Security policy analysis

Technology, Information Technology

Security Policy Analysis al Affiliation) The proposed Cybersecurity Legislation of s and describes responsibility, authority and accountability of various parties. In terms of authority and responsibilities, the Secretary of Homeland Security, the Partnership Advisory Council for critical infrastructure, the private sector and other federal agencies, are empowered to conduct high level cyber security risk assessment on a sector by sector sequence, develop procedures for certain critical infrastructure, identify performance issues and implement plans for restoration. The authority conferred on these institutions is for defending and monitoring cyber security, while also allowing transparency and accountability. Greater emphasis is also placed on personal accountability and responsibility of cyber security.

Section 111(a) stipulates the supremacy of the Act in accordance with other laws relating to cyber security. According to my personal view, this section mimics the supremacy of the Constitution. It distinctly states how the Act, shall supersede very provision, statute, regulation, state rule, that expressly commands comparable cybersecurity practices developed for the purpose of protecting critical infrastructure.

The policy is important in dealing with information security program management. It stipulates the structure for various agencies on now to prevent, assess and even manage cyber security risks. Additionally, it provides a network for federal agencies and other stakeholders to communicate and discuss new developments in cyber terrorism.

According to Borene, every federal agency has a distinct role in policy enforcement. On a general basis, each party is tasked with being at the forefront of responsible global cyber engagement, enhancing information

sharing and facilitating efforts to increase awareness, training and education to the general population (Borene, 2011).

The lack of clear policy enforcements leads to cyber terrorist attacks on government agencies, loss of information and privacy and loss of billions of dollars on an annual basis. One such incident is the cyber-attack on Blue Shield and Anthem Blue Cross in February 2015. Even though no medical information was compromised, the incident breached notification laws at the state level.

When technology moves faster than policy, there are many cases of financial loss and exploitation, such as the period before the establishment of the open data policy, an open source project by the U. S government.

Reference List

Borene, A. (2011). The U. S. intelligence community law sourcebook: A compendium of national security related laws and policy documents (2011 ed.). Chicago: American Bar Association.