Legal aspects of information security (2022)

1 About the seminar

Many actors are increasingly expected to have insight into how the digitalization of society is bringing with it vulnerability and security concerns to both private and governmental organizations. This seminar is a practical exercise where certain identified cybersecurity concerns are to be analyzed and responded to providing a relevant legal context and corresponding argumentation. The overall aim of the seminar is to create an understanding of the skills required in order to manage cybersecurity challenges from the legal perspective and in a digital and international environment.

At the center of this exercise is the energy company called GlobEl. GlobEl is a strongly growing international energy company. The parent company is established in Germany with wholly owned subsidiaries in the Nordics, South Africa and the USA. The business mainly consists of the sale of energy, but also of ancillary products such as heat pumps and other energy-saving products as well as associated credit solutions. The growth in the area of energy sales is mainly due to effective price competition, very good customer understanding and associated favourable and customer-adapted contractual terms. But the peripheral products also contribute to the expansion through well-targeted marketing, sales and relatively extensive financing solutions linked to these ancillary products. GlobEl publishes quarterly reports and annual reports on its website. The website also manages a large part of its customer management. In principle, all customer service issues can be handled via the website, including entering into new electricity contracts, purchasing products, support, etc.

You work in the technical department at the Swedish branch of GlobEl located in Stockholm but are expected to have some basic knowledge of the law in order effectively to address cybersecurity concerns. In relation to GlobEl's present business operations, the Group Chief Compliance Officer (CCO) has identified certain security concerns of a legal nature and directed these concerns to GlobEl's Swedish techno-legal team. The CCO has scheduled an on-site appointment in Stockholm with this team to gain some input in relation to some cybersecurity concerns. Hence, the case scenario is a face-to-face meeting where the GlobEl Swedish techno-legal team presents their opinion of the legal analysis and related responses to the CCO.

2 Seminar process

General information

Students are divided into groups of approximately 7-10 students in each group.

Each group will analyze the list of legal concerns and investigate the related cybersecurity needs. To some extent specific security demands can be found in different regulations, but more vague regulatory demands may also need to be considered. Each student is expected to be well-oriented in all relevant areas of concern and be in a position to respond to the questions from the CCO hereunder.

Commented [SG1]: Is this needed?

The CCO's questions:

1) The CCO of GlobEl is concerned about its customer service department's level of performance. a) To what extent – if at all – is GlobEl allowed to monitor employee emails for quality assurance? Would it be worthwhile to further specify the purpose of such a control measure? b) If the company decides to, for example, store the employee emails must they encrypt these emails?

2) Social media offers key business advantages to companies like GlobEl, but also has well-known security risks. Two of the greatest risks to organizations are malware and the inadvertent disclosure of sensitive information. In order to mitigate these security risks as well as enjoy the benefits of the social media, GlobEl must establish and enforce good social media usage policies. The CCO is wondering what kind of safeguards GlobEl Sweden needs to consider regarding GlobEl's social media accounts?

3) A data controller must be aware of the different users who access their systems/records and their requirements. The CCO is wondering how GlobEl manages the rights of access to the various types of data (i.e. personal data, sensitive data, general business data etc.) within the organization? Are there any legal requirements to provide customers with access to their data?

4) GlobEL's operations are complex, and collaboration is critical to innovation and service delivery. "The world has changed," says an information security service area leader at the company. "We need tools to create a secure environment, but we also need to facilitate collaboration, growth, and the appropriate relationships that drive business forward."

   Given that the transmission of personal data and other sensitive information is critical to GlobEl's business, especially the transfer of data to third countries such as the United States, the CCO wonders what strategies should be applied?

5) In general terms, cloud computing consists of a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space. How can GlobEl Sweden move to the cloud with confidence, particularly where it is clear that EU data protection law places the responsibility for data security squarely on the data controller who is accountable to the individual data subject for the safeguarding of their personal information? In other words,

how can GlobEl Sweden be satisfied that data will be secure if it is outsourced to a cloud provider? What kind of cloud-computing models should be considered?

6) The threat of insiders stealing valuable corporate data continues to escalate, particularly because it is difficult to detect and these people often have access to sensitive information. The inadvertent exposure of internal data has also become of critical concern. Such data leaks can expose enterprises of all types to serious regulatory, public-relations and financial risks. For example, Swedo Bank lost the sensitive data of 400,000 customers and, as a result, suffered devastating consequences to its reputation and received heavy fines as a penalty for this lapse in security. How can GlobEl protect itself against the risk of data loss? What kind of dataloss-preventive strategy(ies) should GlobEl utilize? Is there reason to base such a strategy on an information analysis and a data category classification? Are there any examples that could serve as an illustration?

7) While e-signing documents with smart cards and other hardware devices remain a viable option in the EU market, it does pose a number of challenges. The CCO wants GlobEl Sweden to implement electronic signatures for the purpose of contract management but she is concerned about whether there will be negative consequences for implementing them within the company. What is the current state of affairs in Sweden regarding the security levels of different electronic signatures in relation to business data? What are some of the costs/benefits of customer experience and security when deciding on which e-signature type to implement?

8) John, a GlobelEl employee brought home his company laptop. Unfortunately, his home was broken into that very same day and the laptop was stolen. This incident resulted in the loss of 26.5 million company records. These records included, among other things, information about the names, dates of birth, genders and personal numbers of employees and customers.

   What legal concerns are raised when employees use their own devices to access our company information? How could another event like this be protected against in the future?

3 Practical matters

3.1 Groups

The groups will be posted on iLearn.

3.2 Presentation

Each group will have approximately 45 minutes to present their findings in the form of a Q&A session with the CCO. At the presentation, students are permitted to bring whatever material they would like including, but not limited to, notes, relevant legislation, digital aids and/or text books. Participants must be prepared to

answer all the above questions and must be prepared to discuss the cybersecurity aspects of all the areas of concern pertaining to these questions. Follow up questions to the above-posted questions will occur so students must make sure to comprehend the assigned questions as well as surrounding legal matters. Students are expected to conduct themselves in a professional manner and with a professional demeanor. Therefore, even though outside materials are permitted into the exam, the most successful students will be those who are able to hold a confident and free-flowing and convincing conversation with the instructor while maintaining steady eye contact (just as is expected from a legal advisor in the "real world").

3.2 Reading instructions

Students are expected to have a relevant understanding of course literature, legislation, regulations and cases.

3.3 Bonus points

Students that do an exceptional job during the seminar will be awarded 3 extra points to their final exam.