Project 6

Josephus West

School or Institution Name (University at Place or Town, State)

**Introduction:**

Information technology plays the role of utility not only in the business but in all of the state departments. As all of the state departments have to deal with critical information, protection of such information from cyber-attacks is inevitable. Cybersecurity and threats landscape never remains the same, so it is not possible for any single entity to ensure the protection of critical infrastructure vital to the operations of the federal and state government. Significant developments in the field of information security are made by private sector security firms. To protect national critical infrastructure public-private partnerships are required. A public-private partnership is the cooperation of two entities for co-existence (Carr, 2016). In public-private partnerships, a long-term contract or agreement is established between a government entity and private party to provide services to the public in which the private party shares a significant portion of the risk. A growing number of countries including the United States of America are developing enhanced public-private partnerships to protect the critical infrastructure of the nation against cyber-attacks.

**Public-Private Partnerships for Cybersecurity:**

Integration of information technology into governmental organizations for management and related policy enforcement purposes has made them a potential target for cyber-criminals. Most of the time criminals can be backed by rival states as well to sabotage the infrastructure of the opponents. Threat landscape for critical information technology infrastructure is always changing. Malicious actors are continuously developing sophisticated attacks to bypass the security infrastructure of large-scale organizations including the public infrastructure of facilities as well. In the dynamic world of protecting critical infrastructure intelligence sharing between public entities and related private parties is inevitable. Cyber-attacks cannot be geo-restricted or confined to a particular area.

Cyber-attacks backed by governments can destroy the critical infrastructure of the organizations at a massive scale as it is evident by the ransomware attacks during the last decade. It is an established fact that government and private sector experts need to collaborate to protect nation's security against cyber-attacks, but there are some concerns that need to be resolved regarding the policies (Givens & Busch, 2013). National Institute of Standards and Technology provides a framework that is applicable to most of the organizations for their cybersecurity needs. Legal and strategic implications often serve as obstacles to the increase in public-private intelligence sharing regarding cybersecurity due to cross-border issues such as inconsistent laws of cybersecurity.

**Effects of Public-Private Partnerships for Cybersecurity:**

Most of the time private firms have more resources to hire and utilize best talent in the field of cybersecurity to protect crucial information technology infrastructure as compared to the government. Therefore, increased and extended partnerships between public institutes and private organization have numerous benefits for both the parties in agreement. Intelligence shared by the private firms will help government institutions to formulate policies accordingly. A similar example is on the cybersecurity framework for organizations prepared by the national institute of standards and technology with the help of private sector organizations (Cherdantseva & Hilton, 2013). Private organizations such as Symantec and McAfee employ top talent in the cybersecurity to protect commercial markets from cyber-attacks. Cybersecurity market intelligence sharing is not only occupied by public-private partnerships; there are partnerships between private companies as well. A small to the medium-sized organization may have different cybersecurity requirements as compared to the state-owned enterprise business. However, there are trust issues in such partnerships because a supply chain can also be compromised by criminals such as intelligence sharing networks of such partnerships.

**Best Practices for Companies:**

Partnerships between cybersecurity entities whether private or public are inevitable to build a strong defense against malicious actors targeting critical infrastructure of the nation. However, in a public-private partnership, a private firm may have concerns regarding data exposure to the federal government. Private entities may not agree to expose their internal infrastructures to the governmental agencies as they may be protected by the data protection regulations. Personally identifiable information of their clients may be exposed to the federal or state governments that may result in violation claims for privacy issues. Therefore, organizations must comply with the frameworks and policies made by the collaboration of the security firms such as the cybersecurity framework approved by the NIST (Busch & Givens, 2012). Companies can deploy honey pot networks to detect and halt unauthorized access requests to the system and share intelligence gathered by neutralization of the attack. Effective sharing of knowledge and technical expertise will help the government to make information technology ecosystem secure. Extended partnerships also avoid the building of monopolies in particular area of cybersecurity practice such as in the field of intrusion detection systems.

**Conclusion:**

Building an effective public-private partnership to protect the critical infrastructure of the nation is inevitable. Major potential benefits of intelligence sharing and technical expertise development are prosecution framework of domestic and international cyber-criminals. It will be effective in preventing future attacks on critical infrastructure including state-sponsored targeted attacks. If the goal is not only to detect attacks as quickly as possible but to share the gathered evidence for the successful prosecution of the criminal, public-private partnerships will be very useful and cost-effective. Partnerships in either way are helpful in protecting Nation's infrastructure but to address privacy-related issues of private partners extended negotiations are required to be held on a regular basis. It will help the public as well as private sector to improve the cyber defense.

References

Busch, N. E., & Givens, A. D. (2012). Public-private partnerships in homeland security: Opportunities and challenges.

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43–62.

Cherdantseva, Y., & Hilton, J. (2013). A reference model of information assurance & security. In *2013 International Conference on Availability, Reliability, and Security* (pp. 546–555). IEEE.

Givens, A. D., & Busch, N. E. (2013). Realizing the promise of public-private partnerships in US critical infrastructure protection. *International Journal of Critical Infrastructure Protection*, *6*(1), 39–50.