Good securing america's railroads and passengers essay example

Business, Industries

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

Introduction

The railroad system is an important contributor to the US economy. A disturbance in the system could have serious consequences to the transportation network and the economy at large. A high number of counter measures have been instituted to prevent attacks that would cause disturbance. However, the existing defensive measures entrenched in the railroad system may not be sufficient to guarantee safety against all attacks that may be made against it. If enemies or rivals spot points of weakness, they may initiate attacks to disrupt service or harm human lives. Information is critical for any successful attack to occur. If information security is treated as the first line of defence in mitigating attacks, efforts to improve the security of this information will produce cutting edge solutions.

A holistic view of the industry reveals that the railroad system faces threats of attack both from insiders working in the railroads and outside attackers.

Industry level strategy should consider the issue in terms of protecting an information based industry as a whole where insiders can equally be as dangerous. This will in turn protect the railroad transportation system. The implementation of such approach will require intelligence agencies to adopt a proactive cyber security initiative focused on protecting against infections and not merely reacting to the aftermath they leave behind in their wake.

The operators of the American Railroad infrastructure have the primary duty to protect their assets and the passengers they serve. Securing critical assets against attacks has ramifications for national security and requires a partnership of all stakeholders.

Employee screening

The most immediate threat to railroad system security happens to be the people employed to work in them. Calls to screen railroad employees who coordinate the railroad system have been taken seriously. The screening of employees is a standard procedure in the railroad industry. Proper screening will prevent railroad employees from bringing potentially dangerous materials into the railroads or sharing critical information that could be used to sabotage the system.

There are many ways to screen employees. Best practice dictates that the process begins in the recruitment phase of employment. It is important to ensure that railroad employees who require access to secure locations within the railroad network pass a background investigation to receive an access badge to these critical areas. The combination of the information gathered from such a screen and the day to day interaction with the employee make it

possible for supervisors and other colleagues to know one of them is acting suspiciously (Peterman & Randall, 2008).

Employees should be screened each time they go into a secure area of the railroad. If someone is suspected to be a threat he/ she can easily be pulled off. Mechanisms that allow officers to be deployed to any locations in the railroad community at any time to inspect workers, their property and vehicles, should be put in place. These practices would ensure that workers adhere to proper access procedures when working in secure locations, have the required credentials and do not have in their possession, items that are not related to the task they are handling and may pose a security threat.

Employers in the railroad industry sometimes fail to identify risks or train their managers on how to defuse the tensions that can lead an employee into willingly participating in an attack. They often fail to react despite ample warning signs. They also fail to take extra precautionary measure such as to ramp up security, even after sacking or disciplinary action that is likely to trigger an attack. Regular training sessions should be conducted to educate employees on how to read and interpret warning signals. This should be on a continuing basis.

Intelligence Awareness and communication

U. S. intelligence agencies such as the Department of Homeland Security and TSA should adopt a model of consulting with other transit operators as it happens in Japan to see if new regulations and policies are practical (Tabuchi, 2010).

In order to increase intelligence awareness, efforts to establish a front line of

defence against modern day threats by fostering or enhancing shared situational awareness of network threats, network vulnerabilities, and events within the railroad industry and eventually with state, local, and tribal governments and private sector partners. The intelligence agencies need to develop more capacity to act quickly to cut down on the current soft points and prevent attacks.

The railroad industry needs to enhance counterintelligence capacities in order to defend against all types of threats. It is critical to enhance the security of the supply channel for critical information technologies (Japan Association of Rolling Stock Industries, 2010).

Most essential is the strengthening of the future security environment by expanding education programs, coordinating and redirecting research and development efforts across the railroad industry, and working to invent and develop strategies to discourage hostile or malicious events in the transportation systems.

Emphasize public awareness campaigns. U. S. railroad operators should put more emphasis on public awareness campaigns like the ones conducted in Tokyo and London. It is reported that the London railroad system is called to respond to over 10, 000 cases of unattended bags monthly. While most of those cases turn out to be anything, but a threat to public safety, the active participation by the public suggests an alert and proactive leadership. The awareness in these cases boosts security for the overall rail system (Peterman & Randall, 2008).

Cyber Security

Supervisory control and data acquisition (SCADA) networks cover computers and applications, which present important functions in delivering essential amenities and commodities to all Americans. SCADA is part of nation important infrastructure and needs to be protected from various dangers that exist in cyber space in present days. SCADA networks are effective and are widely used in study and collection of data Nevertheless; they also pose a security threat. SCADA networks were created to capitalize on the functionality, with slight attention given to security.

As a result, dependability, flexibility and safety allocated to control SCADA system are strong, while the securities of those systems are always weak. As a result, SCADA system is rendered vulnerable to manipulation of data, disruption of services, public service control and disruptions of important infrastructures. Major actions are needed to secure SCADA networks as an effort to protect states necessary infrastructures.

Monitor and strengthen the security of any remaining connections to the SCADA system is important to carry out a vulnerability analysis associated with SCADA networks. In so doing, one evaluates security postures associated with this pathway (U. S Department of Homeland Security, 2009). It is important to use this statistics in combination with risk management procedures to create a robust security strategy for any pathways to the SCADA system. SCADA network is only as safe as its faintest connecting point, it is important to execute firewalls, intrusion detection systems (IDSs), and other suitable security amounts at all points of entry.

Arrange firewall rules to forbid access from and to the SCADA network, and

be as detailed as possible when approving connections. For instance, the Independent System Operator (ISO) ought not to be given network access because there is a demand for connection to particular components of the SCADA system. It is important to strategically place the IDS at all entry points to warn security personnel of possible violations of network security. It is the duty of Organization management to comprehend and accept responsibility for any risks connected to the SCADA network (U. S Department of Homeland Security, 2009).

Most SCADA systems in use do not have security features at all. The owners of SCADA system need to ensure that vendor put security feature in the form of product patches and that upgraded different SCADA devices are sent with necessary security features, nonetheless these are usually disabled to safeguard it ease of installation. It is important to analyse all SCADA devices to verify whether security features are available. Moreover, factory evades security settings for instance, computer network firewalls are often set to provide full usability, but with minimal security. It is crucial to set all security features to deliver the maximum security level. (Baker, 2008)

Railway Oversight

The government needs to engage with all the stakeholders in the industry to map out how to proceed in the matter to avoid delays due funding problems. (Frankel & Sheila, 2005)

Railroad projects are huge and require a lot of funds to undertake. Securing these projects is an even more important task. Using funds from the government and other stakeholders, employees can be taken through

training programs. Such training programs should aim at equipping the railroad employees with the requisite skills to deal with emergencies that may arise following an attack. The railroad system does not receive the funding that is commensurate with its share of risk in comparison to the national risk from attacks. Lack of funds has hampered the training of workers in the railway system. Training is essential as it broadens the effectiveness of the officers deployed to secure against threats. The U. S Congress needs should do more to increase the allocation given for rail security from the government and formulate policies that prioritize the key elements.

Attacks to key railroad infrastructures have indicated that security systems need to be integrated into a bigger network of screening centres that comprise of the transportation system, the passengers who use the network and access to other important facilities.

Conclusion

Good mitigation of the risk against attack involves keeping people from compromising railroad system. The system should have mechanisms that are able to detect abnormal and unauthorized actions in case they arise. The mechanisms should ensure that the relevant personnel are informed of the abnormal or unauthorized activity and even recommend the necessary action to take.

References

American Public Transportation Association (2010) Recommended Practice: Securing Control and Communications Systems in Transit Environments--Part

1: Elements, Organization and Risk Assessment/Management

Baker, Al. (2008) “ New Operation to Put Heavily Armed Officers in Subways.” New York Times, http://www. nytimes. com/2008/02/02/nyregion/02machinegun. html? emc= eta1

Baker, Elaine, et al., (2006) NIST SP 800-57, Recommendation for Key Management, Part 1, and General: http://csrc. nist. gov/publications/PubsSPs. html, Part 2, Best Practices: http://csrc. nist. gov/publications/PubsSPs. html.

Bier, V. M (2005) Choosing What to Protect.” Los Angeles, CA: CREATE Homeland Security Centre, University of Southern California.

Frankel, Sheila, et al. (2005) NIST SP 800-77, Guide to IPSec VPNs, http://csrc. nist. gov/publications/PubsSPs. htm

Hiroko Tabuchi, (2010) Japan n Starts to Shop Its Bullet Train Technology,” New York Times

Japan Association of Rolling Stock Industries 2010 “ Current Status of Production,” www. tetsushako. or. jp/. englishoutlook. html

Peterman, & David, Randall. (2008). “ Passenger Rail Security: Issues and Legislation in the 110th Congress.” CRS Report for Congress, RL32625.

U. S. Department of Homeland Security.(2009) Recommended Practice: Improving Industrial Control Systems Cyber security with Defence-In-Depth Strategies.