Dj Smith

April 16, 2014

Risk Assessment and The Critical Impacts

Cybersecurity has had a great impact on technology today. Even though technology has positive impacts and implications that help us on a day-to-day basis. They're also some negative things that can impact us as well. There are political applications that Cybersecurity has brought upon us. The policy that was chosen was risk assessment. Risk assessment is a major key in cyber security because this helps prevent any breaches or attacks that are trying to affect politicians.

Risk assessment is a policy that is a popular policy that is constantly being discussed in the media, especially in politics. When testing risk assessment, this is the time when companies experiment with the negative and positive effects of technology. Ganin et al. (2017) stated that risk assessment does not necessarily eliminate biases and subjectivity necessary for selecting countermeasures but provides justifiable methods for selecting risk management actions consistent with stakeholder and decision-maker values and technical data. Politicians have their trust in cybersecurity companies to see the positive impacts they want to keep; and the hardships that need to be taken away and improved on for their technology to work. This will help everything stay on track with everything they are currently working on.

Politicians must make sure their technology is safe for them to use. meaning they must partner with security firms to make sure their campaigns go smoothly throughout the whole process. Politicians are easily at high risk for any attacks that could happen to them. Especially with campaigns which are very important in our government to self-promote what they believe they can help communities with. As known technology has taken over and with technology,

politicians can promote their campaigns and actions they want the community they are trying to reach to notice. An important action is to make sure they have everything in their circle to be complete and secure. If the self-protection of a firm is observable to an insurer so that it can design a contract that is contingent on the self-protection level, then self-protection and insurance behave as complements (Öğüt et al., 2010). Self-protection risk management helps politicians and gets them way more advanced in the situation that they have the part taken. Politicians work style is extremely confidential and everything must run smoothly, especially with technology.

Risk assessment is becoming more common in politicians' work style. This policy is important because cyber security companies can run tests to prevent attacks and breaches from happening to politicians. Is important because Social Security companies must protect political comp and make sure they are protected from any breaches or attacks. Policymakers wanted to make sure that the assessments that were taken were ready to be approved and run so that once it is public, it can run smoothly. Governments no longer simply issue instructions and monitor their implementation but seek to shape the framework conditions so that cooperation operates as smoothly as possible even without constant oversight (Cavelty & Wenger, 2019). As stated above, the government is trying to implement a smoother way to introduce technology into its policies without constantly looking over it. smoothly. This is going to help politicians with their campaign as well as their daily objectives. As stated earlier it was going to be complicated when doing these risk assessments because you must understand different ways, technology can be interrupted. Therefore, politicians use technology for their daily working activities or campaigns. There will be ways to help make their campaigns smoother than before.

References

Cavelty, M. D., & Wenger, A. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2017). Multicriteria Decision Framework for Cybersecurity risk assessment and management. *Risk Analysis*, *40*(1), 183–199. https://doi.org/10.1111/risa.12891

Öğüt, H., Raghunathan, S., & Menon, N. M. (2010). Cyber Security risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of Self‐Protection. *Risk Analysis*, *31*(3), 497–512. https://doi.org/10.1111/j.1539-6924.2010.01478.x