When it comes to the electric energy companies they fall under what would be a critical infrastructure in the United States. This places further regulations and requirements when it comes to reporting cyber incidents. Electric energy companies fall under The Cyber Incident Reporting for Critical Infrastructure Act. This ensures that energy companies follow the vast amount of regulations and disclosure agreements the government has set. This act requires energy companies to report cyber incidents to CISA “CIRCIA imposes a 72-hour deadline for covered cyber incidents and a 24-hour deadline for ransom payments.”(Skees et al.).Critical infrastructure is important because of the impact it has on the country. If any energy company becomes compromised it could be detrimental to significant parts of the nation. Additionally, a compromised critical infrastructure can pose various risks to its surrounding areas. The government also wants to be alerted to such incidents because they want to be able to assist in any way needed. If the threat is at a large enough scale they can step in to understand what happened. Since crucial infrastructure plays a vital role in how the nation operates it is understandable why CISA has to be contacted.

Old Dominion University has an Information Security Officer and an IT security team that attempts to protect the university from any threats. The ISO's role is to develop and manage ODU’s IT security program. While the IT security team attempts to respond and investigate incidents that are reported. Information must be gathered about each incident to report it accurately and to see if there is a pattern.

Information that is gathered surrounding an incident listed from the ODU website:

{ Name, affiliation, e-mail address, and phone number of people reporting the incident

Description of the suspected security incident

Information to help identify the source of the suspicious activity, like an IP address or an e-mail message with full headers

Date(s) and time(s) of the suspicious activity

Evidence of suspicious activity }

Data Compliance Owners - Compliance side and understand policies that surround incidents.

Ensure that data isn't being shared across multiple departments.

System Compliance Owners - Responsible for systems that are being used and ensuring they are being used appropriately.

Application Administrators - Primarily deal with access control elements.

Information Technology Security Program - Security controls and implementing elements to meet regulations and security expectations.

It roles & responsibilities. Old Dominion University. (n.d.).
https://ww1.odu.edu/about/policiesandprocedures/computing/standards/01/02

It security incident handling standard. Old Dominion University. (n.d.-b).
https://ww1.odu.edu/about/policiesandprocedures/computing/standards/05/01

SKEES, D. J., RAMADEVANAHALLI, A. P., & SOEHNER, C. A. (n.d.). *How new cyber incident reporting regulations impact energy companies*. – Publications. https://www.morganlewis.com/pubs/2023/12/how-new-cyber-incident-reporting-regulations-impact-energy-companies