Section 1:

Fictional Texas Electrical Company (FTEC) is a company founded in 1995 with the passing of State Bill 373, which allowed unregulated energy companies to operate in the state of Texas. Essentially, this allowed texas companies to charge market rates instead of flat rates for their electricity. FTEC provides power to several major data centers that operate in the area due to the relatively temperate weather of North Texas. The company takes cyber threats very seriously after hearing of the multitude of attacks in the 2010s.

Section 2:

2.1 FTEC uses natural gas to power a majority of its plants, though it also uses approximately 30 percent wind power. With 30 plants that FTEC runs, they employ hundreds of workers ranging from engineers and IT professionals to laborers. Many parts of the critical infrastructure in these plants is accessible by the internet.

2.2 FTEC operates in a region that does not have to worry about the effects of its physical environment, with the exception of heat. Despite federal regulations calling for winterization of power plants, FTEC is not required to, due to the nature of the deregulated energy sector in Texas. The recent coronavirus outbreak has affected some families of the employees that work for FTEC, causing economic hardship for many. The infrastructure for the power plants themselves rely heavily on computer programs, most of which are accessible through the internet. As the virus outbreak worsened, FTEC decided that employees may have to live at work if the outbreak demands, rather than allowing any kind of remote access. This has led to a significantly reduced morale amongst the essential workers, who look at the white collar employees of the company working from home while looking at the possibility of being stuck at work around the clock.

2.3 Currently, FTEC views attacks from nation states to be the biggest threat that it faces, taking heed of attacks that happened in Ukraine in 2017. Second, they have been forced to consider the growing possibility of an insider threat as the coronavirus not only weakens their employees financial state, but the possibility of being forced to be away from family while others stay at home has caused a significant concern for the security teams that the company employs. Concerns from the physical environment are minimal, though in 2010, the company experienced a massive outage because of its lack of winterization, something that it does not want to experience again.

2.4 To mitigate threats, FTEC has begun to monitor employees more closely, concerned about the possibility of an insider attack given deteriorating economic circumstances. They have expanded their SOC to include more personnel so that they can keep a better eye on logs and critical infrastructure. FTEC uses the principle of least privilege when giving access to individuals and keeps a very close eye on evolving positions with access being limited to any employee who may be leaving the company. The logs for critical infrastructure are monitored 24/7 using a properly configured SIEM. Despite the lack of regulation, FTEC decided it was in their best interest to winterizer their plants, given the unfortunate incident that happened to them a decade before. These courses of action, despite the inconvenience that they might cause, are vital to the organization and their reputation. Because of this, they have been deemed acceptable by the CEO, though the extra staff employed during the coronavirus might be trimmed when things return to normal and the threat resolves.

Section 3

The Intelligence preparation of the environment helps us to look at some threats holistically, instead of focusing on each threat as if it exists in a vacuum. By focusing on the environment that we are working in as a whole, we can better prepare ourselves for any threat.

As cyber security analysts, we are often focused on only cyber threats, however, there are threats in our environments that can have a potentially more harmful effect on our organization than any single threat actor alone.The recent events in Texas stood out as a particularly unfortunate effect of underestimating environmental threats. They could have the best security systems in the world to keep threats out, but by ignoring the possibility of extreme weather, they caused massive power outages across the state. Companies across the country saw data centers and online services go down for days. By ignoring the environmental risks, Texas energy companies caused extremely preventable damage to companies by essentially allowing themselves to be subject to a Denial of Service act caused not by terrorists or hackers, but by the weather.