Defending the Defenders: Cyber Crime and Government Contracting

David C. Shields

Submitted to Dr. Michael Hanners

In Partial Fulfillment of CSEC620

University of Maryland University College

Contents

Defending the Defenders: Cyber Crime and Government Contracting

Introduction

The modern world is fraught with warring countries, arms races, terrorism, and conflicting ideologies where feeling totally secure is almost impossible. However, it is the government's purpose to protect her people with whatever means is necessary including having the best weaponry and engineering when the battles turn to wars. Few other countries in the world are as well prepared, secured, and defensive as the United States of America which has some of the highest defense budgets, active military members and national wealth in the world (Global Firepower, 2011). In order for the government to maintain the military power it has amassed, it has turned to using several private companies to perform the engineering feats that the military alone is not able to provide. This need led to the creation of the defense contract industry which has launched the success of such industry giants as Lockheed Martin, Northrop Grumman, Boeing, and many others. These companies have access to and must consequently protect some of the nation's closest kept secrets making them a target of foreign militaries, terrorist organizations, rival defense companies, and even from their own staff. The theft of data from such a company could be as damaging if not more damaging than a theft of data from the government itself.

Foreign Militaries and the Arms Race

The USA has been aware of the importance of military prowess even unto the days when it was simply a rebellious colony battling the Revolutionary War in the 18th century. To gain Independence from Great Britain – the most powerful military in the world at the time – the USA developed new and non-traditional battle tactics which ultimately allowed them to win the war.

From that day to the present, the country is aware of the ingenuity and value of creating new weapons and new methods to win battles and this is reflected in the amount of money and the spending habits of the Department of Defense (U.S. Goverment Accountability Office, 2009, pp. 428-430).

Considering the size of the US Military in contrast to other powerful nations of similar size and technology level, it becomes poignantly obvious that the US is the military that would have to be beaten were another nation to become a superpower. To this end, it is no wonder that the weapons and tools in use by the USA are very appealing to any nation with desires to be the strongest in terms of firepower. In no other era was this more apparent than during the Cold War era where the espionage and danger of the unspoken battle between the USA and the former USSR have almost become legendary. Still to this day, Russia is the second most powerful nation in the world in terms of military firepower and were it to attain US military secrets, it could position itself to be first (Johnson, 2010, p. 308).

If a foreign government were to infiltrate or otherwise attain military secrets from a government contractor who had not properly secured the data, the results could be truly terrifying. At best, a foreign military could utilize the knowledge attained from the data to create some sort of defense against the weapon be it a method of detecting the attack of a stealth missile that was thought impossible to detect or by learning how to jam the controls of an automated attack drone such as the Global Hawk (Northrop Grumman, 2012). In a worst case scenario, if a foreign power was to gain access to data on a new weapon that was still being tested, they could possibly create their own version of the weapon and have it production-ready before the USA was able to perfect it. In situations like this, a single failure in the security infrastructure of a defense contractor could invariably result in the loss of countless American lives.

When the stakes are so high, it is no wonder that the US Government already goes to great lengths to protect the secrets it entrusts to a third party. The first line of defense is in the government classification levels which include ‘for official use only (FOUO),’ ‘classified,’ ‘secret’, ‘top secret’, and finally ‘sensitive compartmentalized information (SCI)’ (US Department of Defense, 2006, p. 2.21.5). Each clearance level requires higher and higher scrutiny of the candidate(s) seeking the clearance and includes documentation to prove citizenship, an exhaustive investigation of the person’s life, and sometimes a polygraph test to evaluate the character of the person. Even after a candidate has passed the rigorous background check and attained a clearance, they are still bound by what is known as the “Need to Know” which implies that they will not be given private information that the person has no business need to have (US Department of Defense, 2006).

To protect data, security groups within these military contracting companies are likely to focus their attention on unusual traffic from known foreign IP addresses, access levels to datacenter information, and security training in hopes of reducing as much risk as possible (Clark & Levin, 2009, pp. 19-20). An attack may also be identified by careful analysis of foreign government websites, social media outlets, and even public media outlets both national and international. Yet attention cannot rest on securing the network alone as physical security is also critical in identifying attackers or potential threats. Many defense contractors position themselves on military installations such as Air Force bases to gain military protection or at least create a detailed identification method for allowing external parties access to their facility for meetings or other purposes (Stallings, 2009, p. 639). The more security controls that an organization can put in place from the network to the building the better they can defend against a foreign interest seeking to gain their secrets.

Preventing Terror and Those Responsible For It

The attacks of 9/11 have become synonymous with terror in its worst possible form, serving to awaken a sleeping nation with a fiery vengeance. It is common knowledge that in the aftermath of 9/11, the US Government enacted broad and far-reaching changes in the fundamental makeup of the FBI, CIA and other government bodies to allow them to mobilize quickly to begin the War on Terror. One of the most notable items is the drastic increase in the funds allotted to the DoD to help with the war efforts which gave rise to an explosive growth in the defense industry (Johnson, 2010, p. 315).

Terrorist groups, much like foreign governments have a great deal to gain by having access to government secrets and defense companies must be wary of this possibility. It would not be unimaginable that a terrorist organization might attempt to ‘plant’ an informant within a military contracting firm. The data they could attain from such an informant could prove indispensable in learning what capabilities the military might have against their organization or even allow them to defend against a new weapon or create their own. The very fact that a terrorist cell has access to any kind of privileged government or military data is a terror tool in of itself and could prove to be extraordinarily powerful in advancing the aims of the group.

A critical element of successful terror plots is the ability to induce terror upon the targeted people or people group. If a terrorist group actually obtained the data from a defense contractor about classified government intelligence or a new weapon, it would serve them well toward their goal (Clark & Levin, 2009, pp. 18-19). Not only would there be intrinsic value of keeping the group one step ahead of its foes, but also there would be great value in using what has been collected for any number of propaganda schemes.

It might even be feasible for a terrorist group to sell the knowledge they have acquired to another foreign interest and earn a profit to further fund their terror activities.

The same controls that are in place for protecting this data from foreign militaries are also used to help identify red flags that might indicate terrorism ties including the extensive background checks, the security clearance research, etc. Furthermore, terrorist organizations have taken to the Internet to discuss and plan their activities and organize in relative anonymity, yet federal intelligence agencies have been able to use various methods to acquire information about possible terror plots on the Internet. As a result, the US government can quickly disseminate a large amount of this information to law enforcement and other agencies to coordinate the dissolution of a terrorist attack (Broadhurst, 2006, p. 83).

One final chain of identification and defense against terrorists accessing military contractor data is the use of export control policies when shipping or travelling abroad. These export control polices make it a crime to transfer any thing that could potentially contain government or national security data without a detailed series of export material information being logged (US Department of Defense, 2006, p. 10.202). The use of such stringent guidelines on what can be transmitted as well as how it can be transmitted make the transfer of government secrets to parties outside its borders extremely difficult. Techniques such as this are not guaranteed to protect government data from terrorists but go quite a distance in mitigating a majority of the risk or isolating it were it to occur.

The Capitalism of Neighbors

The United States has created a superpower from a rebel nation by doing things in a way that differentiates it from other nations including the rights to free speech, the overarching authority of the Constitution, and a sense of strong personal identity.

One of the underpinnings of the success it has achieved is the use of a predominantly capitalist system of business which allows all races and walks of life a chance at using their ideas for profit. This desire for profit, however, has created an unintentional dependence and infatuation with money among all people from CEO's to restaurant staff sometimes with little value placed on the morality of the affair. The 2000's saw the exposure of many capitalist follies to the general public and the 2010's ushered in things such as Ponzi schemes being revealed. Although these items are not particularly ethical, they are most certainly capitalistic in nature. The drive to make more money and accomplish more success can sometimes lead the management of an otherwise reputable company to engage in underhanded acts which could ultimately put stakeholders at risk of losing their assets or at least risk the loss of valuable intellectual property (Perkins, 2009, p. 745). The case is just as common in military contracting companies as it is almost everywhere else in the USA.

In the case of defense contracting companies, the common practice for acquiring the rights to work on government contracts is by a detailed selection process known as 'bidding.' In the bidding stages of a contract, multiple organizations are offered the opportunity to present their case for what makes them the best choice for the contract as opposed to their peers. The criteria offered by the bidding company is usually based of factors such as the company's resources and experience in a particular, relevant, project or field coupled with the quality of work performed on prior projects and often the current standards level their company has been awarded such as by auditing organizations like the International Standards Organization (ISO) (Kleiner & Cazeau, 2012).

It is virtually impossible to find another environment where capitalism is more alive than in the world of military contracts where the money being spent and the potential profit are almost endless as perceived by the author of this document who was once part of such a company. If a rival company were to desire to win the award over another military contractor, it would have a considerable amount of motivation to acquire data from its rivals. Chief items of interest are likely to include the procedure used by rival companies in their bidding process as well as some of the proprietary data about prior projects of a similar nature and these items in the defense industry are often as valuable if not more valuable than trade secrets of other industries.

In the event of a data breach by a rival company, a military contractor has a considerable amount of concerns both tangible and intangible of what could be lost. The primary loss may be geared more toward the actual raw data such as design schematics or company intellectual property that could be used to reverse engineer products or techniques (Verizon Business, 2011). The more pronounced issues, on the other hand, are those regarding the public or government's opinion of the organization's security controls and general reputation. Indeed, a breach of military contractor data may not only pose a risk to national security but also may create a negative opinion of the company that could severely hamper it from performing any future work and/or losing the contracts currently in place. The end result could prove most advantageous to a rival company that can use the public opinion of the company that has been breached as a catalyst to earn the contracts it desires.

Considering the tumultuous environment of national security and the often cutthroat industry of military contractors, the identification and concurrent defense mechanisms an organization in this industry must implement are required to be thorough, granular, and uniform.

The most common way for an organization to accomplish this task is to adopt DoD standard security settings such as those outlined in the National Industrial Security Program Operations Manual (NISPOM) as part of the regular security posture. The standards represented in the NISPOM are tested and expert reviewed as some of the best practices for defending against the known vulnerabilities of a program or operating system even if it comes at the expense of less user control in the environment (US Department of Defense, 2006, p. 1.22.1). Furthermore, the NISPOM's guidelines do not limit coverage to only computer systems; they include physical security guidelines, audit guidelines, access controls and even physical placement guidelines to improve the overall security of the organization. When used in tandem with additional standards systems such as ISO, COBIT, and ITIL, the resulting security posture will make detection of breaches from rivals and the proactive security measures needed to prevent said breaches far more attainable (Glass, et al., 2009).

Combatting the Danger Within

A common factor between the items expressed in this document thus far is that each of them is an external force military contractors must secure themselves against but all of them pale in comparison to the potential danger of an insider threat. In the experience of the author, the environment of a defense contractor is not too unlike the environment of a soldier in the military itself: the chain of command is rigid and frequently inflexible, the expectation is for uniformity in both the building and its inhabitants, the acronyms are ever-present, and a large portion of the staff are former military themselves. Despite this stark difference when comparing a defense contractor and most private businesses, it is logical that organizations whose primary customers are military would want to fashion themselves in a similar manner… as the old adage says "When in Rome…" .

As with the military, it is not too far-fetched to conclude that the rigidity and detail oriented world of military contractors may be taxing on the mental state of its employees. Furthermore, employees of defense companies are people just like everyone else and people can be motivated by many factors to perform tasks that could put the organization and its data at risk. An insider may be a disgruntled employee who has been passed over for too many promotions or an employee who has taken to gambling as the result of personal stress and consequently developed a rather nasty gambling debt, or perhaps the employee is simply a talented individual who has been limited to a job with limited creative outlets so they begin to push the limits of what they can do. Any of these factors are completely logical and possible reasons to cause a normal person to become a threat (Dittrich & Himma, 2006, pp. 138-139).

If an insider were to decide to do harm to their employer, the enormity of what is at stake can not be measured in simple terms. It is completely plausible that an insider could use their access to the data as a negotiation tool with any of the parties already discussed in this document. A foreign government could use a willing insider to mine a considerable amount of data while bypassing the existing security controls that would otherwise prevent such an action. A terrorist group could likewise convince an employee or contractor of the defense company to provide them with data, insider information, or guidance on further infiltration to the company's resources – probably for only a small monetary compensation (in fact, this was the backdrop of 'Dissecting the Hack' a computer crime book by noteworthy IT security professional, Jayson Street). Even a rival company could use a well-placed insider to acquire any amount of data they were interested in but the communication of the gathered information may be more susceptible to being noticed than the communication with terrorists or foreign militaries.

The risk of insider threats is one of the most challenging risks to mitigate as it is somewhat challenging to know whether or not an individual runs the risk of becoming a threat but there are a few methods to reduce the risk. It is common protocol in most organizations (especially larger organizations) to perform some form of background check on their employees which can vary in the breadth and scope depending on the company. Additionally, it is becoming more common for companies to request a consumer credit report as a prerequisite for employment offers (Bright, 2012). The simplest way to defend against insider threats is to hire the right people for the right position.

Conclusion

The US government must be able to efficiently create new technology and innovation to remain the leaders of the free world and one of the ways to accomplish that goal is to depend upon the industries of the people including defense contractors. While it is true that any number of rogue elements such as foreign military, terrorists, rival companies, and even the employees of these companies could conceivably put the information at risk, much has been done and continues to be done to reduce that risk. Ultimately, the true means to secure an organization and its data lies in the people and processes that are used which include clearly reviewing backgrounds of people, keeping an eye on the world around them, and demanding only the utmost professional and stable people in the employ of the organization. The need for security clearances, government processes, and virtually all government standards arose from the need to secure the data which protects the people of America. Industry will continue to improve and evolve to protect threats both now and in the future and so will the ways to protect the people.

Bibliography

Bright, P. (2012, January 1). *How Does a Business Do a Background Check on Employees?* Retrieved from eHow: http://www.ehow.com/how-does_4566323_business-do-background-check-employees.html

Broadhurst, R. (2006). Combatting the Cybercrime Threat: Developments in Global Law Enforcement. In H. Bidgoli, *Custom Textbook for CSEC 620* (pp. 83-95). Hoboken: Wiley & Sons Publishing Inc.

Clark, W. K., & Levin, P. L. (2009, November/December). Securing the Information Highway: How to Enhance the United States' Electronic Defenses. *Current*(518), 18-22.

Dittrich, D., & Himma, K. E. (2006). Hackers, Crackers, and Computer Criminals. In H. Bidgoli, *Custom Textbook for CSEC620* (pp. 137-154). Hoboken: Wiley & Sons Publishing Inc.

Glass, D., Davis, C., Mason, J., Gursky, D., Thomas, J., Carr, W., & Levine, D. (2009). Security Audits, Standards, and Inspections. In S. Bosworth, M. E. Kabay, & E. Whyne, *Computer Security Handbook Volume 2* (pp. 54.1-54.24). Hoboken: Wiley and Sons Publishing Inc.

Global Firepower. (2011, July 1). *Military Strength of the United States of America*. Retrieved March 13, 2012, from Global Firepower: http://www.globalfirepower.com/country-military-strength-detail.asp?country_id=United-States-of-America

Johnson, L. (2010). Evaluating "Humint": The Role of Foreign Agents in U.S. Security. *Comparative Strategy, 29,* 308-332. doi:10.1080/01495933.2010.509635

Kabay, M. E., & Robertson, B. (2009). Employment Practices and Policies. In S. Bosworth, M. E. Kabay, & E. Whyne, *Computer Security Handbook Volume 2* (pp. 45.1-45.17). Hoboken: Wiley & Sons Publishing Inc.

Kleiner & Cazeau. (2012, January). *Government Procurement 101: The Bidding Process and How It Works*. Retrieved March 14, 2012, from Kleiner and Cazeau, Attorneys at Law: http://www.kleinercazeau.com/government-contract/government-procurement-101-the-bidding-process-and-how-it-works/

Northrop Grumman. (2012, January 2). *The Value of Taking the Ultimate High Ground*. Retrieved March 14, 2012, from Norhtrop Grumman Corporation: http://www.northropgrumman.com/performance/#/unmanned-systems/air/q-4-enterprise

Perkins, K. (2009). Data Loss Protection. In J. R. Vacca, *Computer and Information Security Handbook* (pp. 745-762). Hoboken: Morgan Kauffman.

Stallings, W. (2009). Physical Security Essentials. In J. R. Vacca, *Computer and Information Security Handbook* (pp. 629-643). Burlington: Morgan Kauffman.

U.S. Goverment Accountability Office. (2009). Federal Contracting: Guidance on Award Fees Has Led to Better Practices But is Not Consistently Applied. *Journal of Public Procurement, 9*(3-4), 420-463.

US Department of Defense. (2006). *National Industrial Security Program Operating Manual.* United States Government, Department of Defense. Washington D.C.: DoD.

Verizon Business. (2011, July/August). 2010 Data Breaches Quintupled, But Less Data Stolen. *Information Management, 45*(4), 15.