Delphi

Cybersecurity 2023

Trends and Developments

Agne Lindberg / Partner / Advokat, **Felix Makarowski** Senior Associate / Advokat & **Petri Dahlström** / Associate

Delphi

Cybersecurity 2023

Trends and Developments

Agne Lindberg / Partner / Advokat, **Felix Makarowski** Senior Associate / Advokat & **Petri Dahlström** / Associate

The article was first published in the Chambers Cybersecurity 2023 Global Practice Guide.

Introduction

Cybersecurity has become a hot topic in Sweden in recent years, with several high-profile cyber-attacks and IT incidents taking place and being reported by the national media. For example, in late 2022, a suspected cyber-attack caused the Swedish federation of unemployment insurance funds (Sw. *Sveriges A-kassor*) to shut down a key IT system for several days, leading to a delay in unemployment benefits payments. However, while disruptions to critical systems are among the most severe cybersecurity-related risks most organisations face today, they are hardly the only ones – with loss of data, exposure of confidential or trade secret information, high administrative fines, and bad-will from the public also representing significant risks.

In Sweden, cybersecurity regulation is still in its infancy. Cybersecurity is largely considered an IT matter and it is, therefore, in most cases up to each organisation to individually set its cybersecurity standards and safeguard its IT systems. Most regulatory initiatives in Sweden to date have come from the EU – such as, eg, the NIS1 and NIS2 directives, the Cyber Security Act and the GDPR. Below, we will discuss EU law solely in relation to national developments in Sweden. In addition to regulatory requirements, information security is also a top priority for stock exchange requirements.

In practice, most regulatory requirements have not only a direct effect but may also have an indirect effect. Direct effect refers to the impact of the regulatory requirements on organisations and persons within the scope of the relevant statutory provisions. Indirect effect, meanwhile, refers to the regulatory requirements being passed down to suppliers and subcontractors outside the direct scope of the relevant statutory provisions through contracts. In our experience, questions related to risk management and implementation of regulatory requirements through contracts are often subject to significant amounts of negotiation between customers and suppliers.

Protection of National Security Interests

Introduction

Protective security refers to preventative measures taken to protect the security-sensitive activities of public agencies and companies against espionage, sabotage, terrorist offences and other crimes that might threaten their operations. Security-sensitive activities are activities that are of importance to Sweden's security or are covered by an international protective security commitment that is binding for Sweden. Additionally, protective security also refers to the protection of security-sensitive information.

The scope of the Swedish Protective Security Act (2018:585) (Sw. *Säkerhetsskyddslagen*) is vague. The assessment of whether an organisation falls under its scope is based on whether an activity is of importance to Sweden's external or internal security. If an activity falls into one of these areas, the activity falls within the scope

of the Protective Security Act. Sweden's external security refers to, inter alia, Sweden's defence capabilities and any related activities. Sweden's internal security refers to the ability to maintain and safeguard Sweden's democratic form of government, its judiciary and its law enforcement capabilities as well as the protection of some critical facilities, functions and information systems.

The scope of the Protective Security Act is vague, with the result that many different types of organisations within a variety of fields fall within its scope. While some organisations – such as, eg, the Swedish Armed Forces, the Swedish Parliament and the Swedish Government – fall squarely within the scope of the Protective Security Act, it may be less obvious that some other organisations (especially some private companies) do so. Public authorities or private companies within certain sectors, such as, eg, the defence industry, energy industry, water and sewage, banking, healthcare, digital infrastructure, artificial intelligence and the automotive industry could potentially fall within the scope of the Protective Security Act. It is up to each organisation to determine whether it conducts security-sensitive activities or processes security-sensitive information, and the assessment must be made on a case-by-case basis.

Under the Protective Security Act, all public authorities or companies carrying out security-sensitive activities ("operators") must ensure that the security-sensitive operations and information are sufficiently protected. This obligation carries over in cases where external suppliers may gain access to the security-sensitive operations or activities. The Protective Security Act contains provisions to ensure that sufficient protection is guaranteed. The most important of these provisions are summed up below.

Obligation to enter into a protective security agreement

All suppliers and subcontractors that will be granted access to certain categories of security-sensitive information and operation must enter into a protective security agreement with the operator. The protective security agreement sets out the relevant security provisions that will apply to the supplier and any subcontractors in their performance of services for the operator – including a provision on approval by the operator of any subcontractors to be used by the supplier.

Security screening of personnel

All personnel of the supplier or subcontractor that may gain access to the security-sensitive activities or information must undergo a security screening. This obligation also extends to the board and management of the supplier or subcontractor. The security screening is conducted by the operator, but any background checks are conducted by the Swedish Security Police (Sw. *Säkerhetspolisen*) on request by the operator.

Screening of contracts

All contracts where an external party may gain access to security-sensitive activities or information are subject to a special protective security assessment and suitability assessment by the operator. In case the operator finds that the contract is not unsuitable from a security perspective, the operator must consult with the supervisory authorities, which essentially amounts to a security screening of the contract. If the operator fails to consult with the supervisory authorities, the supervisory authorities may initiate the consultation.

During the consultation, the supervisory authorities may order operators to take measures to ensure that the operator is fully compliant with the Protective Security Act and all regulations that follow from it. If the operator fails to implement such measures, or if the supervisory authorities find that the contract is unsuitable from a security perspective, the supervisory authorities may prohibit the operator from entering into the contract. Failure to abide by such a decision could result in a fine of not less than SEK25,000 and not more than SEK50 million for the operator.

Restrictions on which suppliers and subcontractors may be used

In addition, the Swedish Security Police's regulations on protective security contain obligations related to screening of all IT equipment on which security-sensitive information will be stored. Further, from 1 January 2025, operators will not be permitted to provide access to security-sensitive information to organisations in countries with whom Sweden has not entered into a bilateral security

agreement. The list of countries with whom Sweden has entered into bilateral security agreements mainly includes EU member states, with a few non-EU countries such as the USA, the UK and Canada also included.

Impact of the Protective Security Act on contracts

The Protective Security Act sets high security standards for operators – standards that in many cases must be passed on to suppliers through contracts. This has multiple effects. First, it has a chilling effect on outsourcing, where operators may be afraid of or prohibited from outsourcing certain functions. As security must be maintained throughout the supply chain if any subcontractors are granted access to security-sensitive information or operations, the suppliers are under pressure to pass on the requirements to the subcontractors. This can lead to difficult negotiations with the subcontractors and may in some cases not be possible if the subcontractors are unwilling to take on the costs and risks required to meet the high security standards set forth in the Protective Security Act and the protective security agreements.

Nasdaq's Requirements for Governance and Information Security

Nasdaq Stockholm has established requirements for governance and control in listed companies. Listed companies must identify material risks in their IT systems and implement internal governance documents, such as an IT policy and information security guidelines (including cybersecurity). In addition, listed companies are required to implement systems and routines for sharing information and for financial reporting.

Under the Nasdaq rules, the Board of Directors of a listed company is responsible for the company's governance and control, including any business activities carried out by external parties. For outsourced activities that in any way have or are intended to have a connection with the company's disclosure of information, financial reporting, regulatory compliance, or other areas deemed material to the company, the company's governance documents should set out how the company ensures that the external party maintains appropriate and effective internal control over the parts of the business that the external party delivers. In this regard, the agreement between the company and the external party should govern the relevant control mechanisms as well as the evaluation of the control mechanisms.

Use of Cloud Services in the Public Sector

Since 2018, a debate concerning the use of cloud services has put the Swedish public sector in a state of uncertainty. In essence, the debate can be expressed as two separate issues:

- Does using cloud services provided by US cloud service providers to store classified documents amount to an unauthorised disclosure of the classified documents under the Swedish Public Access to Information and Secrecy Act (2009:400) (Sw. *Offentlighets- och sekretesslagen*)?
- Is using cloud services provided by US cloud service providers compliant with the security requirements for processors under GDPR Article 28(1)?

Both issues stem from an interpretation of the relevant legislation in conjunction with the US CLOUD Act, under which US authorities can, in certain cases, require US cloud service providers to disclose information stored in the cloud. It has been argued that it is not legally possible to use cloud services if confidential data is made technically available to a service provider that is bound by the rules of another country, according to which the provider may be obliged to hand over information without the use of international legal assistance or other legal basis under Swedish law.

In 2019, the Swedish Government initiated an investigation into the Swedish Public Access to Information and Secrecy Act matter, the results of which were presented in December 2021. The investigation concluded that Swedish authorities do not act in violation of the Public Access to Information and Secrecy Act if they use US cloud service providers. Neither the risk that a US authority will request data from a cloud service provider nor the fact that a cloud service provider could potentially disclose data to US authorities amounts to an unauthorised disclosure of classified information under the Public Access to Information and Secrecy Act. The conclusion of the investigation was welcomed by public

authorities and Swedish and US cloud service providers alike, many of whom have operations or customers in the US and may therefore fall under the scope of the US CLOUD Act. However, this is still at a proposal stage.

Due to the legal uncertainty, many public authorities in Sweden have been hesitant to use cloud services provided by US cloud service providers, which has had a significant negative impact on the digitalisation of public authorities.

Confidentiality Obligations for IT Outsourcing Suppliers

On 1 January 2021, the Act on Secrecy in Public Sector Outsourcing of Technical Processing or Storage of Data (2020:914) (Sw. *Lag om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter*) entered into force. The act's purpose is to make it easier for public authorities to outsource IT services to private IT suppliers. The act imposes a duty of confidentiality on anyone who, by employment or otherwise, is or has been involved in carrying out technical processing or technical storage of data on behalf of a public authority.

The obligation of professional secrecy for employees of private operators is intended to be equivalent to that applicable to the authorities' staff in corresponding cases. As is the case for public employees, breach of confidentiality by employees of IT suppliers may give rise to criminal liability under the Swedish Criminal Code (1962:700) (Sw. *Brottsbalken*), which carries a maximum penalty of imprisonment of up to one year. The obligation of professional secrecy applies during and after employment with the IT suppliers and subcontractors concerned.

For the obligation of professional secrecy to apply, the assignment must relate solely to technical processing or storage of data. It may, for example, concern actions related to the introduction, management, development and decommissioning of a service or the introduction of additional services and support services. The obligation may also cover activities related to back-ups, upgrades and updates, and export of information when a service is discontinued.

Recent Developments Concerning the GDPR

The Swedish Data Protection Authority (DPA) (Sw. *Integritetsskyddsmyndigheten*) has been quite active in its supervision of the GDPR in Sweden. Looking at its decisional practice, enforcement of the GDPR's requirements on appropriate technical and organisational measures has been among the DPA's priorities in recent years.

Investigation of the 1177 incident

Following an investigation, the Swedish DPA announced a decision in the 1177 case. The investigation was launched in 2019 when recorded calls to 1177, a healthcare service owned by all of Sweden's regional councils (Sw. *Regioner*), were made openly available on the internet. In its decision, the Swedish DPA concluded that the companies MedHelp and Voice Integrate were mainly responsible for the incident. MedHelp, the data controller, answered calls to 1177, while Voice Integrate, the data processor, was responsible for the switchboard functionality and call recording on behalf of MedHelp.

The incident occurred due to a security weakness in Voice Integrate's server. Through a misconfiguration, the server could be accessed from the outside, allowing access to unencrypted communication. As a result, a large number of calls became accessible, without password protection or other security measures, to anyone with an internet connection. All that was required was knowing the server's IP address.

The Swedish DPA found that the personal data involved was sensitive and subject to confidentiality. The companies had thus failed to protect the personal data against unauthorised access or unauthorised alteration. They had therefore failed to comply with their obligations as data controller and data processor to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The Swedish DPA further stated that both MedHelp and Voice Integrate lacked effective procedures for regularly testing, examining and evaluating the technical and organisational measures required to fulfil their obligations.

It is important to highlight that it is not sufficient to develop a system that ensures an adequate level of security at

the time of development. The obligation also includes a requirement to continuously review and ensure that the security is adequate in relation to the risk. As a result of the investigation, the Swedish DPA issued fines amounting to slightly over SEK13.5 million.

Other investigations of note concerning technical and organisational measures

In December 2020, the Swedish DPA concluded an investigation of eight healthcare providers. The primary focus of the investigation was whether the healthcare providers had conducted the needs and risk assessment required to assign adequate access authorisation for personal data in the electronic health records to personnel. The investigation concluded that seven of the eight healthcare providers did not limit access authorisations for personnel in the patient journal system to what was strictly necessary for the performance of their tasks. The deficiencies resulted in administrative fines between SEK2.5 million and SEK30 million.

In January 2022, the Swedish DPA published a decision following an investigation into the Uppsala regional council's handling of personal data. The first part of the investigation concerned sensitive personal data and personal identity numbers sent by email. The Swedish DPA found that the transmission of emails was encrypted, but that the information and patient data contained in the emails were not. Some of the emails were automatically sent to relevant regional health administrations, while other emails were sent manually to researchers and doctors within the region.

The second part of the investigation concerned how the Uppsala regional council sent emails containing patient data to patients and referrers in third countries. The Uppsala regional council had sent unencrypted sensitive personal data over an open network and had also stored sensitive personal data in the email hosting service Outlook. As a result, the Swedish DPA imposed a total fine of SEK1.9 million on the Uppsala regional board for the deficiencies identified regarding the hospital's technical and organisational measures.

Swedish Implementation of the NIS2 Directive

In early 2023, the NIS2 directive entered into force, with the EU member states having until 17 October 2024 to transpose the NIS2 directive into national law. The NIS2 directive is discussed in the 2023 Introduction to the Guide. Hence, we will not go into depth on the differences between the NIS1 and the NIS2 directives. Worth noting is that there are significant differences between the two directives: for example, in terms of the NIS2 having a wider scope and containing more detailed security requirements than the NIS1 directive. Many operators of essential and important services will likely have to invest significant resources to meet the requirements of the NIS2 directive, not least when it comes to renegotiating agreements to pass on new regulatory requirements to their suppliers and subcontractors.

NIS Supervision in the Digital Infrastructure Sector

The Swedish Post and Telecom Authority (Sw. *Post- och telestyrelsen*) (PTS) is the supervisory authority for essential services in the digital infrastructure and digital services sectors under the Swedish NIS Act, which implements the NIS1 directive into Swedish law. In September 2022, the PTS announced that it had initiated supervision of three operators of critical services in the digital infrastructure sector that provide domain name system services and top-level domain registries. The current supervision, which is scheduled and not prompted by any specific event or incident, concerns the operators' work with risk analyses and risk assessments.

To comply with the NIS Act's requirements, operators of essential services must carry out a risk analysis, forming the basis for the providers' technical and organisational security measures. The PTS's regulations and general guidelines on security measures for essential services in the digital infrastructure sector (PTSFS 2021:3) (Sw. *Post- och telestyrelsens föreskrifter och allmänna råd om säkerhetsåtgärder för samhällsviktiga tjänster inom sektorn digital infrastruktur*) provides a more detailed description of the expected contents of the risk analysis. The risk analysis must be documented and updated annually and include an action plan. It should identify the relevant threats and risks, the effectiveness of existing security measures in relation to the risks, and the negative consequences that an incident could have.

Concluding Remarks

A fundamental problem in cybersecurity is the inherent vulnerability of all digital solutions, which in many cases make attractive targets for cybercriminals and state-sponsored hackers looking to make quick money, steal confidential and classified information or cause disruption to important services.

While cybersecurity is still widely viewed as an IT matter to be handled individually by each organisation, there have been some legislative initiatives in recent years. Most of these have come from the EU, but there have also been some initiatives on a national level in Sweden. Most legislative initiatives have targeted protecting operators in key sectors to the economy, to society and to the functioning of the state – see, eg, the Swedish Protective Security Act and the NIS directives. Other initiatives have had a broader scope – see, eg, the GDPR. The question going forward is "What's next?" Early indications are that the EU will be a driving force in regulating the cybersecurity space with legislative initiatives such as the Cyber Resilience Act.

Experience has shown that there is a strong will in Sweden to comply with the applicable cybersecurity legislation. Most organisations work hard to ensure that they meet the requirements set out in the legislation and that they have a high level of cybersecurity. However, one area that has not been given as much thought is how the regulatory requirements affect contracts and which requirements must be passed on to suppliers and subcontractors. The issue of how the regulatory requirements are passed on and the allocation of risks is in many cases subject to a significant amount of negotiation.

Kontakt:
Agne Lindberg / Partner / Advokat
+46 (0) 709 25 25 25
agne.lindberg@delphi.se

Felix Makarowski / Senior Associate / Advokat
+46 (0) 709 25 25 27
felix.makarowski@delphi.se

Petri Dahlström / Associate
+46 (0) 767 72 00 35
petri.dahlstrom@delphi.se