PART 1:

Tesla data leak by a disgruntled employee (2018)-
https://www.darkreading.com/cyberattacks-data-breaches/tesla-employee-steals-sabotages-company-data

It was found that in 2018 a disgruntled employee would make use of false credentials to access sensitive data. The employee was effectively trying to sabotage Tesla by potentially giving the data to competitors. The employee acted out of frustration that they did not get a promotion that they felt they deserved. Leading to the employee attempting to sabotage the company and potentially make money by giving the information to third parties. The employee was able to effectively make changes to the manufacturing operating system which gave them access to sensitive data they would otherwise not have access to. The lack of privilege restrictions that were in place for individuals who worked at Telsa is what led to this individual being able to access the data. If better privilege restrictions were set it could have prevented the employee from being able to access the data. Limiting what the employee had access to or could change within the systems.

2022 former hospital worker-
https://www.valdostadailytimes.com/news/local_news/ex-hospital-worker-arrested-in-sgmc-data-breach/article_7ca92b22-a2e5-5541-b3b3-38472d3706b1.html

A former hospital worker at South Georgia Medical Center before quitting would download sensitive information about patients. The employee would download the information onto a USB. Upon downloading the documents the security system would detect that unauthorized downloading of documents had occurred. This would lead to an investigation being conducted to determine what had been downloaded. The USB stick would be recovered and believed that the information was not leaked or shared. It was believed that the former employee was upset with the hospital in some way and wanted to harm the organization. Thankfully the hospital had security features set that alerted IT professionals about the documents being downloaded. The issue that is present with this case is that all the employees had access to such documents. While the download of the documents is not allowed since users still have access to the documents it can easily happen without restriction. This is a good example of a time when stricter privilege controls should be set in place to restrict users from having access to information they otherwise shouldn't.

Submarine leak-
https://www.defensenews.com/naval/2016/08/26/submarine-data-leak-roils-three-governments/

A disgruntled former employee released highly sensitive documents about a classified submarine. This would be a breach into three separate governments that

were developing and assisting in the creation of said submarine. It was believed that it could have been espionage as well as someone who disliked the idea. Releasing the data about the collaboration efforts to create the submarine would potentially cause backlash or harm to those involved. Additionally, the release of the designs and sensitive information about the submarine places those who would operate the submarine at risk. Placing a hold on creation and potentially having the concept abandoned due to the risk of the leak.

PART 2:

Three major threats that come with electrical utilities are attacks on SCADA systems, ransom attacks, and insider threats. SCADA attacks are of prominent concern when it comes to electrical utilities because if attacked could cause drastic issues. SCADA or supervisory control and data acquisition machines monitor and have control over a wide range of machinery. If an attacker were to gain access to a SCADA machine then they could alter the machine leading to malfunctions or major disasters. This poses major concerns if a SCADA machine is compromised that oversees a critical infrastructure. If a critical infrastructure were to be compromised it could lead to deaths or major issues across a wide span of area. Improper security measures and permission controls could lead to users having more access than needed. Ensuring that there are proper privilege restrictions set in place could reduce the impact a threat actor has. Reducing the likelihood they could gain access by restricting the tools they have access to.

Ransom attacks are an issue when it comes to electrical utilities because if an attacker were to gain access to a company's assets. They would be able to hold the assets captive until a company pays the ransom. The company would either have to pay the ransom or try to gain control of their systems. This could cost companies money and time which could be an issue depending on the company and assets being held. Ransom attacks could be caused due to employees' failure to practice safe cyber hygiene or an attacker gaining access to a known flaw in a system. Companies have to ensure that systems are being kept up to date as well as employees understand cybersecurity topics.

Insider threats pose a great risk to electrical utilities because an insider could bring harm to the asset on purpose. An insider could also give access to third parties or threat actors if they desire to. Leading to systems being compromised or systems being damaged. If a company doesn’t set proper security controls on their systems or have physical security it could make it easy for an insider to commit such actions.

https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities

PART 3:

When companies implement electric utilities they are at risk of data leaks, safety concerns, and business disruptions. When companies implement complex electric utilities into their business they run the risk of potential threat actors targeting them. An attacker could cause harm in various ways and at times an attack can pose multiple risks for a company. One major risk can be data leaks. If an electrical utility is attacked and compromised it could lead to the attacker gaining access to sensitive data. This data could be held for ransom or leaked. This can ruin a company's reputation and cost them millions in order to solve it. Cybercrime can also lead to safety concerns. Not only could sensitive information put people's lives in danger electrical systems being compromised could put people at risk. If an attacker alters any switch that controls large electrical systems it could be life threatening. Ultimately all cyberattacks are going to cause business disruptions whether it is a ransom attack or one that targets the system physically. Having to replace parts or systems can take time and cost companies money. Having large utilities or assets down could cause a business to be inoperable if it is a critical system.

https://www.circadianrisk.com/resources/blog/10-security-risks-faced-by-the-utility-industry

Bailey, T., Maruyama, A., & Wallance, D. (2020, November 3). The energy-sector threat: How to address cybersecurity vulnerabilities. McKinsey & Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities

Jai Vijayan, C. W. (2023, December 8). Tesla Employee Steals, Sabotages Company Data. https://www.darkreading.com/cyberattacks-data-breaches/tesla-employee-steals-sabotages-company-data

Staff. (2022a, August 19). Submarine Data Leak Roils Three Governments. Defense News. https://www.defensenews.com/naval/2016/08/26/submarine-data-leak-roils-three-governments/

terry.richards@gaflnews.com, T. R. (2022, January 14). Ex-hospital worker arrested in SGMC data breach. Valdosta Daily Times. https://www.valdostadailytimes.com/news/local_news/ex-hospital-worker-arrested-in-sgmc-data-breach/article_7ca92b22-a2e5-5541-b3b3-38472d3706b1.html

Young, D. (n.d.). *10 Security Risks Faced by the Utility Industry*. Circadian Risk. https://www.circadianrisk.com/resources/blog/10-security-risks-faced-by-the-utility-industry