Stručni rad *UDC 004.6:35*

CYBER SECURITY IN PRIVATE INDUSTRY CRITICAL INFRASTRUCTURE

Edita Bajramovic
American University in Bosnia & Herzegovina, e-mail: edita.bajramovic@gmail.com

Summary: *Cyber attacks are threatening not only military targets but also United States critical infrastructure. Stopping such threats has become a top priority and main concern for the United States government. Interruptions caused by cyber attacks can bring tragic results. Increasingly sophisticated technologies make it more difficult to detect, track, and destroy malicious programs. After the terrorist attacks on September 11, 2001, government is more and more adopting preventive actions on improving cyber security especially, on critical infrastructure [1]. In order to satisfy users and government requirements in security systems, private industry must develop adequate technology and incorporate best security practices. Government's task in cyber security is to work with private industry to improve and protect critical infrastructure.*

Keywords: *cyber security, laws and regulations, government, private industry, critical infrastructure.*

1. INTRODUCTION

Breaching security in cyberspace is continuously growing. Cyber attacks are threatening not only military targets but also United States critical infrastructure. Stopping such threats has become a top priority and main concern for the United States government. Public and private industry could at any moment experience a deep and destructive cyber attack. For national security—particularly critical infrastructure such as telecommunications, energy pipeline, refineries, financial networks, health systems, and other essential services—cyber attacks pose a significant problem [1]. Private industry is in possession of 85% of critical infrastructure [2]. Interruptions caused by cyber attacks can bring tragic results. In recent years, the risk of cyber attacks on the United States' critical infrastructure has increased. Users in companies rely on all kinds of portable media devices. A USB stick with a malicious computer code can easily be connected to a computer. Malicious programs penetrate inside the computer network and collect secret and public information and instantly send it to hackers. Cyber attacks have become a reality and a source of national fear: dangerous programs can secretly be executed on computer systems and send out confidential data straight to the terrorists. As computer viruses and worms become "smarter" and better every day, cyber attacks on government and private industry pose an increasing threat to national security. Increasingly sophisticated technologies make it more difficult to detect, track, and destroy malicious programs. After the terrorist attacks on September 11, 2001, government is more and more adopting preventive actions on improving cyber security especially, on critical infrastructure [1].

2. REASONS FOR AND METHODS FOR GOVERNMENT INTERVENTION

Government's task in cyber security is to work with private industry to improve and protect critical infrastructure. Homeland Security Presidential Directive (HSPD) 7 is the policy made to promote effective cyber security in protecting critical infrastructure. Any breach and attack on critical infrastructure could interrupt services and cause mass casualty [3]. Department of Homeland Security (DHS) is the United States government's main defense against cyber attacks targeting non-military government agencies, private industry, corporations, and academic and financial institutions. HSPD 7 allows DHS to coordinate cyber defense [4]. Security can be compromised in either public or private industry so government and private industry must work together to improve cyber security. Cyber attacks on critical infrastructure are as dangerous to national security as an armed attack. HSPD 7 focuses on protection of critical infrastructure from cyber attacks that might cause mass casualties, harm government and its departments, damage the private industry and stop delivery of vital services, and have a negative impact on the nation's economy [3]. Government must recognize and protect critical infrastructure and work closely with private industry on cyber security improvements and enforce security laws and regulations.

3. GOOGLE AND GOVERNMENT INTERVENTION

In the case of government intervention, according to HSPD 7, DHS and private industry must discuss suggested recommendations and analyses before intervention [5]. First, government must set up a partnership with private industry. Google is a perfect example of such a partnership. The cyber attack Operation Aurora was an intellectual property theft attack. Hackers broke into large organizations, including Google and Adobe, looking for source code [6]. Exploit.JS.Aurora.a is the program created to take advantage of vulnerabilities and weaknesses in different software products. In this case, the vulnerable software was Internet Explorer [6]. Aurora was designed to steal personal information and corporate intellectual property, such as the project source code [6]. The attack was performed using e-mails that consisted of links, directing users to malicious sites. Such websites contained exploits that resulted in downloading the main executable file on the target computer [6]. In Operation Aurora, attackers gained access to security servers that Google employees actually use to generate reports on the use of Gmail when they get a court order. Gmail hides the IP addresses in the header so users cannot figure out who sent the mail, but using this system, all such data becomes available. After the attack occurred, Google asked National Security Agency (NSA) for help mitigating risk and system vulnerability evaluation [5]. Google entered into a partnership agreement with NSA. Usually, private industry does not want to seek assistance from government. However, Google's case showed that government intervention can be the best choice. Therefore, government must make sure that private industry improves cyber security and evaluates software products for vulnerabilities [5]. Frequently, government and the private sector do not practice very good cooperation. Private industry is often opposed to government cyber security integrations. Second, government must confirm what the outcomes are before particular actions are taken during intervention. Also, government must make sure during intervention that local, state, or federal laws are not in conflict with each other

[5]. For example, in the case of a cyber attack on a power grid, DHS can require cyber attack discussions only in front of government agencies or personnel. However, in the same case, local authorities could require public discussion regarding power grid cyber attacks. Another important fact is that government must assess all existing and new regulations using security filters. For example, for safety reasons, a power grid can reserve a certain amount of fuel in the generator to use in emergencies. If the power outage is for long time, the power grid will not have enough fuel [5]. Loss of power will occur, and government and private industry will not be able to restore their services. During intervention, government should incorporate flexibility and also provide funding for implementing better security policies and regulations. Finally, government should enforce gradual incorporation of new rules and regulations [5]. It would be chaotic if all rules and regulations must be enforced at once.

4. LAWS AND REGULATIONS IN CYBER SECURITY

Numerous laws, proposals, and regulations are published in order to enhance cyber security in government and private industry. While some businesses never discover that they had a security breach and valuable information had been stolen, other companies are seriously damaged by a cyber attack. Businesses are mainly concerned with negative publicity — the main reason for not reporting intrusions and cyber crime to law enforcement. They fear that negative publicity will cause loss of reputation and business. Instead of reporting a cyber attack, most companies try to improve the security of their information systems to prevent further intrusions. On the other hand, if a cyber crime occurred but was not reported to law enforcement, the business could be taken to court for not reporting loss of valuable information. If cyber crime is not reported, cyber attackers become emboldened and continue with attacks, so internet security issues will grow. To enforce breach reporting, the Obama administration proposed a Data Breach Notification law stating that businesses must report security breaches and inform consumers and government [7]. In addition, the Security breach notification (SBN) law supports the security of personal information. Additionally, the Cyber Security Act of 2012 focuses on improving cyber security of critical infrastructure. The Act suggests that private industry critical infrastructure accept new voluntary standards [8]. However, private industry should not have voluntary standards for critical infrastructure. Furthermore, critical infrastructure should be protected in the best way possible. All standards must be mandatory and government should enforce standards to avoid further cyber attacks [8]. Authorities should work on increasing cyber security knowledge in private industry, creating partnerships with government and private industries to create cost-effective cyber security [8]. Also, they should work on improving internal security practices. Cyber attacks on national critical infrastructure such as energy grids can cause large problems. Several companies that provide electricity reported an incident in their networks caused by a computer worm, Stuxnet [9]. Like the most malicious malware, Stuxnet is taken seriously as a threat to the critical infrastructure and industrial processes. The Stuxnet worm can sneak into and hide in cyberspace for a long period. The worm may wait almost everywhere within the network and be prepared to do damage by a keystroke or mouse click. Cyber security and Information Sharing Effectiveness Act of 2011 helps protect information sharing as well as cooperation between government and private industry [10]. In addition, Chairman Genachowski recognizes

potential areas where commercial communication network needs to be protected. His suggestion is that Domain Name System (DNS) must be protected to avoid spoofing; protection should be increased on Border Gateway Protocols to avoid Internet route capture [11]. Also, lawmakers must identify themselves with techniques that allow threats to execute. They must create efficient procedures to alleviate risks. According to the Commerce Department, the yearly cost of intellectual property stolen through the Internet is $250 billion. Furthermore, due to cost of stolen information, around 750,000 U.S. jobs are cut annually. Secretary Janet Napolitano said that during fiscal year 2011, the United States Computer Emergency Readiness Team (US-CERT) reacted to more than 100,000 incidents [9]. One of them included a spear-phishing operation against owners in the Nuclear and Energy Sectors. US-CERT worked with those companies to assist them in removing threats from their networks [9]. Also, numbers of incidents in critical industry increased from 41 in 2009 to 198 in 2011 [9].

Even when DHS is not allowed directly to control the cyber security requirements of some industries, it does not mean that the private industry is not covered by regulations and law. For example, the electric power industry maintains required cyber security standards and policies. Sarbanes Oxley Act makes sure that organizations and industries, through certification bodies, confirm that they have appropriate internal security controls in place on their financial accounting systems [4]. In addition to protecting unclassified networks, National Protection and Programs Directorate (NPPD) provides technical knowledge to the private industry critical infrastructure by supporting risk evaluations and incident response. One of DHS's goals is to increase security awareness in private industry [4]. National Cyber security and Communications Integration Center (NCCIC) is managing incident response for cyber incidents in public and private industry. On the other hand, the National Cyber Security Division (NCSD) works closely with private industry to try to alleviate risks in private industry critical infrastructure IT. Besides mitigating risks, NCSD performs evaluations of system weaknesses as well as incident response support [4].

5. EFFECTS ON NATIONAL SECURITY WITH DIFFERENT LEVELS OF SECURITY REQUIREMENTS

In order to satisfy users and government requirements in security systems, private industry must develop adequate technology and incorporate best security practices. To prevent security breaches and increase security in private industry, government set up standards that have to be followed. Currently, government and their contractors follow National Institute of Standards and Technology (NIST). The frequency of attacks on organization information systems that contain confidential and sensitive data shows the need for implementing information security standards that will protect the material and intellectual values of an organization. Clearly, it is not possible to predict or sometimes prevent the attack, but it is possible to take all precautions to reduce the damage caused by the attack to a minimum. Failure to comply with cyber requirements can lead to catastrophic results. Keeping the critical infrastructure information system secure is a great challenge for the private industry as well as for government. The main goal of each organization is to provide constant availability of all IT resources and to protect data from theft, loss of consistency, or natural disasters while, on the other hand, ensuring normal operation of the information system. The vulnerability of the information system can cause financial loss,

harm the company reputation, and reduce productivity. Also, recovery of the information system would be costly and time-consuming. Government should enforce regulations that private industry must comply with at least with minimum requirements [12]. According to US-CERT, the latest cyber security incident in critical infrastructure involved infection with USB media. Investigators found out that company did not have appropriate detection tools to recognize risk on time [9]. Enforcing minimum security requirements assure that private industry is partially protected [12]. A minimum security requirement is not a perfect solution — breaches still can happen. But it will protect industry from basic malicious behavior. Security awareness training for employees is also important. An employee of the Dutch chemical giant DSM found an infected USB. Rather than plug the USB into computer, he brought it to IT Department. In this way, employee prevented system infection [9]. Even if the private industry exceeds the minimum security requirements, incidents and security breaches could happen. Vulnerabilities and weaknesses in popular software continue to represent the main threat to users and their data. The fact that cyber-criminals are still trying to exploit vulnerabilities that were discovered a few years ago is proof that cyber attacks are still a security threat. Unfortunately, even regular software updates of big manufacturers do not guarantee system protection, given that software makers do not always promptly publish the necessary patches. It is therefore very important to be careful, especially during browsing, and, of course, regularly updating antivirus software is a priority. An electrical utility invited US-CERT to assist in incident response when they found many abnormal activities on their network during regular assessment of its security controls. The company exceeded its security requirement by finding abnormalities before they occurred [9]. Government should eliminate barriers that prevent creation of risk-based systems connected to the private industry. Also, government should create and enforce consistent techniques regarding private industry weaknesses and threats as well as enforce baseline level of security and existing policies [3]. All these steps will help improve cyber security The DHS must discuss with government representatives how to use all resources to protect critical infrastructure from further cyber attacks [3]. Security policy should include all methods of using information systems in the company that will protect information and assets from threats, external as well as internal. Security policy should be unique and specific to each industry [12]. Private industry should use webmail services that offer encryption and decryption servers and eliminate the ability for users to manage their own encryption keys, and thus the possibility of encryption between the users. There is no company or manufacturer users can trust more than their own company. Corporate manufacturers almost always look to protect their profits and market share. Private industry needs to review security needs and to choose products that will meet those needs, no matter from which manufacturer [13].

6. PRIVATE INDUSTRY RESPONSIBILITY

Any system at any time can become a victim of targeted attacks. All potential threats, which we often are not even aware of until the threat activates, raise the priority of protecting the information systems. Security threats and attacks increase each day. Security maintenance is becoming an ever greater challenge each day for private industry. Private industry must be responsible to defend their critical infrastructure. Security could be at least at baseline level to deter cyber attackers from attacking critical infrastructure. Also,

users must be trained how to recognize potential threats. Raising awareness of users on information security, and the threats and attacks coming with cyber technology development, and training users on how to protect themselves to avoid unwanted damage are only basic steps in cyber security improvement in private industry. But, even though private industries usually train employees how to use a system, employees themselves are not always willing to participate in such training. Not all private industries pay too much attention on security training. In these cases, government should step in and mandate private industry to do security and awareness training for their employees. Internal threats pose security threats. Management of private industries needs to be convinced that investing in good security policy, purchasing and installing high-quality security equipment, and training users on information security are good investments. Cyber security will pay off after the first unsuccessful cyber attack. These investments will allow better protection of private industry information systems and thus lower the damage caused by intrusions [14]. Even when the best plan for information system security of the company is practiced, the company must be careful. With the development of new technologies, new options and possibilities are developed, and someone can easily break into the system.

7 CONCLUSION

Recent security breaches, such as ones on Google and private industry, are the cost of not improving cyber security in private industry. Government must make sure that private industry effectively protects its networks. Private industry is obligated to protect national security. It should incorporate good cyber security controls, follow security standards and regulations, evaluate systems for potential vulnerabilities, and perform risk assessments especially on critical infrastructure [3]. Any cyber attack on critical infrastructure can cause tragic consequences. Cyber attackers could potentially destroy critical infrastructure. Unsatisfactory protection could allow cyber attackers to attack and penetrate electric networks, water supplies, or nuclear networks. Such attacks could create damage to cities and eventually even kill or injure citizens. Power grids are very important for our economy, state security and, lastly, for quality of life [15]. Electrical energy is an essential factor for daily life, homes, hospitals, industry, and companies [16]. Any interruption of electrical energy would have a powerful effect on the economy as well as on state defense and recovery [16]. Stuxnet is the perfect example of how a malicious program targeted Siemens industrial software and equipment [6]. Critical infrastructure systems must be continuously evaluated and monitored for possible weaknesses and vulnerabilities. As much as government and private industry should be responsible for protecting critical infrastructure, it is very important that each individual has a role in protecting critical infrastructure. Individuals should have security awareness training to recognize risks and prevent potential attacks.

BIBLIOGRAPHY:

[1] Moteff, John D. Statement on critical infrastructure security (CRS Issue Statement, IS40271). Library of Congress. Defense Technical Information Center (DTIC), 2010, http://www.dtic.mil/dtic.

[2] Martin, Christopher. Protecting critical infrastructure: Making our program more effective. Carlisle: U.S. Army War College. Defense Technical Information Center (DTIC), 2006, http://www.dtic.mil/dtic.
[3] HSPD 7 Homeland Security Presidential Directive 7. Office of the White House Press Secretary, 2003, http://www.whitehouse.gov.
[4] DHS cyber security mission: promoting innovation and securing critical infrastructure: Hearing Before the Subcommittee on Cyber security, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security (Serial No. 112-19), 112th Cong, 2011.
[5] Rosenzweig, Paul. Cyber security and Public Goods: The Public/Private 'Partnership'. Hoover Institution, 2011, http://media.hoover.org/.
[6] Symantec Internet security threat report: Trends for 2010. Symantec Corp., 2011, https://www4.symantec.com/mktginfo/downloads/21182883_GA_REPORT_ISTR_Main-Report_04-11_HI-RES.pdf.
[7] Stevens, Gina. Data Security Breach Notification Laws (CRS Report for Congress, R42475). Library of Congress. Congressional Research Service, 2012.
[8] Rosenzweig, Paul. Cyber Security Act of 2012: Revised cyber bill still has problems (Heritage Foundation Issue Brief No. 3675). Heritage Foundation, 2012. http://www.heritage.org.
[9] ICS-CERT Incident Response Summary Report. Computer Emergency Response Team, 2012, http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Incident_Response_Summary_Report_09_11.pdf.
[10] Fischer, Eric. Federal laws relating to cyber security: Discussion of proposed revisions (CRS Report for Congress, R42114). Library of Congress, 2012.
[11] Cybersecurity: Threats to communications networks and public-sector responses: Hearing before Committee on Energy and Commerce, Subcommittee on Communications and Technology, the United States House of Representatives, 112th Cong. 2, 2012.
[12] FIPS PUB 200. Minimum security requirements for federal information and information Systems. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, March, 2006.
[13] Protection from Cyber Attacks. March 19th, 2010, http://www.personalmag.rs/internet/zastita-od-cyber-napada/?comments=true.
[14] Ledinek, Sanja. McAfee i Operacija Aurora, January 20th, 2010, http://www.racunalo.com/zanimljivosti/plavusa-u-ict-svijetu/6136-mcafee-i-operacija-aurora.html.
[15] Bidgoli, Hossein. Custom Textbook for CSEC 620. Hoboken: John Wiley & Sons, Inc., 2011.
[16] Bennett, Brian T. Understanding, Assessing, and Responding to Terrorism: Protecting Critical Infrastructure and Personnel. Hoboken: John Wiley & Sons, Inc., 2007.