfer much financial risk from one party to another, they are typically the subject of intense negotiating activity. Parties can also cap indemnities to those breaches that are attributable to particular failures, like the failure to comply with security standards, data protection laws, or place monetary limits to contain exposure.

Limitations and Exclusions: Limitations of liability are a traditional aspect of commercial contract theory; however, their application to losses related to cyber-related exposure is still a common point of contention. The parties to such agreements need to make a wise decision on whether the cyber incidents should fall under the same general liability limits or whether they should be treated as carve-outs. Particular losses, such as regulatory fines, expenditures related

[22] ENISA, Contractual Obligations and Cybersecurity in Supply Chains (2023).
[23] Reed C and Angel J, Computer Law (7th edn, OUP).

to data-breach notification, and intellectual-property abuse, can be entirely exempted from the liability capping.[24] This needs to be done with precision to reduce ambiguity and eliminate future conflicts. Scrupulously designed limits and exclusion approach will thus guarantee a reasonable distribution of cyber risk at the same time maintaining business predictability and fairness.

SECTOR-SPECIFIC CONSIDERATIONS

Cyber-security responsibilities that are ingrained in commercial agreements are quite diverse in the industrial sectors due to the risk profile, operational needs and regulatory requirements. Therefore, cybersecurity provisions need to be industry-specific and capture industry-related risks and obligations instead of being based on a single, one-size-fits-all structure. Contractual provisions in the financial services sector focus on the resilience of the system, the integrity of data and high standards of regulatory compliance.[25] Banking institutions work in conditions of increased regulatory control and, therefore, become the targets of advanced cyber-attacks due to the vulnerability of financial information and the infrastructure of transactions. In this connection, the contractual language usually involves higher levels of security, mandatory reporting of the incidents, audit privileges of the regulators, and extensive business continuity and disaster recovery requirements. Healthcare contracts, on the contrary permanent protection of sensitive patient information and compliance with health-data protection laws. Some of the common cybersecurity provisions in this industry include access control, data encryption, breach-notification periods, and limitations on data use and storage. Due to the possible consequences of violations on patient privacy and safety, liability and indemnity rules are expected to be stricter. In the manufacturing and critical-infrastructure industries, the main issues are continuity of operations and the security of supply chains.[26] The cyber-attacks in such settings may cause disruption of production, safety systems, and create far-reaching economic effects. In turn, network security, system availability, and pre-coordinated incident-response procedures across interdependent suppliers are emphasised in contracts. Contracts will be more effective in terms of exposure management and the enhancement of operational resilience if the cybersecurity provisions are aligned with the risks in the sector.

[24] IT Act 2000.
[25] OECD, Digital Security Risk Management.
[26] ENISA (2023).

CROSS-BORDER AND JURISDICTIONAL PROBLEMS

With a rapidly globalised digital economy, business dealings are habitually spanning across various jurisdictions, thus creating complex legal and regulatory challenges. Cybersecurity provisions on cross-border contracts should be able to accommodate the differences in national laws and regulations as well as enforcement procedures. The differing data-protection, cyber-security and breach-notification mandates in various jurisdictions create a sense of uncertainty about the compliance requirements and legal liability in the occurrence of a cyber-incident.

One of the major threats is to determine the legal framework that regulates cybersecurity responsibilities and liability. Inequality in ensuring the protection of data, regulatory fines and enforceability of the contract may foster overlapping or even contradictory requirements. Organisations might also be simultaneously subject to more than one regulatory regime, especially when they store, process or transmit data internationally.[27] In this respect, cybersecurity provisions commonly contain detailed compliance requirements that specify various legal frameworks or imply the need to comply with the most rigorous one in place.

Effective cross-border contract management on cyber-risks is directly associated with choice-of-law and dispute-resolution provisions. The certainty in the rules and application of cyber conscription is brought about by explicit identification of the controlling law. Equally, agreed dispute-resolution processes, be it arbitration or specific courts, help in countering the risks of multi-jurisdictional litigation. It is possible to mitigate legal uncertainty by carefully balancing the clauses concerning cybersecurity with the jurisdictional ones, and hence improving the management of the cross-border cyber risks.

NEGOTIATION PROBLEMS AND IMBALANCES OF POWER

Cybersecurity terms in business contracts are often complex to negotiate due to the existence of a strong power distance between the contracting parties. The superior bargaining power is routinely enjoyed by large corporations, specifically multinational businesses and regulated companies like banks or telecommunications companies. They, therefore, often enforce severe cybersecurity standards on smaller vendors, start-ups or service providers as a condition to contractual interaction. Such requirements can include adherence to global guidelines, including ISO/IEC 27001, regular third-party security assessments, penetration testing,

[27] Kuner C, Transborder Data Flows and Data Privacy Law (OUP 2013).

massive documentation requirements, and a compulsory cyber-insurance policy. Although these measures are meant to reduce risk, smaller entities are usually not in a position to meet these requirements; in terms of fiscal, technical, and human capabilities, leading to disproportionate compliance costs.

On the other hand, technology vendors and cloud-service companies that are leading players in the field do not tend to acknowledge contractual terms that would significantly limit them to huge uncertainties about the damages resulting from data breaches, cyber-incidents, or system malfunctions. These entities often demand standard-form contracts with extensive exclusions of liability, low liability limits, and restricted indemnity due to the market dominance and the necessity to use their services.[28] Smaller clients, especially in business-to-business dealings, may have minimal effective remedy but to adopt such arrangements, even in cases where they do not fairly represent the risks concerned.

This lopsidedness creates a central dilemma of achieving proportion and equity in cybersecurity negotiations. The character of the services, the sensitivity of the data under its care, and the capabilities of the contracting parties should, in principle, be aligned with the cybersecurity duties and liabilities required. But the balance is often destroyed by differences in bargaining power. The constantly changing nature of cyber threats requires a growing need for more equalised contracting mechanisms, which are oriented to risk-sharing, scalable compliance, and shared accountability, which in turn guarantees the effectiveness and commercial reasonability of cybersecurity clauses.

CYBER SECURITY PROVISIONS AND CONTRACT LIFECYCLE MANAGEMENT

The clauses of cybersecurity contained in commercial agreements do not exist as fixed requirements attached to a specific moment of the contract implementation; instead, they follow the whole lifecycle of the contract. A single re-evaluation of security measures, during the signing phase, cannot suffice in the context of cyber threats, technologies, and regulatory requirements, which vary quickly. A successful management of a contract life cycle (CLM) thus necessitates continued monitoring, control, and adjustment of cybersecurity requirements to ensure protection of data and systems remains intact. At its performance stage, parties need to be proactive in ensuring that they comply with the agreed cybersecurity standards. This can be in the form of periodic security audits, compliance reports, vulnerability assessments and

[28] Greenleaf G, Asian Data Privacy Laws (OUP 2014).

incident-response exercises. Contracts are increasingly requiring continuing obligations like patch management, updates on software and other infrastructure, training employees, and compliance with new standards or laws of the industry. These provisions take note of the fact that cyber risks are dynamic and that security frameworks have to change accordingly. In order to meet these changes, commercial contracts usually have provisions on the necessity to periodically review and amend cybersecurity requirements. Review clauses can allow parties to revisit security practices either yearly or when certain trigger events happen, e.g. a drastic shift in technology, a breach of data, a change in a regulatory requirement or the increase of services. The amendment provisions help the parties to revise security requirements without the need to revise the whole contract, and thus they retain flexibility without compromising the stability of the contract. The termination and post-termination aspects of a contract are also related to cybersecurity. Responsibilities in relation to the data returned, safe erase, confidentiality, as well as the ongoing notifications of breach, very often survive the dissolution of a contract. Failure to address these issues in CLM may put parties at risk of cyber threats despite the end of the contractual relationship. Overall, the introduction of cybersecurity provisions in the contract lifecycle management will guarantee that the contractual safeguards will be effective in the long term. An active, dynamic concept improves resilience towards emerging risks, regulatory adherence and increases trust between purchasing and selling organisations in an ever-growing digital business environment.

NEW TRENDS AND FUTURE PROJECTIONS

The fast development of digital technologies and the increasing level of sophistication of cyber threats are changing the way in which cybersecurity provisions are written and implemented in commercial contracts. With the increasing integration and reliance of organisations on intricate digital ecosystems, the contractual method of cyber risk management is also changing significantly.

Supply-Chain Security: The recent high-profile cyber-attacks have shed light on the areas of critical weakness in digital supply chains, showing that the cyber resilience of an organisation is often the minimum of its vendors or subcontractors. It follows that, going forward, commercial agreements will tend to place trickle-down cyber-security liabilities across the supply chain. Primary contractors can be obligated to require their subcontractors, vendors and

third-party service providers to comply with similar standards of cybersecurity.[29] The contract can provide due-diligence checks, flow-down, audit rights over subcontractors and the need to give timely notice to the upstream parties of any security incident. This tendency indicates that individual risk management has become more integrated and ecosystem-oriented at the level of cybersecurity.[30]

Risk of Artificial Intelligence and Automation: The growing use of artificial intelligence (AI), machine learning and automated decision-making systems is posing new cybersecurity and data-protection threats. The technologies tend to be data-intensive, intricate and ongoing in data processing, which increases the effect of a data breach, manipulation of algorithms, or loss of systems. In turn, the future clauses of cybersecurity will probably tackle AI-specific risks by adding the clauses of data integrity, model security, transparency, mitigating bias, and human supervision.[31] Responsibility of AI-related mistakes, system behaviour that has not been granted, and non-compliance with regulations may also be distributed using ways of contracts, which need more sophisticated and future-oriented contracting approaches.

Continuous Compliance and Reporting is an Issue: Most of the conventional cybersecurity provisions have been based on traditional models of compliance, where compliance with security standards is evaluated at specific periodic points in time. Nevertheless, the changing character of cyber threats is leading to a shift in the focus to continuous compliance and real-time monitoring. Future contracts can have requirements of continuous security evaluation, automated approval systems, and automatic reporting of vulnerabilities or incidents. These provisions help to increase the possibility of detecting early and responding quickly, minimise chances of systemic failures and encourage transparency among contracting parties. This development highlights a trend toward active and dynamic cyber risk management in commercial contracting processes.

LAST BP DRAFTING OF EFFECTIVE CYBER SECURITY CLAUSES

A delicate balance between the legal certainty, technical feasibility and commercial practicality is required in drafting effective clauses on cybersecurity. Cyber risks vary significantly by sectors, contractual settings, and technological setups and hence make a universal and one-fits-all approach irrelevant. One of the most notable best practices is the use of a risk-based

[29] WEF (2024).
[30] ENISA (2023).
[31] Schneier B, Click Here to Kill Everybody.

approach, as a result of which cybersecurity requirements are carefully adjusted depending on the nature of the rendered services, the data sensitivity involved, and the consequences of a cyber-attack.[32] Contracts involving critical infrastructure, personal data or financial information must have stricter protection level standards than those that involve low-risk or non-sensitive datasets. Another important practice is to involve technical and cybersecurity experts when drafting. Lawyers might be incompetent in admitting the expertise necessary to determine the sufficiency of technical protection; therefore, structural cooperation with information technology, information security and risk management staff is unavoidable. This interdisciplinary contribution would make the contractual obligations realistic, measurable, and in line with current technological possibilities, which would help to decrease the compliance risk. Congruency between the contractual and internal policies is also significant. The organisations need to ensure that the standard of cyber security, incident-response schedules and requirements, as spelt out in agreements, correspond with the internal structures and workflows. Misalignment may trigger unintentional contractual violations, including those that have adequately secured. The drafting should be based on clarity and enforceability. The clauses in cybersecurity also require the use of specific terminology, ensuring that the key terms or concepts in the text are stated or defined, i.e., the meaning of security incident, or data breach, and the roles, time requirements, and solutions. False or overly technical clauses might not be enforced easily and might lead to conflicts. Lastly, flexibilities are to be added to the cybersecurity clauses to provide for technology change and dynamic threats. The mechanism of review, amendment and reference to flexible industry standards allows contracts to survive through time, thereby providing resiliency and legality in the long term.[33]

CONCLUSION

The clauses of cybersecurity have become an inevitable and inseparable part of business contracts in the modern digital economy. With organisations increasingly becoming interdependent on digital infrastructure, cloud, and data-driven business, cyber risks have taken a pervasive and potentially disastrous nature. In turn, contractual systems which are targeted at cybersecurity imply a fundamental recognition that cyber risk is not the responsibility of one party only but is rather an activity shared by all parties and that needs to be explicitly divided and addressed, as well as implemented according to clear contractual provisions. Effectively

[32] ISO/IEC 27001:2022.
[33] NIST Cybersecurity Framework.

written cybersecurity provisions are capable of a host of important activities. They assign the task of pursuing security protection, defining standards of care and offering aspects of incident identification, reporting and resolution. This way, they minimise uncertainty, narrow the points of contention, and provide an ordered approach to the response to cyber incidents. These are crucial clauses as they are helpful in achieving adherence to emerging regulatory frameworks in the data protection sphere, privacy, information security, and reducing liability and reputation damages. As the aspect of digital dependence is increasingly becoming more interlinked and as the commercial ties strengthen, the contractual approach to cyber risk management is bound to become all the more prominent.[34] The appearance of new technologies with manipulative supply chains and cross-border information flows will make the situation with cyber threats even harder, and the stable or standard contractual provisions will become even more ineffective. The cybersecurity clauses in this respect should be dynamic, risk-sensitive and mitigating to the business goals and technological realities.[35]

Finally, properly developed cybersecurity provisions are the key to safeguarding a business's value and maintaining trust in business relations. Having contributed to the resilience against cyber threats by creating transparency, accountability, and collaboration between the parties of the contract, they help ensure the stability and integrity of the digital commercial ecosystem in the long term.

REFERENCES

1. Information Technology Act 2000 (India).
2. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.
3. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation) [2016] OJ L119/1.
4. International Organisation for Standardisation, *ISO/IEC 27001:2022 – Information Technology – Security Techniques – Information Security Management Systems Requirements* (ISO 2022).
5. National Institute of Standards and Technology (NIST*), Framework for Improving Critical Infrastructure Cybersecurity* (Version 2.0, 2024).

[34] OECD (2015).
[35] World Economic Forum (2024).

6. Organisation for Economic Co-operation and Development (OECD), *Digital Security Risk Management for Economic and Social Prosperity* (OECD Publishing 2015).
7. European Union Agency for Cybersecurity (ENISA), *Contractual Obligations and Cybersecurity in Supply Chains* (ENISA 2023).
8. United Nations Conference on Trade and Development (UNCTAD), *Data Protection and Privacy Legislation Worldwide* (UNCTAD 2023).
9. Greenleaf G *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP 2014).
10. Kuner C *Transborder Data Flows and Data Privacy Law* (OUP 2013).
11. Reed C and Angel *J Computer Law: The Law and Regulation of Information Technology* (7th edn, OUP).
12. Schneier B *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World* (W W Norton 2018).
13. Solove DJ *Understanding Privacy* (Harvard University Press 2008).
14. IBM Security, *Cost of a Data Breach Report 2024* (IBM 2024).
15. World Economic Forum, *Global Cybersecurity Outlook 2024* (WEF 2024).
16. Cavoukian, A. *Privacy by Design: The 7 Foundational Principles* (Information and Privacy Commissioner of Ontario).