JULY 2024

Stricter cyber security requirements ahead

VINGE

Against the backdrop of the current geopolitical climate and the increasing digitalisation, the EU is implementing the NIS 2 directive with the aim to strengthen the level of cyber resilience throughout the EU. The NIS2 Directive sets new requirements for businesses' cyber risk management and incident reporting. The new rules are proposed to be introduced in Sweden through a new law - the Cybersecurity Act (Sw. *Cybersäkerhetslagen)***. The Act imposes strict requirements and severe financial consequences for non-compliance.**

Background

The NIS Directives aim to achieve a high common level of cybersecurity within the European Union. The first NIS directive was adopted in 2016. Since then, the EU has recognised that the cyber threat has increased. The EU has therefore adopted a new directive, the NIS2 directive. The directive will apply from 18 October 2024 and will be implemented in Swedish law. The new Cybersecurity Act is proposed to enter into force on 1 January 2025 (without any transition period).

Will Your Business Be Covered by the New Rules?

The Cybersecurity Act is proposed to apply to both public and private actors (referred to as operators in the Act), across a range of sectors. The provisions of the Cybersecurity Act will apply to your business if the following conditions are met:

1. **the business operates, in whole or in part, in one of the listed sectors:** the rules apply to businesses operating in one of 18 sectors identified by NIS2 and the Cybersecurity Act,
2. **established in Sweden:** as a general rule, the Act applies to businesses established in Sweden; and
3. **the business fulfils the requirements of a 'medium-sized enterprise':** small companies will, generally, not be affected, see below.

Covered Sectors

The Cybersecurity Act is proposed to cover 18 different sectors. Assessing whether a business is considered to operate in a relevant sector is not always straightforward.

The requirements will apply to the entire business. This means that if any part of the company's business is conducted in one of the listed sectors, the entire company's business will be subject to the rules.

The Sectors That Will Be Covered Are:

Energy
Includes, among others, companies selling electricity to customers (both end-users and retailers), charging operators, district heating and cooling operator and actors active in gas and hydrogen production, supply etc.

Transport
Includes, among others, airlines, airports, railway operators including service providers, operators of intelligent transport systems and maritime passenger and freight operators.

Banking
Credit institutions, i.e. companies whose business is to receive deposits from the public and to grant credits for their own account.

Financial Market Infrastructure
Stock exchange and trading platforms.

Health and Medical Services
Hospitals and clinics, businesses that develop or manufacture medicines or medical devices listed by the National Board of Health and Welfare (Sw. *Socialstyrelsen*) as critical to public health.

Drinking water
Includes businesses that manage drinking water pipes and networks, as well as businesses that distribute bottled water to customers or businesses.

Wastewater
Companies dealing with domestic or industrial wastewater.

Digital Infrastructure
Includes providers of cloud services, data centers and network services. Further, includes providers pf trusted services (such as electronic identification or certificates for website authentication), public electronic communication networks and electronic communication services available to the public.

Operators providing public electronic communication networks or publicly available electronic communication services are **not** required to be established in Sweden to be covered by the law. Such businesses will fall within the scope of the Act if the operator offers services in Sweden.

ICT Services
Operators providing services related to the installation, management, operation or maintenance of information and communication technology products, networks, infrastructure, systems, etc.

Public Administration
Public operators such as state authorities, with some exceptions, counties and municipalities.

Space
Operators of land-based infrastructure supporting space-based services such as satellite communication.

Postal and Courier Services
Providers of services that are part of the postal and courier supply chain, such as the collecting, sorting, transportation and delivery of postal items.

Waste Management
Operators whose main activity is waste management.

Manufacture, Production and Distribution of Chemicals
Operators that manufacture, produce or distribute certain chemical substances, mixtures or articles, as defined in the REACH Regulation.

Production, Processing, and Distribution of Food
Operators engaged in industrial production or processing of food.

Manufacturers of Certain Products
Includes manufacturers of a wide range of products, such as medical products, computers, electronic goods, optics, electric motors, generators, motor generators, household appliances, trailers and semi-trailers.

Digital Suppliers
Includes providers of online marketplaces where consumers can enter into purchase agreements with other consumers or with traders, search engines and social media.

Research and Development
Organisations whose main focus is research, with the aim of using the results for commercial purposes.

The Size Requirement

As a general rule, in order to be covered by the Act, a business must:

1. have at least 50 employees: *or*
2. have an annual turnover exceeding €10 million.

This means, in general, that small businesses will not be affected. Turnover is assessed on a group basis, including partner enterprises. The implication is that even a company that does not fulfil the size requirement as a separate legal entity may do so because of, for example, its parent company.

Some identified businesses will be covered regardless of size. The Swedish Civil Contingencies Agency (Sw. *Myndigheten för samhällsskydd och beredskap*) will have the authority to designate critical businesses to fall within the scope of the Act.

Further, the Cybersecurity Act is proposed to contain several exceptions to the size requirement. For example, exceptions apply if the operator is of particular importance at regional or national level, if a disruption to the service provided by the operator could have an impact on human life and health, or if the operator provides public electronic communications networks or is a provider of trusted services.

Business out of scope –Indirectly Impacted?

Even for companies not covered by the Cybersecurity Act, the Act may have an indirect effect. Operators covered by the Act will have an obligation to take risk management measures vis-à-vis their suppliers and service providers. For suppliers to companies covered, the law will thus have an indirect effect.

Main Provisions of the Cybersecurity Act

Obligation To Notify

An operator covered by the Act must register with its supervisory authority and provide information such as identity, contact details and activities. The supervisory authority varies according to sector. Indirectly, the notification requirement means that all organisations need to assess whether or not they are covered by the Cybersecurity Act.

Obligation To Take Risk Management Measures

The new Act imposes a responsibility on operators to implement risk management measures - more specifically, an obligation for businesses to protect network and information systems and their physical environment against incidents.

The measures taken must be based on risk analysis, be proportionate and be continuously reevaluated.

The measures must cover the following:

1. incident management;
2. business continuity management;
3. security in the supply chain;
4. security in the acquisition, development and maintenance of network and information systems including vulnerability management and vulnerability information;
5. strategies and procedures for the use of cryptography and encryption;
6. staff security;
7. access control and asset management strategies;
8. secured solutions for communication, and solutions for authentication.

Obligation To Report Incidents

The Act imposes an obligation to report "significant incidents" to MSB. An operator must notify MSB of the incident within 24 hours of the operator becoming aware of the incident. Furthermore, a formal incident notification must be handed in within 72 hours and a final report must be prepared within one month.

The following definitions of 'significant incident' are proposed:

1. an incident that has caused or may cause serious disruption to the service provided or financial damage to the operator concerned; or
2. an incident that has affected or may affect other natural or legal persons by causing significant tangible or intangible damage.

Management Responsibilities

The proposal clearly states that the management body of the operator is responsible for approving and monitoring the implementation of the risk management measures. For limited companies, the management body means the board of directors, the managing director and the deputy managing director. The proposal makes it possible to prohibit such persons from exercising management functions due to violations of the Act.

Furthermore, management is required to undergo training on risk management while employees must be offered similar training.

Sanctions

The supervisory authorities may impose fines if an operator violates the Cybersecurity Act. According to the proposal, the Act establishes more severe penalties compared to current legislation. The maximum fine will be the highest of:

1. **2 per cent** of the operator's total worldwide annual turnover in the preceding financial year; or
2. **ten million euros**.

Additionally, it is proposed that supervisory authorities will have the authority to order operators to take remedial action, to publish information on breaches of the provisions of the Act and to inform people and organisations that may be affected by a significant cyber threat.

How Can Organisations Prepare?

- Analyse whether your business or any of your customers can be expected to be covered by the rules.
- Identify the relevant supervisory authority and monitor news regarding the notification process.
- Develop a clear policy for monitoring and complying with the new legal requirements. Remember management's liability!
- Review the organisation's existing incident management procedures and incident reporting to identify whether they need to be updated to reflect the new requirements. If the company does not have such procedures, they need to be adopted.
- Review the supply chain security - contracts may need to be renegotiated to include cybersecurity requirements for suppliers.

What Happens Next?

The inquiry is expected to present its final report on cybersecurity in the autumn 2024, after which the government is expected to present a bill on the Cybersecurity Act.

Guidance and regulations related to the implementation of the NIS2 Directive and the Cybersecurity Act are also expected to be published in the coming months.

Vinge continuously monitors developments. Feel free to contact us if you want to know more.

Contact Us

Sofie Nordgren
Partner, Lawyer
sofie.nordgren@vinge.se

Lisa Bourghardt
Counsel, Lawyer
lisa.bourghardt@vinge.se

Henrik Borna
Partner, Lawyer
henrik.borna@vinge.se