Cyber attacks: a new paradigm in warfare essay examples

Law, Security

Cyber attacks: Costs and impacts

On the 11th of September, 2001, the canons of airport security was forever changed when a number of airplanes with innocent passengers were commandeered by extremists. Armed with nothing more than box cutters, these killers went on to redirect the planes from their original flight plans and careened them into some of the most iconic structures in the United States. As a result, airport and border security authorities stepped up airport and border security to meet the new threat.

However, though the physical aspects in airports have improved, a new menace has arisen with the advances of technology-cyber attacks. Due to the diverse number and assortment of business concerns parallel to their maintenance policies and data stores, information systems in airports form a great web of information that must be secured. With the rise of cyber attacks, the challenge is how to safeguard the various information technologies systems and infrastructures in an airport (Researched Solution, n. d., par. 1, 3).

There must be first a definition on what actually constitutes a cyber attack on the IT infrastructure of a facility or company. A “ computer network attack,” or a cyber attack, interrupts the “ integrity or authenticity” of information via the use of a virulent code that changes the “ program logic” responsible for controlling the data, resulting in flaws in the output. “ Hackers” scan the Internet for opportunities for computer infrastructures that are configured incorrectly or do not have the necessary security software installed. By uploading the virulent code into the targeted systems, the hacker can then remotely control the system and use the system as a

launch pad to attack other computers or illegally monitor the contents of the target computer (Navy Department Library, 2005, p. 5).

The costs of a cyber attack on an airport can be quite significant. Only recently, the Ataturk International Airport in Istanbul was hit with a cyber attack. The cause of the breakdown was attributed to an assault on the Polnet data system. As a result, the airport went into complete chaos-plane departures were delayed, passengers had to wait for inordinately long periods, passport control systems closed down (Paganini, 2014, p. 1). Considering the complex operating systems in these facilities as a sole contributing factor to exposure to cyber attacks, airports are extremely vulnerable to external attacks. However, the threat is not only against the external, physical components of the facility, but more against the internal units of the airport. For example, Heathrow’s Terminal 5 supports a diverse and complex security system anchored on an amalgam of analog, digital and Internet Protocol telephoning that is all defenseless against cyber attack risks. These threats can be uploaded into the airport systems via a number of seemingly harmless means. These include the use of USB drivers, laptops and similar gadgets, CD’s and DVD’s, social networks, and “ denial of service” attacks, among others (Gopalakrishnan, Govindarasu, Jacobson, Phares, 2013, p. 370).

The growing trend of interconnectivity does have a number of benefits; nevertheless, with these benefits comes a great potential for security attacks. With this in mind, there must be a recognition that one, there is indeed a threat with regards to the threat of cyber attacks on airport facilities, and two, there must be steps taken in order to ensure that the

threat is minimized or even eliminated. In the report of the Center for the Protection of National Infrastructure of the UK entitled “ Cyber Security in Civil Aviation,” the group noted that cyber security concerns should be included in all aspects of civil aviation. The group, noting the concern of a growing cyber security threat, mentions, among other goals, that there must be a thorough road map in strengthening cyber security measures to protect airport systems from cyber attack. Among the recommendations include standardizing aviation systems with regards to IT infrastructures, defining and developing a culture dedicated to the protection and defense of cyber structures in the facility, and increasing the levels of coordination of civil and public sectors in the area (American Association of Independent Advisors, 2013, pp. 9-10).

The recovery procedures mandates that critical personnel from all facility and operations units be designated as members of the planning group and will be involved in all stages of the disaster recovery initiative. The members of the group must be thoroughly knowledgeable with the various business processes, technologies, structures and mechanisms in the facility in order to craft an effective DRP. The objective here is to develop cost effective and viable system recovery and restoration on all IT domains, particularly the operations of “ mission critical” and crucial business operations.

It must be noted that system recovery time, and the status of the data impacted, are critical features of the level of service that a business can perform in cases of attacks. However, businesses and the IT operating units seldom see the issue in the same way; as businesses increase their levels of interconnectedness, the leeway for system down time and information loss is

growing smaller. However, if the BCP and the DRP is implemented extensively with adequately trained personnel, losses due to cyber attacks will be minimal and businesses will be able to continue with their operations (Bahan, 2003, p. 12).

References

American Association of Independent Advisors (2013). “ The connectivity challenge: protecting critical assets in a networked world.” Retrieved 2 July 2014 from < https://www. aiaa. org/uploadedFiles/Issues_and_Advocacy/AIAA-Cyber-Framework-Final. pdf>

Bahan, C. (2003). “ The disaster recovery plan.” Retrieved 2 July 2014 from

Gopalakrishnan, K., Govindarasu, M., Jacobson, D. W., Phares, B. M. (2013). “ Cyber security for airports.” International Journal for Traffic and Transport Engineering Volume 3 number 4 pp. 365-376

Navy Department Library.(2005). “ Computer attacks and cyber terrorism: vulnerabilities and policy issues for Congress.” Retrieved 2 July 2014 from

Paganini, P. (2014). “ Istanbul Ataturk International Airport targeted by a cyber attack.” Retrieved July 2, 2014 from

Researched Solution (n. d). “ Protecting airport information systems against cyber attacks.” Retrieved 2 July 2014 from