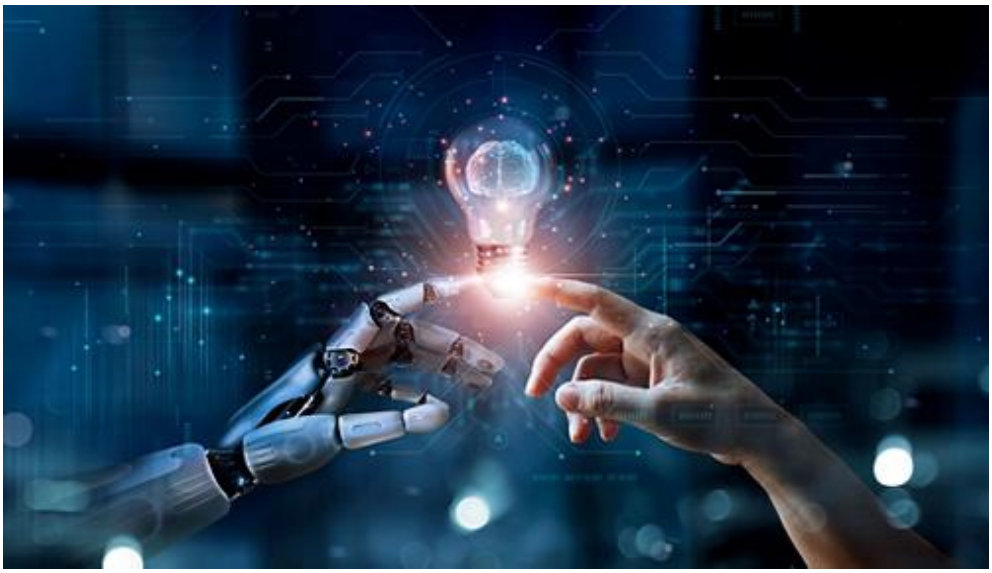
LEGAL UPDATE
NEWSLETTER

INSIDE THIS ISSUE



PREPARING FOR NEW CYBER COMPLIANCE DUTIES IN VIETNAM

OVERVIEW

Vietnam is entering a new phase in the regulation of digital activities, with authorities placing stronger emphasis on preventing cybercrime, reducing online fraud, and increasing accountability across the digital ecosystem. As online transactions, social platforms, cloud services, and digital financial tools continue to expand, the legal framework is also moving toward stricter oversight of how services are provided and how users behave in cyberspace. This direction reflects a broader policy concern that cyber-enabled misconduct is no longer limited to isolated scams or technical attacks, but has become a persistent threat affecting businesses, consumers, institutions, and vulnerable groups.

In this context, one of the most important issues for businesses is no longer whether cyber-related compliance will become more demanding, but how soon they should begin preparing for it. Even before any final rules take effect, the policy direction is already clear. Companies operating digital platforms, communications systems, payment tools, hosting environments, e-commerce services, or other internet-based solutions should expect closer scrutiny of user identification, data handling, reporting obligations, and cooperation with regulators. The likely shift is from reactive compliance to active prevention, requiring businesses to detect risks earlier and respond faster when violations appear.

A BROADER COMPLIANCE PERIMETER

A notable feature of Vietnam's current regulatory trend is the broadening of the range of entities that may be expected to carry compliance duties in cyberspace. In the past, many businesses may have assumed that cybercrime prevention was mainly the responsibility of law enforcement bodies, telecommunications operators, or a limited group of regulated intermediaries. That view is becoming increasingly difficult to maintain. The emerging approach suggests that responsibility may extend to a much wider set of actors whose services, infrastructure, or digital tools can be used in online misconduct.

This broader compliance perimeter matters because it changes how companies should assess legal risk. A business does not need to be a social media giant or a financial institution to become relevant in cybercrime prevention. A cloud-based service provider, a marketplace operator, a digital content platform, a logistics technology company, or even a business that manages user communities online may all find themselves expected to maintain stronger internal controls. The practical lesson is that businesses should not focus only on their industry label, but on whether their services can be misused in cyberspace.

This also means that legal exposure may arise not only from direct wrongdoing, but from inadequate prevention, delayed response, weak user verification, or failure to cooperate with competent authorities. For many companies, this is a meaningful shift. Compliance will increasingly depend on whether an organization has systems, processes, and governance structures capable of identifying suspicious conduct and acting on it in a timely manner.

FROM USER ACCESS TO USER ACCOUNTABILITY

Another likely development in this area is the stronger linkage between digital access and user accountability. For many years, online services were designed to reduce friction, make onboarding easy, and encourage rapid user growth. That commercial model may now need to be balanced against heightened expectations around identification, authentication, and misuse prevention. In legal terms, this reflects a move away from anonymous or lightly verified participation in digital spaces and toward a more traceable model of online activity.

For service providers, this may require a fresh review of how users register, how accounts are authenticated, how suspicious activity is flagged, and how access is restricted when abuse is detected. The issue is not only whether user data is collected, but whether it is collected in a lawful, proportionate, and usable manner for compliance purposes. Businesses may also need to review whether existing terms of service, privacy notices, escalation procedures, and internal incident workflows are aligned with the expectations of Vietnamese regulators.

For users, the policy direction also signals that digital participation carries corresponding legal duties. The use of an account, online group, or communication channel is no longer a purely private matter where responsibility ends with the content creator. If authorities continue along the current direction, individuals may be expected to safeguard their account information, avoid misuse by third parties, and support investigations when requested under applicable laws. This creates a more structured relationship between service access and legal accountability.

ONLINE COMMUNITIES UNDER CLOSER SCRUTINY

One of the most sensitive areas of cyber regulation concerns the management of online groups and communities. These spaces often serve legitimate and valuable purposes, including business networking, consumer support, public discussion, and social interaction. At the same time, they can be exploited for scams, misinformation, harassment, unlawful trading, or other harmful conduct. As a result, online communities are increasingly viewed not merely as neutral communication spaces, but as environments that require active oversight.

This has important implications for administrators, moderators, and platform operators. It is no longer sufficient to create a group and intervene only when a problem becomes obvious. The regulatory expectation is moving toward a model in which managers of online communities should establish rules, monitor content more carefully, respond to reports, and remove unlawful material within a reasonable time. Service providers may also be expected to support these efforts with technical tools, reporting channels, and verification mechanisms.

For businesses, this means that community management should not be treated as a minor operational function delegated without structure or legal support. Companies that host branded groups, customer forums, social commerce communities, or discussion spaces should consider whether they have clear moderation rules, appropriate training, escalation paths, and documented response procedures. The reputational and legal risk attached to unmanaged online spaces is likely to increase, especially where those spaces can be linked to fraud, abuse, or repeated harmful conduct.

FRAUD PREVENTION AS A CORPORATE DUTY

Online fraud has become one of the most visible and damaging forms of cyber-enabled misconduct. It evolves rapidly, adapts to user behavior, and often relies on impersonation, false information, manipulated images, fabricated payment evidence, and increasingly sophisticated digital tactics. Because of this, fraud prevention is no longer only a criminal enforcement issue. It is becoming a key part of corporate compliance and risk management.

Businesses should therefore examine how their own systems, brands, personnel, or communication channels could be exploited by fraudsters. A company may become part of a fraudulent scheme even without direct involvement, for example where scammers misuse its name, imitate its staff, forge transaction records, or create fake online pages that appear connected to the business. The result can be financial loss, reputational harm, customer complaints, and regulatory attention.

To reduce these risks, companies should consider strengthening customer communication protocols, internal verification procedures, reporting channels, and incident response frameworks. They should also review whether employees understand common fraud patterns and know how to respond when suspicious activity is reported. In many cases, the first sign of fraud does not appear in a legal notice or regulator request, but in a confused message from a customer, a complaint about a fake account, or unusual activity affecting a payment process.

An effective compliance approach should therefore combine legal review, technical safeguards, customer awareness, and internal coordination. Fraud prevention works best when it is embedded into business operations rather than treated as a separate emergency issue.

PROTECTING CHILDREN AND VULNERABLE USERS ONLINE

Another area likely to receive stronger legal and policy attention is the protection of children and other vulnerable users in cyberspace. This reflects a wider understanding that digital harm is not limited to financial scams or data breaches. It also includes coercion, exploitation, humiliation, unlawful collection of personal information, and the circulation of abusive content. As digital platforms become part of everyday life, the legal system is under growing pressure to respond more directly to these risks.

For businesses, this issue should not be seen as relevant only to social media companies or child-focused services. Any platform that allows interaction, content sharing, direct messaging, livestreaming, or user-generated participation may need to think carefully about how harmful conduct can arise and how it can be prevented. The legal, ethical, and reputational consequences of failing to address abuse involving children are severe, and companies should not assume that general content policies alone will be enough.

Practical preparation may include reviewing age-related safeguards, reporting procedures, moderator training, content escalation standards, and coordination channels for urgent cases. It may also involve reassessing whether personal data handling practices are sufficiently sensitive to the risks associated with minors and vulnerable users. As Vietnamese regulation continues to evolve, companies that take this issue seriously at an early stage will be better placed to demonstrate responsible conduct.

CONCLUSION

Although legal texts may still be developing, businesses should not wait for final implementation before taking action. Early preparation is often the most effective way to reduce future disruption. Companies should begin by identifying which parts of their operations are exposed to cyber-related compliance risk. This includes not only IT infrastructure, but also customer onboarding, online communication, account management, payment flows, data retention, moderation practices, and response coordination.

A useful starting point is a gap assessment. Businesses can review whether they have reliable identification and authentication processes, whether incident reporting is clearly assigned, whether suspicious conduct can be escalated quickly, and whether legal and technical teams are aligned on response obligations. Contracts, internal policies, user terms, and operational manuals may also need attention. In many organizations, the challenge is not the absence of effort, but the fragmentation of responsibilities across departments that rarely work together until a crisis occurs.

The likely future of cyber compliance in Vietnam is one in which preparedness, traceability, and cooperation carry increasing weight. Businesses that invest early in governance and control measures will be in a stronger position not only to comply with legal requirements, but also to build trust with customers, partners, and regulators. In a digital environment where risks move quickly and reputational damage spreads even faster, readiness is no longer optional. It is part of responsible business practice.

DAITIN & ASSOCIATES

Lawyers and Consultants

CONTACT

Please contact Daitin & Associates if you require any further information or guidance in the procedures of acquiring, protecting intellectual property rights in Vietnam | Cambodia | Laos | Myanmar | Thailand | Philippines | Brunei | Indonesia.

info@daitin.com.vn | www.daitin.com.vn