




MYANMAR CYBERSECURITY LAW, 2025

KEY INSIGHTS



This article is based on our understanding of the publicly available Cybersecurity Law, 2025. It may be affected by laws subsequently passed by the Myanmar government or notifications adopted by various ministries.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means – electronic, mechanical, photocopy, recording or otherwise – without the publisher's or copyright holder's prior written permission. This publication, and any form of copy of this publication, may not be sold, re-sold, hired out, or otherwise disposed of by trade by any person or entity without the publisher's or copyright holder's prior written permission. The information contained in this book is provided for information purposes only and is not intended to constitute legal advice. Legal advice should be obtained from qualified counsel for all specific situations.

For more information, please email us at myanmar@dfd.com or visit www.dfd.com.

CONTENTS

| | |
|--|----|
| INTRODUCTION | 6 |
| 1 REGULATORY OVERSIGHT | 7 |
| A. Regulating Bodies | 7 |
| B. Office holders of the Regulating Bodies | 8 |
| 2 SERVICES, LICENSING REQUIREMENTS AND PENALTIES FOR NON-COMPLIANCE | 9 |
| A. Services Regulated under the CSL | 9 |
| B. Responsibilities of the Cybersecurity Service Providers | 11 |
| C. Responsibilities of the Digital Platform Service Providers | 11 |
| D. Virtual Private Network: What is it, and how does CSL regulate it? . . . | 12 |
| E. Business continuity challenges | 12 |
| 3 DATA PRIVACY AND PROTECTION | 13 |
| A. CSL and ETL – two peas in the (personal data protection) pod | 13 |
| B. Comparison of Personal Data Provisions in ETL and CSL | 14 |
| C. Conflicts between ETL and CSL | 15 |
| 4 CRITICAL INFORMATION INFRASTRUCTURE | 16 |
| A. What is Critical Information Infrastructure under the Cybersecurity Law? | 16 |
| B. Non-compliance Penalties | 17 |
| 5 THREAT OF OFFENCE, OFFENCE, COLLECTION OF EVIDENCE AND PROSECUTION | 18 |
| A. Cybersecurity Threats and Cyberattacks, Collection of Evidence and Prosecution | 18 |
| B. Cybercrime, Collection of Evidence and Prosecution | 20 |
| C. Extra-territorial Jurisdiction | 20 |
| CONCLUSION | 21 |

FOREWORD

Cybersecurity has become more important than ever in an era where digital technologies play a crucial role in economic growth and national security. The Cybersecurity Law 2025 establishes a legal framework to safeguard Myanmar's cyberspace, protect critical information infrastructure, and combat cybercrime.

This law introduces regulatory oversight, licensing requirements, and enforcement mechanisms to enhance security in cyberspace. It also defines responsibilities for businesses, digital service providers, and government authorities to ensure compliance with cybersecurity standards.

By strengthening investigative capabilities, imposing penalties for cyber offences, and promoting cybersecurity cooperation, this law aims to create a safe and secure digital environment. Effective implementation and ongoing regulatory clarity will be essential to achieving these objectives as technology continues to evolve.

DFDL remains committed to supporting stakeholders with precise, innovative, and actionable legal insights. We trust that this article will serve as an information resource for understanding this new legislation and its implications for business operators in Myanmar.

Warm regards,

Nishant Choudhary
Partner & Managing Director, Myanmar
Head of Regional Dispute Resolution Practice



EXECUTIVE SUMMARY

The Cybersecurity Law, 2025 was enacted to establish a comprehensive legal framework for cybersecurity governance, critical information infrastructure protection, and digital platform regulation in Myanmar. It will become enforceable upon receiving the assent of the President.

The Cybersecurity Law, 2025 introduces measures to combat cybercrime, secure digital services, and promote cybersecurity compliance among businesses and individuals. It also guides investigatory and enforcement mechanisms by granting authorities the power to seize digital evidence, conduct forensic investigations, and impose penalties for cyber-related offences.

Further, the law establishes a hierarchical regulatory structure, with the Central Cybersecurity Committee overseeing

Summary of key concerns:

- Uncertain enforcement of licensing and compliance obligations.
- Potential conflicts with existing laws such as the Electronic Transactions Law.
- Risk of data privacy violations due to mandatory disclosure rule.
- Unclear government control over digital platforms.

policy direction, the Steering Committee managing implementation, and specialised work committees handling cybersecurity threats, cybercrime investigations, and regulatory enforcement. A dedicated Investigation Unit is tasked with identifying cyber threats, conducting inquiries, and collaborating with digital forensic laboratories, including the National Digital Laboratory, to analyse evidence pertaining to cyber-related offences.

The law introduces licensing requirements for cybersecurity and digital platform service providers, requiring them to obtain approval from the relevant authorities—non-compliance results in severe penalties,

including fines, license revocation, and imprisonment. Additionally, the law regulates Virtual Private Network services, mandating government approval before offering such services.

The law defines critical information infrastructure across key sectors, including defence, financial services, healthcare, and communications, imposing strict security requirements for data protection and emergency response planning. It also mandates data retention obligations for digital platform service providers, requiring them to store user data for three years and provide it to authorities upon request, raising potential concerns over privacy and regulatory compliance.

The law introduces stringent measures against cyberattacks and cybercrime, prescribing prison sentences ranging from six months to seven years and financial penalties for offences such as hacking, identity theft, online fraud, and data manipulation. The government is empowered to suspend, control, or shut down digital platforms deemed harmful to national security or public interest.

While the law provides a foundational legal structure for cybersecurity governance, its implementation challenges, including unclear procedural guidelines, undefined compliance criteria, and potential conflicts with existing laws (notably the Electronic Transactions Law, 2004, which it does not repeal) require further government clarifications.

Summary of potential business actions:

- Align with global cybersecurity standards to reduce compliance risks.
- Seek formal legal guidance on data retention and licensing obligations.
- Request clearer regulations through industry associations and direct engagement with policymakers.

INTRODUCTION

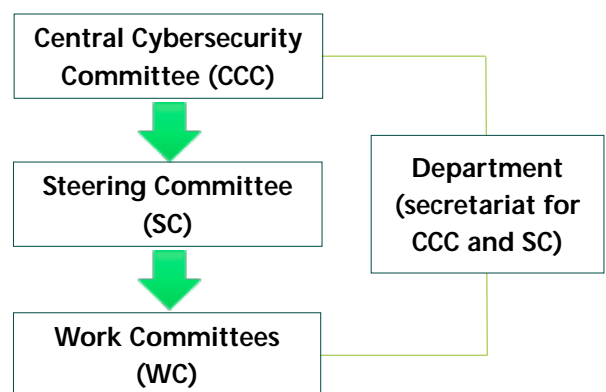
The Cybersecurity Law, 2025 (“CSL”) was enacted to establish a legal framework for cybersecurity governance, critical information infrastructure protection, and cybercrime prevention in Myanmar. It introduces regulatory oversight, digital and cybersecurity services licensing requirements, and enforcement mechanisms to address cyber threats.

In this paper, we discuss the broad scheme of CSL and comment on the potential pitfalls, business continuity challenges and criminal sanctions for cyberattacks and cybercrimes.

1 REGULATORY OVERSIGHT

A. Regulating Bodies

Below is a hierarchical representation of the nodal authorities under the CSL.



The CCC, SC and the WCs have been tasked with various works such as developing and overseeing cybersecurity policies, strategies, and operational plans, coordinating cybersecurity measures with international and regional entities while enhancing infrastructure and human resource development, supervising the storage of critical information and

Key concerns:

- No designated cybersecurity regulatory body or implementing Ministry.
- Difficulty for businesses to determine compliance expectations.

authorising cybersecurity teams, determining fees, fines, and regulations for cybersecurity and digital platform services and so on.

The SC establishes the WCs, which operate under its supervision and are responsible for preventing cybersecurity threats, cyberattacks, and misuse; assisting law enforcement in cybercrime investigations and risk assessments; mitigating secondary

risks arising from cyber threats; evaluating and monitoring cybersecurity levels across sectors and advising government entities; identifying, investigating, and addressing cybersecurity incidents; assessing services provided by cybersecurity and digital platform operators; and supporting the National Digital Laboratory and other digital labs.

The department serves as the secretariat for the CCC and the SC and is responsible for office operations. It may coordinate with international and regional cybersecurity organisations under the implementing ministry's directives, issue recognition certificates based on cybersecurity qualifications and competitions, and initiate sector-specific cybersecurity cooperation. Additionally,

it establishes regulations for cybersecurity services and digital platform registrations, imposes fees and fines in compliance with the law, and implements cybersecurity policies, strategies, action plans, and guidelines set by the CCC.

Potential business actions:

- Businesses should establish direct communication channels with regulatory bodies to stay updated on enforcement trends.
- Industry associations should seek clear procedural guidelines from the government.

B. Office holders of the Regulating Bodies

The CCC is chaired by the Vice-President, with the Union Minister of the relevant implementing ministry serving as Vice-Chairperson. Other members include Union Ministers and chairs from relevant Union-level organisations. A secretary and a joint secretary are also appointed. At this time, it is unclear which ministry will implement the CSL.

The SC is chaired by the Union Minister of the relevant ministry, with deputy ministers, permanent secretaries from relevant ministries, vice-chairpersons from Union-level organisations, cybersecurity experts, and NGO representatives as members. The director-general of the relevant department serves as the secretary.



Privacy
Please



2 SERVICES, LICENSING REQUIREMENTS AND PENALTIES FOR NON-COMPLIANCE

A. Services Regulated under the CSL

Cybersecurity service providers (“CSPs”) or digital platform service providers (“DPSPs”) must incorporate a company in Myanmar to provide said services. Evidently, there are no alternatives for providing these services without forming a local entity or establishing a business presence in the country.

Key concerns:

- No timeline provided for license issuance, leading to operational delays.
- No transition period for existing businesses, creating compliance risks.
- Unclear treatment of foreign service providers already operating in Myanmar.

DPSPs already providing platform services from offshore and qualifying the registration requirements per CSL, it remains unclear whether the government will take action against them immediately for non-compliance or, grant them a transition period to comply with the incorporation requirement. The former appears unlikely, making it reasonable for businesses to anticipate a transition period.

However, whether businesses choose to incorporate under the current circumstances or suspend operations and wait for a more favorable economic environment to incorporate their business will ultimately be their decision.

Potential Business actions:

- No timeline provided for license issuance, leading to operational delays.
- No transition period for existing businesses, creating compliance risks.
- Unclear treatment of foreign service providers already operating in Myanmar.

| Service | Meaning | Licensing requirements | Penalties for non-compliance |
|----------------------------------|---|--|--|
| Cybersecurity Services | Means services offered using cyber resources (such as computers, software, networks databases and related accessories) or similar technology and equipment and includes services that the relevant ministry may notify as cybersecurity services. | <ul style="list-style-type: none"> ▪ <u>Must be registered as a company</u> under Myanmar Companies Law. ▪ CSL does not mention a timeline for the regulator to issue these services' licenses. ▪ Apply for license renewal 6 months before expiry. | <p>Providing cybersecurity services without a license is punishable by 1 to 6 months imprisonment, a fine of MMK 1–10 million, or both, with all related evidence subject to government confiscation. Companies face a fine of up to MMK 10 million. The offence is cognisable. Operating with an expired license carries a MMK 1–5 million fine.</p> <p>Failure to follow the obligations under CSL would lead to administrative sanctions.</p> |
| Digital Platform Services | It is a service that allows users to express, send, distribute or use data information by using cyber resources (such as computers, software, network databases and related accessories) and similar systems or equipment. | <ul style="list-style-type: none"> ▪ License mandatory for platforms with over 100,000 users. ▪ <u>Must be registered as a company</u> under Myanmar Companies Law. ▪ CSL does not mention a timeline for the regulator to issue these services' licenses. It also provides no transition period for registration to existing platform services. ▪ Apply for license renewal 6 months before expiry. | <p>The penalty for operating digital platform services without a registered entity is MMK 100 million, with all related evidence subject to government confiscation. The offence is cognisable.</p> <p>CSL also mandates administrative penalties for non-compliance with certain legal obligations outlined thereunder, such as not retaining users' data for the mandatory three-year period or failing to take immediate action against cyberattacks.</p> <p>Failure to follow the obligations under CSL would lead to administrative sanctions</p> |

| Service | Meaning | Licensing requirements | Penalties for non-compliance |
|--------------------------------------|--|---|--|
| VPN Services | A service that utilises a specific system as a backup within the original network employs technology to ensure the secure linkage of networks. | Approval from the Ministry is mandatory for establishing or providing VPN services. | Establishing or providing VPN services without prior permission from the relevant ministry is punishable by 1 to 6 months imprisonment, a fine of MMK 1–10 million, or both, with all related evidence subject to government confiscation. Companies face a fine of up to MMK 10 million. The offence is cognisable. |
| Non-profit cybersecurity team | A group authorised by the Steering Committee to operate without profit for the nation’s cybersecurity activities per the guidelines set by the Steering Committee. | <ul style="list-style-type: none"> ▪ Must obtain approval from the Steering Committee. ▪ No profit-making allowed. ▪ Apply for approval within 6 months if formed before the law’s enactment | No specific penalties are mentioned under the CSL |

B. Responsibilities of the Cybersecurity Service Providers

CSPs must comply with all applicable legal and regulatory requirements, including the terms of their license, implement preventive security measures, and support cybersecurity monitoring and emergency response efforts. They must identify and warn their customers against potential cybersecurity breaches, maintain response plans for handling malware and cyberattacks, and promptly notify relevant stakeholders of such incidents. Additionally, they must adhere to international cybersecurity standards and safeguard user data.

Quite understandably, to effectively fulfil these obligations, local CSPs may benefit from knowledge-sharing partnerships with similar entities in jurisdictions that have evolved their cybersecurity legal framework to match the novelty of cybersecurity threats and incidents there.

The CSL also requires CSPs to submit “cybersecurity business reports following set criteria” to the relevant department. However, CSL does not specify the format, reporting frequency, or consequences for delayed submissions. Moreover, while CSL references “set criteria” for reporting, but this term remains undefined. The government will likely issue

further clarifications and establish ad hoc criteria to regulate these aspects.

C. Responsibilities of the Digital Platform Service Providers

The CSL states that DPSPs must comply with relevant laws (such as, for example, the E-Commerce Guidelines, 2020), obtain necessary approvals, and adhere to the conditions in their registration certificates. They must securely store user information according to regulatory requirements and ensure compliance when engaging in business or profit-making activities through digital platforms.

The DPSPs must implement measures to detect and manage harmful content, including material that incites hatred, disrupts unity, peace and stability, spreads false news or rumour, discloses sensitive content, exploits children, violates laws, harms reputations, infringes intellectual property, or promotes violence. They must promptly block, remove, or suspend such content when they detect it themselves or upon receiving official notification, following a ‘set criteria.’ However, the law does not define these criteria, leaving uncertainty regarding the standards DPSPs must apply.

Additionally, the basis on which DPSPs are expected to assess the accuracy of published news or information remains unclear. The extent of government oversight in enforcing these obligations remains to be seen.

The CSL further mandates that DPSPs retain user data, including their personal information, service usage records, and any data required by authorities, for at least three years. Further, the CSL states that ‘individuals or organisations, authorised under existing law’ may request this information in writing, and the DPSPs must comply with such request per specified regulations. We have analysed the pitfalls and the need for clarity regarding these two topics in Section III of this paper.

D. Virtual Private Network: What is it, and how does CSL regulate it?

CSL defines a ‘virtual private network’ as a secure system that is a backup within an existing network, using technology to ensure safe network connections (“VPN”). CSL requires VPN service providers to provide said services after obtaining the relevant ministry’s approval. It restricts the ‘establishment’ and provision of VPN services without prior approval of the relevant ministry. Furthermore, CSL stipulates a mix of fines and imprisonment for those violating this restriction (please see the table in [paragraph II\(A\)](#) above).

The term “establishing” a VPN is not defined in the CSL. Under the Interpretation of Expressions Law, 1973, legal provisions must be interpreted according to their ordinary meaning. Consequently, it is unlikely that “establish” would be construed to include “use” or similar activities. That said, it is unclear at this stage if one could argue that VPN services function as a tool enabling users—whether natural or legal persons—to establish a private network. In this context, “establishment” could then be construed as setting up of a backup communication network, which may be deemed to require prior approval from the relevant ministry. Consequently, using a VPN without such authorization could be viewed as a breach of the law.

However, unless further clarity is provided by the regulators by way of implementing regulation or other similar notification, it would be difficult to indicate precisely whether this reflects the intent of the lawmakers, as it would impose significant logistical challenges on users and obstruct legitimate business operations—an outcome that cannot be reasonably presumed to align with the intent of the CSL.

Further, the process and timeline for obtaining the approval to establish a VPN service in Myanmar is not currently explained in the CSL. It is likely that the government would provide further clarifications in this regard.

E. Business continuity challenges

The CSL grants the relevant implementing ministry the authority to take certain actions against CSPs in coordination with Union-level ministries and organisations, citing national defence, security, or public benefit as justifications. The ministry may conduct inspections or exercise control over cybersecurity and digital platform services if necessary. However, the CSL does not specify the circumstances under which such actions would be deemed necessary.

Regarding DPSPs, the implementing ministry, with the Union Government’s approval, may take the following measures in the public interest:

- Temporarily suspend services or electronic information;
- Temporarily control materials related to the services;
- Close or declare a digital platform service unsuitable for public use.

The CSL does not define “public interest” or “public benefit,” leaving broad discretion for the government to determine and enforce these measures. It is likely that the government may publish the specific criteria and process for implementing such actions in the future.



PRIVATE

3 DATA PRIVACY AND PROTECTION

A. CSL and ETL – two peas in the (personal data protection) pod

The CSL defines 'data' as data that can be stored in various forms in a network or a computer system. It does not, however, define 'personal data.' Only ETL defines 'personal data' as information that identifies or is capable of identifying an individual. As indicated in paragraph II(C) above, the CSL states that DPSPs must retain the 'personal data' of users, their usage records, and data set by the department from time to time for three years. One could infer that DPSPs must maintain all personal data that helps identify an individual, including potentially sensitive personal data that users may share, as part of platform access requirements.

Key concerns:

- No clear legal basis for data requests, raising concerns over potential misuse.
- No data minimization principles, contradicting global best practices in privacy protection.
- Uncertainty regarding cross-border data transfers, which could impact international businesses.

Further, CSL does not specify when this retention period begins. It is unclear whether it starts from the date the data is received or likely intended to apply for three years after users deactivate their accounts, and thus further clarification is needed in this regard.

CSL further states that ‘individuals or organisations, authorised under existing law’ may request this information in writing, and the DPSPs must comply with such request per specified regulations. CSL does not indicate the grounds on which the ‘individuals or organisations, authorised under existing law’ would seek such information.

The phrase ‘authorised under existing law’ potentially casts a wide net that would permit any government (including

any government-owned) entity to request for and obtain the above data from the DPSP, at any time, without the data subject’s consent.

Although it is not an uncommon feature of data protection laws of several jurisdictions for the government to request personal data from data controllers, those laws almost always state the basis for said request. However, there is no similar basis in the CSL.

The draft Cybersecurity Bill, 2022, included provisions on personal data protection, which are notably absent from the CSL. This raises the relevance of the Electronic Transactions Law, 2004 (last amended in 2021) (“ETL”), which addresses personal data protection, albeit in a very basic form. Since CSL does not repeal ETL, both laws may apply to certain overlapping areas, potentially causing uncertainty in their implementation.

Without government clarification, this ambiguity could create compliance challenges for businesses

Potential Business actions:

- Implement data governance policies aligned with international standards.
- Seek clarification from authorities on permissible data handling practices.
- Engage in industry advocacy efforts to push for privacy protections in line with the ETL.

B. Comparison of Personal Data Provisions in ETL and CSL

| Aspect | ETL | CSL |
|---|---|---|
| Definition of Personal Data | Defines personal data as information identifying an individual. | No specific definition; CSL focuses on users' personal data held by DPSPs. |
| Data Protection Officer | Personal Data Management Officer must ensure data security and compliance. | There is no dedicated officer role, but it mandates DPSPs to store user data. |
| Data Collection & Processing | Requires systematic storage, protection, and restricted use of personal data. | Allows authorities to request personal data from digital platforms. |
| Data Retention & Deletion | Data must be deleted after the retention period (undefined) | DPSPs must store user data for three years. |

| Aspect | ETL | CSL |
|---------------------------------|---|---|
| Disclosure & Sharing | Prohibits sharing personal data without the data subject's consent, except under the grounds mentioned in the ETL, such as court-mandated investigation/inquiry about a cyberattack or cybercrime such as hacking and so on. | Mandates disclosure to authorities when requested by said authorities. |
| Exemptions | Exceptions for law enforcement in national security cases. | Broad authority is needed for the government to seize, analyse, and access users' personal data. |
| Penalties | Imprisonment terms and fines are placed on the designated data protection officer for failure to protect personal data and anyone who discloses personal data without the consent of the data subject, creating misinformation to spread panic and carrying out cyberattacks (domestic and cross-border). | Fines and business sanctions on DPSPs for engaging in digital platform services with an expired license and continuing to provide services without renewing the license, violating provisions of the CSL. |

C. Conflicts between ETL and CSL

Both ETL and CSL classify cyberattacks as offences when committed with the intent to undermine state sovereignty, governance, the economy, the rule of law, or national security. However, while ETL prescribes specific penalties and imprisonment terms for cyberattacks, CSL does not. This lack of clarity raises concerns about whether cyberattacks will be subject to two different punishment regimes. Although it is likely that the government may come up with clarifications but the timeline for that is unclear. If not, then it could potentially be likely that the punishments will run concurrently and the offender will be required to serve the higher of the two punishments, similar to the provisions in this regard in the Myanmar Criminal Procedure Code. However in the absence of guidance from the relevant regulator, it would be difficult to say with precision that jurisprudence of Criminal Procedure Code will be imported on the application of ETL and CSL.

Another key issue is the non-consensual disclosure of personal data. ETL restricts the transfer of personal data without the data subject's consent but provides exceptions in certain circumstances, including:

- Cybersecurity, cybercrime, or related investigations by authorised government bodies.

- Criminal investigations or legal proceedings by designated authorities.
- National security concerns related to cybersecurity or cybercrimes.
- Actions taken under specific authority following established standards.

In contrast, CSL mandates that DPSPs provide users' personal data to the government upon request without specifying the legal grounds for such requests. This seems to create a direct conflict between the two laws—while CSL compels compliance, ETL prohibits disclosure without consent, except in defined situations. This inconsistency creates ambiguity in the legal framework and raises questions about the implementation of personal data protection under ETL. It is not unusual for a government to request personal data; however, such requests are typically grounded in a clear legal basis—something notably absent from the CSL.

It is also important to recognize that the CSL is a general law, whereas the ETL is a specialized law governing data protection. Under established common law principles, a general law cannot override a specific law. Accordingly, while the CSL may require DPSPs to disclose users' personal data to the government, it cannot do so in a manner that overrides the consent requirement under the ETL.



4 CRITICAL INFORMATION INFRASTRUCTURE

A. What is Critical Information Infrastructure under the Cybersecurity Law?

CSL identifies certain cyber resources and lists them as critical information infrastructures (“CII”), potentially implying that these resources are critical to the functioning of the state, its economy and security. CII encompasses cyber resources across sectors such as defence, e-government services, financial services, transportation, communications, healthcare, and energy, along with any additional sectors designated by the Union government. CSL also lists relevant organisations’ and government departments’ rights and duties in managing CII data.

Key concerns:

- Unclear criteria for CII designation – making it difficult for businesses to know if they’re subject to additional regulations.
- No defined cybersecurity standards for CII entities leading to potential arbitrary enforcement.
- Lack of guidance on how businesses should report security incidents



It mandates the CCC to direct Union Ministries and Union-level organisations to manage, plan, and implement cybersecurity measures to protect CII. This includes establishing emergency response teams and submitting annual cybersecurity reports.

Additionally, CSL mandates these entities to appoint a designated individual to manage CII data. However, it does not specify the eligibility criteria for this role. It is also unclear whether such a person would be appointed from within the government ranks or from a CSP with whom the government contracts to manage CII data.

Among other responsibilities, this individual must maintain CII data per prescribed standards, though CSL lacks clarity on these standards, leading to ambiguity regarding the scope of responsibilities. The individual must also accept, store, release and manage the CII data.

Additionally, they must submit an annual CII report to the relevant ministry through the appropriate government department. While the CSL does not include a predefined report format, the government is expected to issue such guidelines separately.

B. Non-compliance Penalties

If the individual designated to, among other things, manage CII data fails to do so (and if such person is not a government employee), then, upon conviction, such person may be imprisoned for up to six months or fined up to MMK 10 million, or both.

The CSL further prescribes that any unauthorised tampering with, destruction of, or damage to information related to CII constitutes an offence. Upon conviction, the offender shall be imprisoned for a term not exceeding three years, a fine not exceeding MMK 20 million, or both.

Potential business actions:

- Conduct internal risk assessments to determine if your business falls under CII regulations.
- Implement cybersecurity best practices to align with global regulatory expectations.
- Request formal guidance from authorities on security requirements and reporting obligations.



5 THREAT OF OFFENCE, OFFENCE, COLLECTION OF EVIDENCE AND PROSECUTION

A. Cybersecurity Threats and Cyberattacks, Collection of Evidence and Prosecution

Under CSL, cybersecurity threats refer to any action taken within the cyber domain using cyber resources or related technologies that compromise cybersecurity. Cyberattacks are defined as deliberate acts intended to harm, disrupt, or degrade national governance, financial systems, the economy, national security, public safety, or the rule of law. These attacks may involve interference with information and communication systems, including hacking, malware deployment, and denial-of-service attacks.

To investigate cybersecurity threats and cyberattacks, CSL provides for establishing specialised WCs under the SC to oversee identifying, assessing, and mitigating such incidents. The relevant WC may, per regulations, seize and analyse cyber resources from individuals suspected of involvement in cyber threats, cyberattacks, or cyber misuse, including those connected to such individuals. After conducting forensic



analysis, the relevant WC must return seized cyber resources under prescribed conditions.

CSL also states that the implementing ministry, with Union Government approval, may assign individuals or organisations to conduct data analysis and forensic examinations to proactively prevent cyber threats. It must also support telecommunications companies in verifying information and conducting forensic examinations as required.

SC authorises the Investigation Unit (an *ad hoc body*) to investigate, seize cyber resources from individuals suspected of involvement in cybersecurity threats or cyberattacks, and analyse digital evidence. CSL grants the Investigation Unit the power to confiscate computers, storage devices, and other digital assets, which can then be examined in the National Digital Laboratory or other approved forensic labs. These laboratories are responsible for conducting forensic investigations, analysing electronic evidence, and submitting expert findings for judicial proceedings.

Potential business actions:

- Monitor enforcement trends and ensure legal counsel is prepared for regulatory inquiries.
- Develop incident response plans to minimize risks in case of regulatory action.
- Engage with government agencies to seek clarifications on enforcement policies.

Key concerns:

- Unclear threshold for government intervention, creating risks of service disruption.
- Vague criteria for what constitutes cybercrime, leading to potential misuse.
- Extra-territorial jurisdiction, meaning Myanmar citizens abroad can be prosecuted under CSL.

CSL prescribes strict penalties for cyberattacks. Individuals found guilty of damaging cyber resources, deploying malware, or altering critical data can face imprisonment ranging from one to seven years, depending on the severity of the offence. Fines can range from K1 million

to K20 million. Additionally, offenders may have their equipment and digital assets confiscated as national property. CSL also allows authorities to take preventive measures, such as suspending digital platforms or controlling specific online content if it threatens national cybersecurity (as noted in the previous sections).

B. Cybercrime, Collection of Evidence and Prosecution

Cybercrime under CSL includes various offences committed using cyber resources or related technologies. These offences include unauthorised access to computer systems, data theft, online fraud, identity theft, and digital impersonation. Additionally, cyber misuse—such as modifying, transferring, or deleting computer programs without authorisation—falls under cybercrime. CSL also penalises disseminating false information, online defamation, and activities that incite violence or disrupt public order.

The Investigation Unit is the primary body responsible for investigating cybercrimes. It is empowered to seize digital evidence, analyse cyber resources, and conduct forensic examinations in collaboration with the National Digital Laboratory. Per CSL, digital forensic labs are critical in investigating cybercrimes by analysing seized data, verifying electronic evidence, and preparing expert reports for court proceedings. The findings of the National Digital Laboratory are legally binding and serve as final approvals in disputes over digital evidence.

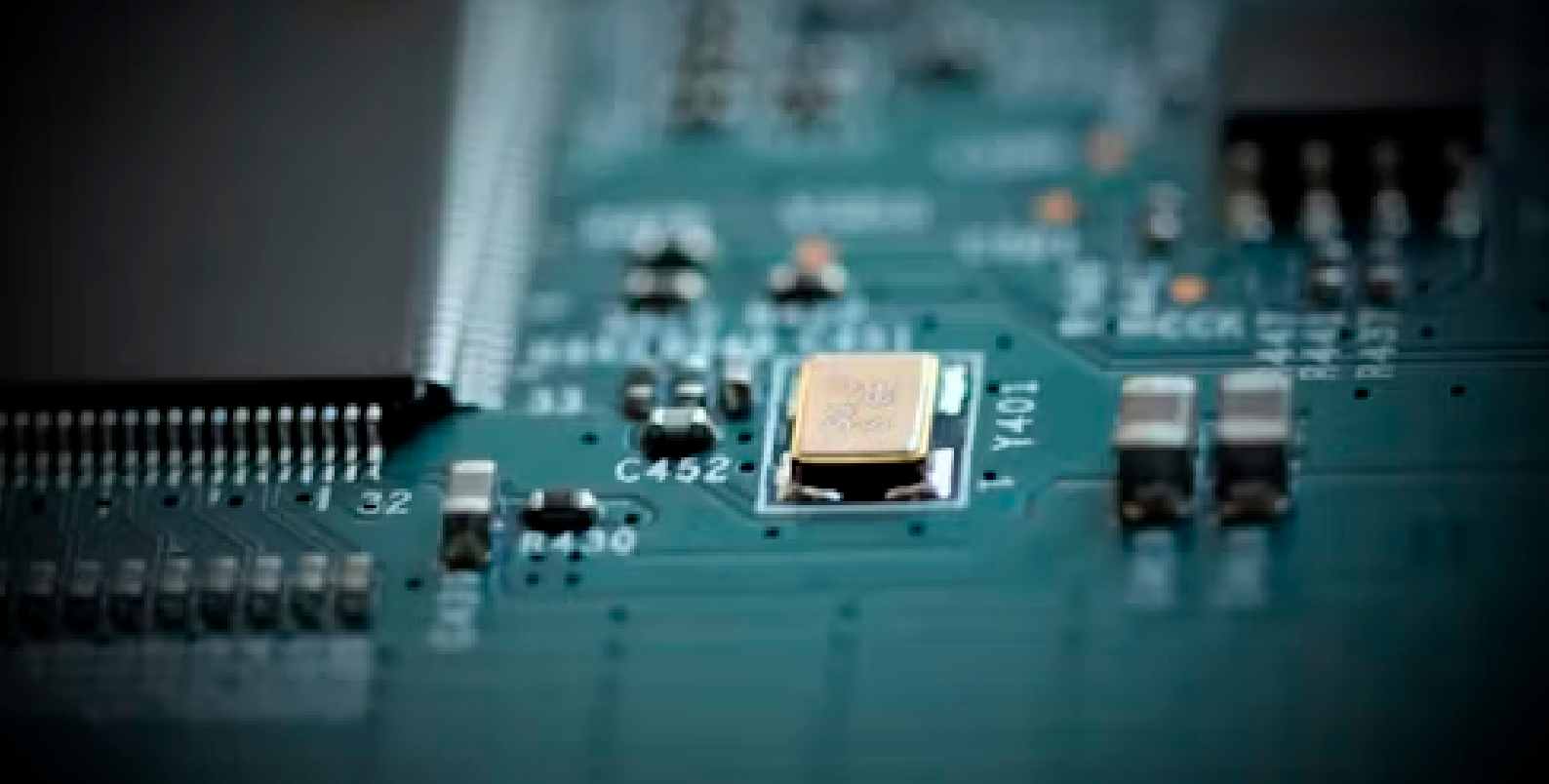
Punishments for cybercrime vary depending on the nature of the offence. Unauthorised access to computer systems, illegal data tampering, and cyber fraud can result in imprisonment from six months to three years, with fines ranging from K1 million to K20 million. More severe cyber offences, such as online financial fraud or theft, can lead to imprisonment of up to seven years. Companies operating digital services without proper registration or licensing may face substantial fines, with penalties reaching K100 million, and their assets may be seized. The law also includes provisions to blacklist non-compliant entities and permanently revoke their operating licenses.

To enhance cybercrime prevention and investigation, CSL mandates the implementing ministry to collaborate with telecommunication service providers, who must verify information and submit electronic records for forensic examination. In matters concerning national security, the government is authorised to inspect, control, or suspend digital services if deemed necessary. These measures ensure that cybercrimes are promptly addressed while maintaining public safety and national security.

C. Extra-territorial Jurisdiction

The CSL has extra-territorial jurisdiction, meaning that Myanmar citizens residing abroad are subject to its provisions and may be prosecuted for offences committed under its scope. The government may leverage extradition treaties with other countries to facilitate the return of offenders for trial and punishment. However, the practical enforcement of this provision remains uncertain.





CONCLUSION

The CSL represents a step in Myanmar's digital security framework. By establishing governance structures, licensing requirements, and enforcement mechanisms, CSL seeks to protect national security, prevent cybercrime, and enhance public trust in digital services.

However, CSL also raises concerns regarding data privacy, business continuity risks, and broad government oversight powers. The requirement for data retention and disclosure without explicit safeguards could pose challenges for DPSPs and user privacy rights. Furthermore, the lack of transition periods for compliance and the potential overlap with existing regulations (such as ETL) may create legal uncertainties for businesses operating in Myanmar's digital economy. We hope that further clarity will be provided by implementing CSL regulations and that different laws will be harmonised where necessary.

We also hope that the relevant ministry under the SAC will issue detailed guidelines, compliance roadmaps, and procedural clarifications to support stakeholders in adapting to the new regulatory environment. Collaborating with international cybersecurity organisations and industry stakeholders could help refine enforcement mechanisms and enhance Myanmar's cybersecurity resilience.

CONNECT WITH US



NISHANT CHOUDHARY

Partner & Managing Director

✉ nishant.choudhary@dfdl.com



SURATH BHATTACHARJEE

Senior Legal Adviser

✉ surath@dfdl.com



MYA MYINTZU

Legal Adviser

✉ myamyintzu@dfdl.com

DFDL Myanmar Limited,
134/A Thanlwin Rd,
Golden Valley Ward 1,
Yangon, Myanmar (Burma)

AWARDS & RANKINGS

DFDL is honored to have received recent awards from leading industry publications recognizing our achievements, including the following:

2025 Chambers Asia Pacific

Band 1 – Projects & Energy – Bangladesh
Band 1 – General Business Law – Cambodia, Lao PDR, Myanmar
Band 2 – Corporate & Finance – Bangladesh
Band 3 – Projects & Energy, Real Estate, Tax – Thailand
Band 3 – Corporate/MA, Projects, Infrastructure & Energy – Vietnam
Band 4 – Corporate/M&A – Thailand

2025 The Legal 500 Asia Pacific

Tier 1 – Leading Firm – Cambodia & Lao PDR
Tier 1 – Corporate and M&A/Projects and energy– Myanmar
Tier 1 – Tax – Vietnam
Tier 2 – Banking and Finance – Bangladesh
Tier 2 – Projects & Energy – Thailand & Vietnam
Tier 2 – Tax – Thailand
Tier 3 – Corporate and M&A – Bangladesh & Vietnam
Tier 3 – Restructuring and Insolvency – Thailand
Tier 3 – Real Estate and Construction – Thailand
Tier 3 – TMT – Thailand
Tier 4 – Corporate and M&A – Thailand

2024-25 IFLR1000

Active – Financial and Corporate – Bangladesh
Tier 1 – Financial and Corporate – Cambodia, Lao PDR, Myanmar
Tier 1 – Project Development – Cambodia & Myanmar
Tier 2 – Projects – Thailand & Vietnam
Tier 3 – Banking and Finance/Capital Markets: Debt/M&A – Thailand
Tier 3 – Banking and Finance/M&A – Vietnam
Tier 4 – Project development – Foreign – Singapore
Notable – Banking/M&A/Restructuring and Insolvency – Indonesia
Notable – Capital Markets: Equity/Restructuring and insolvency – Thailand
Notable – Capital Markets: Equity/Capital Markets: Debt – Vietnam

2024 Asia Business Law Journal

Thailand Law Firm Award 2024

Insolvency & Restructuring
Taxation

2024 Asia Legal Business (ALB) Asia M&A

Thailand Law Firm Award 2024

Tier 2 – M&A – Vietnam
Notable Firm – M&A – Thailand

2024-25 Asialaw

Cambodia
Firm of the Year
Practice Areas
Outstanding – General Business Law
Industry Sectors
Highly Recommended – Banking and Financial Services/Consumer Goods and Services/Industrials and Manufacturing

Lao PDR
Firm of the Year
Industry Sector
Highly Recommended – Banking and Financial Services/Infrastructure
Practice Area
Outstanding – General Business Law

Thailand
Industry Sector
Highly Recommended – Consumer Goods and Services/Technology and Telecommunications/Banking and Financial Services/Energy/Infrastructure
Recommended – Aviation and Shipping/Industrials and Manufacturing/Real Estate
Practice Area
Highly Recommended – Banking and Finance/Construction/Tax/Corporate and M&A
Recommended – Labour and Employment/Restructuring and Insolvency
Notable – Capital markets

Vietnam
Industry Sector
Highly Recommended – Energy
Recommended – Banking and Finance Services/Real estate
Notable – Consumer Goods and Services/Industrials and Manufacturing
Practice Area
Highly Recommended – Corporate and M&A/Energy/Tax
Recommended – Banking and Finance/Capital Markets

2025 World Tax & World Transfer Pricing

Cambodia Tax Firm of the Year 2021/2022

Active – Tax – Cambodia & Myanmar
Active – Transfer Pricing – Cambodia
Tier 2 – General Corporate Tax – Thailand & Vietnam
Tier 2 – Customs – Vietnam
Tier 3 – Transfer Pricing – Thailand & Vietnam



ABOUT DF DL

Pioneers in frontier markets of Asia

DFDL was established in 1994 and founded on a unique vision: to create an integrated legal and tax advisory firm, with in-depth knowledge of the developing jurisdictions in which we are based.

Our dedicated professionals exhibit the acumen and insight necessary to assist you in navigating the legal complexities and challenges. Drawing on a wide-ranging industry experience and finely tuned local knowledge in countries we operate in, we strive to provide concise, commercially focused and innovative advice.

DFDL has 12 offices, including collaborating firms, in Bangladesh, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam.

DFDL collaborated with the following local firms:

- Sarin & Associates, Cambodia
- Nusantara DFDL Partnership, Indonesia
- Robin Lynn & Lee, Malaysia
- Ocampo and Suralvo Law Offices, Philippines

DFDL in Singapore is qualified as a foreign law practice and is not licensed to practice Singapore law.



OUR SOLUTIONS

We are constantly adapting in fast-changing environments. As a full-service and fully integrated legal and tax firm, we remain focused on our fundamental mission: to bring you successful solutions and add value to your projects across Southeast and South Asia. We are committed to our clients' success and to providing them with commercially focused legal solutions that help them overcome their business challenges.



Anti-Trust and Competition



Employment



Aviation and Logistics



Energy, Natural Resources, and Infrastructure



Banking and Finance



Investment Funds



Compliance and Investigations



Real Estate and Hospitality



Corporate Advisory



Restructuring



Corporate, Mergers and Acquisitions



Tax and Transfer Pricing



Dispute Resolution



Technology, Media, and Telecoms

EXCELLENCE · CREATIVITY · TRUST
Since 1994

BANGLADESH | CAMBODIA* | INDONESIA* | LAO PDR | MALAYSIA* | MYANMAR | PHILIPPINES* |
SINGAPORE | THAILAND | VIETNAM

*DFDL collaborating firms

