Catastrophic cyberattack

Catastrophic Cyber Attack The essay aims to address a two-fold objective, to wit to identify and describe cyber attacks in a water supply system, and (2) to briefly describe the implications of a cyber attack in a water supply system. Catastrophic Cyber Attack Introduction Water supply systems are prone to various levels of risks due to major disasters, accidents, and acts of terrorism. Among these causes, the acts of terrorism such as the cyber attack on the infrastructure of the water supply system seriously affects the society and need to be addressed promptly. A cyber attack has been defined as a computer-to-computer attack that undermines the confidentiality, integrity, or availability of a computer or information resident in it (O'Shea, 2003). Cyber attacks involve virus and worm attacks delivered through vulnerable exploit engines, denial-of-service attacks (DoS), web defacements of informational sites, and unauthorized intrusions into systems (Colarik, 2006, p. 84). According to the CSI/FBI 2005 Computer Crime and Security Survey, rate of losses from attacks are: viruses (33%), unauthorized access (24%), theft of proprietary information (24%), DoS (6%), net abuse (5%), laptop theft (3%), and financial fraud (2%) (Colarik, 2006, p. 83). But for a cyber attack to be successful, phases of attack must also be successful. The five phases of cyber attacks are reconnaissance, penetration, identifying and expanding internal capabilities, intruder damages the system, and removal of evidence of penetration or theft (Colarik, 2006, p. 83). Cyber attack penetrates the Supervisory Control and Data Acquisition (SCADA) system of a water supply system and poses detrimental effect over the system. Cyber Attack on a Water Supply System During the late 1990s, medium to large water utilities integrated IT and SCADA system. Among of those utilities was the Water Corporation of Western Australia (WCWA), one of the largest utilities in the world (Mays, 2004, p. 5. 1). A cyber attack could cause data alteration and destruction, blocked or rerouted communication, financial damage, disruption of the water utility’s internal operation, and failure of the equipments to operate when needed. However, cyber attacks will not cause immediate water supply disruptions provided that the duration of attacks were not prolonged. In order to understand the impact of cyber attacks to the water supply system, it is important to fully understand the elements of the SCADA system. The term SCADA refers to plant-computer-based process control systems and computer-based systems. These systems monitor and control remote raw water production and treated water distribution facilities (Mays, 2004, 5. 2). Unprotected SCADA network access may lead to cyber attacks; the reason why water utilities should be periodically reviewed and vulnerabilities must be addressed. A detailed vulnerability assessment approach and planning tools were devised to address cyber attacks in the water utilities. Conclusion Cyber attacks pose the highest risk for water system disruption as it involves unauthorized computer-to-computer connection. In a cyber attack, the use of viruses account for the highest rate of losses. A successful cyber attack involves the completion of reconnaissance up to the removal of penetration evidence. Water supply systems utilize the SCADA system. A break in the security system during cyber attacks could cause detrimental effects on the water supply’s production, treatment, or distribution in the community. Periodic monitoring and review of assessment and planning tools are necessary to secure the water supply system. References Colarik, A. M. (2006). Current Cyber Attack Methods. Cyber Terrorism: Political and Economic Implications (p. 82-110) Philadelphia: Ideal Group Inc. Mays, L. W. (2004). Cyber Threats and

IT/SCADA System Vulnerability. Water Supply Systems Security (p. 5. 1-5. 10) New York: The McGraw-Hills Company, Inc. O’Shea, K. (2003). Cyber Attack Investigative Tools and Technologies. Institute for Security Technology Studies at Dartmouth College. Retrieved on June 8, 2011 from http://htcia_siliconvly. org/contacts. htm