Federal Council considers introduction of cyber incident reporting duty

20 December 2019 | Contributed by Walder Wyss

While many countries have introduced far-reaching obligations to report cyber incidents, Switzerland has not yet followed this lead. However, on 13 December 2019 the Federal Council adopted a report which considers key issues with regard to the introduction of a general reporting obligation for operators of critical infrastructure. The report also discusses possible implementation models. A decision is expected by the end of 2020. The press release is available in English, German, French and Italian.

Contrary to international trends, Switzerland has not yet adopted a general obligation to report cyber incidents. The current system is based on voluntary notification and information exchange via the Reporting and Analysis Centre for Information Assurance and, depending on the sector of activity (eg, nuclear, financial or telecoms services), mandatory notification to the supervisory authority. The introduction of a general obligation to report cyber incidents has been one of the objectives of Switzerland's National Strategy to Protect Switzerland Against Cyber Risks (NCS) (for further details please see "Federal Council to create new cybersecurity competence centre").

Based on the newly adopted report, the Federal Council will examine the following four implementation models:

- Introduction of a single reporting office. This solution would allow for the central collection of information, enabling a comprehensive and coordinated response to cybersecurity threats across industry sectors.
- Extension and strengthening of existing reporting offices. This model could rely on and extend experienced and reliable structures as well as the expertise of existing regulators.
- Decentralised reporting offices complemented by central reporting office. This mixed system would combine the first two models to make use of existing regulators' expertise while allowing a cross-sectoral and coordinated response to threats.
- Maintaining the current regulatory situation.

Further issues to be clarified include who will be subject to the reporting obligations and the types of incident to be reported. The obligations will most probably apply to companies operating critical infrastructures, which may comprise sectors such as energy supply, telecoms, finance and insurance. In addition, it will have to be determined which events will be considered as relevant security incidents triggering a reporting duty. Finally, it remains unclear how this general reporting obligation would be coordinated with the new notification duties under the revised Swiss Data Protection Act.

In view of the rapid development of cyber risks, the Federal Council's upcoming decision could have a considerable impact on the compliance obligations of companies in certain industry sectors. It will therefore be necessary to monitor developments in this area.

For further information on this topic please contact Jürg Schneider, Christophe Gösken or Florian Roth at Walder Wyss by telephone (+41 58 658 58 58) or email (juerg.schneider@walderwyss.com, christophe.goesken@walderwyss.com or florian.roth@walderwyss.com). The Walder Wyss website can be accessed at www.walderwyss.com.

AUTHORS

Jürg Schneider

Christophe Gösken

Florian Roth