SINGAPORE POLYTECHNIC

**Computer Law & Investigation**

**ST2502**

**E-Learning Week Assignment – 6 to 12 Jan 2020**

**-------------------------------------------------------------------------------------------------------------------------------**

The Cybersecurity Act (Act 9 of 2018) (the “Act”) came into force in Singapore on 31 August 2018. The Act was passed to take measures to prevent, manage and respond to cybersecurity threats and incidents, to regulate owners of Critical Information Infrastructure (“CII”) and cybersecurity service providers.

Elly, the CEO of Elly Electric Co Pte Ltd (“EECPL”) which generates, transmits and distributes electricity, is trying to figure out whether her company has obligations/duties under the Act and if so, what these obligations/duties are.

Vicky runs a business which provides penetration testing and managed security operations centre monitoring services. She has questions about the new licensing framework in the Act which she understands would apply to her business.

Greg is starting a new job at the Cyber Security Agency of Singapore (“CSA”) where he will be part of the team responding to cybersecurity threats and incidents. Hence, he is trying to understand the CSA's powers under the Act.

Please assist Elly, Vicky and Greg with their following queries. *(Hint: you may wish to check the CSA website (Explanatory Statement & FAQs on the Act) to find the answers.)*

1. Is Elly’s company within one of the critical sectors listed in the Act; and if so, which sector? Elly would also like to know what are the other critical sectors covered in the Act.

The Cyber Security Agency of Singapore (CSA) has worked closely with Sector Leads to identify the Critical Information Infrastructure (CII) supporting the provision of essential services across 11 critical sectors.  
  
The critical sectors are Energy, Water, Banking & Finance, Healthcare, Transport (which includes Land, Maritime, and Aviation), Government, Infocomm, Media, and Security & Emergency Services. The list of essential services in these sectors are published in the First Schedule of the Act. Elly’s company deals with electricity which is part of the energy sector, a critical sector listed within the act.

1. What is the criteria for a computer system to be designated as a CII? In other words, when would EECPL’s computer system be designated as a CII?

n arriving at the list of essential services in the Cybersecurity Act, the Cyber Security Agency of Singapore (CSA) took reference from the list of critical sectors in the Computer Misuse and Cybersecurity Act (CMCA). CSA also surveyed the definition of "essential services" in other jurisdictions.  
  
CSA then identified a total of 11 sectors with Critical Information Infrastructure. For each of these 11 sectors, CSA worked with the relevant Sector Lead to identify their essential services based on criteria such as impact to Singapore's economy.

1. If EECPL’s computer system is designated as a CII, what are EECPL’s duties under the Act?
2. Vicky would like to know why did the CSA decide to license providers of penetration testing and managed security operations centre services? And what would happen if she does not obtain a licence for her business to provide the said services?
3. What are the licensing conditions that Vicky’s business would have to comply with?
4. Greg wants to know what are the powers of CSA which can be exercised against persons affected by cybersecurity threats or incidents?
5. Does CSA have the power to investigate and prosecute foreign hackers /organized groups attacking Singapore from overseas?