Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Lack of Oversight Spoils Funding for Cyber Security

<p>In the 1983 MGM movie, War Games, the main character was speaking to a computer that was trying to start a real World War III using a war game scenario. After a long rest, the computer started to restructure some of its moves, prompting David to say, "Are you still playing the game?" The computer responds, "of courseâ ¦." And begins its countdown to launch of missiles. When we hear of a new type of attack on a US computer system it is a reminder that we are still playing the game and it hasn't changed very much ...

Copyright SANS Institute
Author Retains Full Rights

AD

Lack of Oversight Spoils Funding for Cyber Security

Dennis F. Poindexter
Dennyp06@gmail.com
703-405-9659

Submitted for Pre-publication review to DNI on October 11, 2010
Finished review by DoD on 5.12.2011 and approved by DNI 13 May 13, 2011

© 2011 SANS Institute, Author retains full rights.

The Game

In the 1983 MGM movie, War Games, the main character was speaking to a computer that was trying to start a real World War III using a war game scenario. After a long rest, the computer started to restructure some of its moves, prompting David to say, "Are you still playing the game?" The computer responds, "of course…." And begins its countdown to launch of missiles. When we hear of a new type of attack on a US computer system it is a reminder that we are still playing the game and it hasn't changed very much in the last 15 years. There are lulls, breaks and periods of relative calm, but they are still playing the game.

I was Program Manger of a development program called SHADOW, an intrusion detection network that started as a thought of how Missile Defense might be able to do intrusion detection fast enough to find, stop, and maintain the information systems that make up a ballistic missile intercept network that finds and shoots a target before it can reach the United States. If we were going to stop a network attack it would have to be able to detect the attack event, identify the root cause, prepare to isolate it, and continue to operate the rest of the network to fire the defending missiles. Most of the systems we had were having difficulty doing this type of thing in less than a few hours. We had to be able to do it much faster than that.

What SHADOW showed was something that scared a lot of people, including us. There are some pretty sophisticated people out there mapping our networks, testing various types of penetrations, and leaving behind little evidence that they had been there. They were able to do some interesting things like this:

On Tuesday, a person pings a computer on a network by sending out a brief command, directed towards any computer that might be found at an address that says, "Are you there?" Most computers will reply. On Wed, a person pings a computer on another network in the same subnet. On Thursday, another ping... and so on. If we did the same kind of thing on a street, each day we would mail a letter to one possible street address in a given series, like on the 400 block of James Avenue we send a letter to 401 and we keep track of the addresses where the mail is returned as "No such address". The second day, we send a similar letter to 400 Bluebell Lane, which is the next street over, and we keep doing this until we have all the street numbers. Electronically, this can go pretty fast, and at the end you would have a map of all the computer addresses of every computer on every network, if none of them were protected from such things.

Nobody does this, of course, unless they are mapping the networks and don't want us to know they are doing it. They ping (or use a variety of other methods to get through firewalls to map inside) infrequently on any single network because anyone seeing this kind of activity on a single network would become suspicious. They were mapping all the systems where we had sensors, from the East Coast to the West.

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Next, they would go back and run certain types of "probe" attacks against each system to check to see what types of operating systems were being used. Then they would try certain types of attacks to see if patches for known vulnerabilities had been installed on each one. At he end of all of this, they have a map of the network, what each type of computer is, what it is vulnerable to, and, if they take the time to update this once in awhile, they can attack pretty much anywhere and be successful. What they learned to do was to capture these vulnerable computers, chain them together, and use them to launch attacks against other computers. These people have a lot of time on their hands and they are very, very good at what they do.

It reminds me of something Dr. Parker used to tell us at USC, "Criminals spend as much time at their job, as you do at yours." They were preparing to do successive generations of software builds on their attack software, each with new capabilities to do automated penetration and attacks and to gradually improve their products. We observed them testing but not deploying some software, which means they had capabilities they were not showing to anyone else. We were able to predict and warn certain people in the government, that the attacks, which brought down E-Bay and a few others in February of 2000, were going to occur. We said they would happen in January, based on their previous software development cycle, but they did not keep their schedule up very well over the holidays.

That was 11 years ago. They have made quite a few improvements since then and they have a great deal of competition.

Today, a hacker is not a 16 year-old in the U.K. building a reputation for himself in the swampy black holes of the Internet. He is more likely a government-sponsored ring or a gang member from an organized gang who has devoted considerable resources and time to learning a trade and profiting from it. This was a change that we were not, but should have been, ready for. We used to say that it was difficult to defend against a nation state if one decided to attack, but that it was not as difficult to defend against the average threat. Now the gangs are organized and the governments allow them to operate and it is a completely different game. The banking community has had state-tolerated criminal gangs operating from Nigeria since the early 1980s, and they are still playing the game today. They were the first to employ the "we found a bag of money that we think belongs to you, so send us some money to get it" type of scam that is still working on the more gullible of the Internet users. A gang can steal credit card numbers in the US and have them in Eastern Europe in a few minutes. They can use those account numbers in the same day, and they have done it so often that the price of those numbers is below one dollar. General Alexander at the National Security Agency's Cyber Command, notes Verizon's study earlier this year that said it is not a lack of ability that keeps most of the hackers out, it is a lack of time to attack all the vulnerable systems they see[1]. This kind of criminal activity is said to cost businesses nearly a trillion dollars a year[2].

---

[1] Alexander, Keith, *Cybersecurity Policy and he Role of U.S. Cybercom*

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (CSIS), 3 June 2010, page 5.

http://www.nsa.gov/public_info/_files/speeches_testimonies/100603_alexander_transcript.pdf

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

But, it is not just about the financial losses of the business community. Either through neglect or purpose, the Russians and Chinese seem to have become our adversaries in collecting information from computer systems owned by our businesses and government. This is espionage. The dollar losses of industry, reported by the FBI, are indicators of the level of *criminal* activity, which is often measurable by a loss and can be found through good transaction-based auditing. But what the Russians and Chinese do is different. Good espionage does not show a loss and is hardly ever noticed or reported to anyone. We only see it when the information is used to produce goods or services that are based on the information being collected. They let us do the research, then steal it and use it.

The type of attacks, and success of them, is pretty much the same whether the purpose is espionage or criminal activity. The purpose is what the Intelligence Community euphemistically calls, "exfiltration" which almost sounds like something good, but it really the surreptitious removal of information. It is a little hard to imagine that our enemies do this simply by allowing private citizens the opportunity to use the Internet for their own profit. They help them overtly, or they tolerate their activities because they are beneficial. At the introduction of e-mail, Nigerians began sending out letters that told people large sums of money were being held for them and could be retrieved by sending a handling fee to their representatives. Those who do this sort of thing claim to be unable to control hacking of US systems anymore than we can control our own Internet users from hacking in China. It is hardly a coincidence that most of the attacks we see coming at the US are ultimately traced back to China and Russia; we have been playing this game for along time.

- Over 20 years ago, East German hackers [a Russian proxy at that time] were stealing information from US companies to sell it to the Russian government. Cliff Stoll published The Cuckoo's Egg about one of these incidents. The jacket of the 1989 book says, "Computer espionage is without question the single most important security issue of the 1990's". Cliff was not a security expert and did not care much about security in general. He was an astronomer by profession. We were sitting on the fantail of a boat in the harbor in Baltimore and I asked how he could have the persistence to continue on when he was not getting very much help from the government, and was only doing this part-time. He said, "They were in our computer systems and they didn't belong there. I had to do something about it." This clear thought might be useful to the federal agencies charged with protection of our networks.

- In 1987, a hacker (the 16 year-old) broke into Defense Department computers, AT&T and NATO, stole an artificial intelligence program worth a million dollars. Over the years many people have stolen information from the Defense and Defense contractor computers, but it rarely makes the news.

---

[2] Mills, Elanor, Cybercrime Cost Firms $1 Trillion Globally, CNET News, 28 Jan 2009 http://news.cnet.com/8301-1009_3-10152246-83.html

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

"There is growing evidence of the use of electronic intrusion techniques by industrial spies. Hackers have reported that they have been offered substantial sums of money to gather information on corporations. There is evidence that technical intelligence officers from Eastern European foreign intelligence services, in particular the former East German Ministry for State Security, are selling their talents to the highest bidder. [26] Scott Charney, Chief of the Computer Crime Unit, General Litigation and Legal Advice Section, U.S. Department of Justice summarized the problem:

High-tech spying is becoming commonplace, and hackers/spies are being actively recruited. When such a hacker strikes, he or she is often weaving through the telephone network and it may be extremely difficult to tell where the hacker is coming from, what the motives are, who he or she is working for (if any one), and what locations have been attacked...In a recent survey of 150 research and development companies involved in high technology industries, 48 percent indicated they had been the target of trade secret theft. The use of computers in developing and storing trade secrets has made such secrets more susceptible to theft."[3]

The Intelligence Threat Handbook, 1996[4]

- In 1988, Robert Morris Jr. (it was Robert Morris Sr. who got Cliff Stoll into the National Security Telecommunications and Information Systems Security Committee (NSTISSC) which ultimately got him the support he needed) created the Internet Worm that infected thousands of computers and was prosecuted in Federal court. He says he didn't mean to do it, but Internet postings after the fact, indicate the worm sent passwords back to Morris, tried attacks with commonly used passwords, analyzed encrypted passwords, then used successful attacks to try to infiltrate other similar systems the user was connected to[5].

- In 1994, Russian student Vladimir Levin, and his gang hacked into Citibank and stole more than $10 million. At the time the biggest computer theft ever. Levin and his accomplices used stolen access codes and passwords to transfer stolen funds across the United States, Europe, and Israel. Months after, he was arrested by Interpol and extradited to the U.S. to stand trial, where he managed a plea bargain.[6]

---

[3] Charney, Scott, *The Justice Department Responds to the Growing Threat of Computer Crime,* Computer Security Journal, 3:2, Fall 1992, pp. 1-12.

[4] *The Intelligence Threat Handbook*, Interagency OPSEC Support Staff, April 1996, Section 5

[5] Spafford, Eugene, *The Internet Worm Incident*, Department of Computer Science, Purdue University, 19 September 1991.

[6] Ramirez, Jessica, Educating Elite Hackers, Jessica , Newsweek Web Exclusive

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

- In 1998, there was a great deal of publicity about Moonlight Maze, Russian hackers in US systems, which Vernon Loeb, Washington Post Staff Writer reported this way: [7]

> "A series of sophisticated attempts to break into Pentagon computers has continued for more than three years, and an extensive investigation has produced "disturbingly few clues" about who is responsible, according to a member of the National Security Agency's advisory board.
>
> The NSA consultant, James Adams, says U.S. diplomats lodged a formal protest with the Russian government last year after investigators determined that the cyber attacks, which they code-named "Moonlight Maze," appear to have originated from seven Russian Internet addresses. But Russian officials replied that the telephone numbers associated with the sites were inactive and denied any prior knowledge of the attacks, according to Adams.'
>
> "Meanwhile, the assault has continued unabated," Adams wrote in this month's Foreign Affairs magazine, published by the Council on Foreign Relations. "The hackers have built 'back doors' through which they can re-enter the infiltrated systems at will and steal further data; they have also left behind tools that reroute specific network traffic through Russia."

We learned from SHADOW that we were nowhere near ready to deal with the types of people we were observing. They were much more sophisticated, thoughtful and careful about their products and it was good quality work, regardless of how the press portrays it. They made rapid progress in their builds and they had quite a bit of time. They worked at it. They had development cycles we could observe and they improved their products incrementally. It was almost more efficient than a business that does the same thing. They were not as clever about their code, but they were steady.

Last year, Verizon published a report on the criminal hacking they had been observing, that found 75% of the attacks were coming from outside and most of them were from Eastern Europe. The majority of attacks were directed towards financial institutions (not exactly a revelation, of course) and they were very successful in their work[8].

Mar 10, 2010

2. Shimomura, Tsutomu *Takedown: The Pursuit and Capture of America's Most Wanted Computer Outlaw -- By The Man Who Did It,* with John Markoff (Hyperion, January 1996).

3. Washington Post, Monday, May 7, 2001; Page A02

[8] Verizon Business Risk Team, *2009 Data Breach Investigations Report*, page 22.

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

It is getting easier for hackers, and they are getting better at it. Yet, we don't seem to be making the same type of progress in stopping them. The Administration will tell us that these new attacks require immediate attention (money) and that something extraordinary has to be done, right away. Keep those types of comments in perspective. There are many new people in the government who are not very good at history, past the last election, and they can be easily led. New money is not what is needed. A new focus is required. We need to better manage the money we do have.

Silver Bullets for the Good Guys – Following the Money

In 1977, I was a Computer Staff Specialist in the Defense Department doing inspections of computer systems in contractor systems that processed classified information. When the government brought us in, they explained that we were to be in our jobs for "about 5 years" and then we should start looking for jobs elsewhere. By that time, the people coming out of school would know enough about computer systems to be able to deal with most of the auditing of systems that we were being hired to do. They would understand computer systems, be comfortable with them, and be able to secure very complex systems. That certainly never happened.

One of the inspections took me to a Mid-West research facility, to audit a classified program of the Defense Department. ARPANET was designed as a distributed system with survivability in the event we were attacked with nuclear weapons carried by Soviet bombers. It needed to be able to reroute messages somewhere else if a huge section of the infrastructure were to be melted under one of those bombs. It did not seem like a very likely scenario, but it was magical to see notes appear from nowhere and try to get a grasp on how to secure something that was moving around and had no substance. The professor who was researching this project was working on a task called Multi-level Security (MLS). The way it was supposed to work was to have users of different classification levels (TOP SECRET, SECRET, CONFIDENTIAL and Unclassified) engaging these messages according to what they were allowed to see. The basic rules were that you could not read something at a classification level above yours, but you could read things below, i.e. a user with a TOP SECRET clearance could read anything on the network, but a user cleared CONFIDENTIAL could not read TOP SECRET or SECRET messages. It seemed to be simple, but he took the time to teach, his real profession after all, and it left my brain totally absorbed in the complexity of it.

It tuned out that the idea that person could have a TOP SECRET clearance and get access to everything was overly simplified. There were compartments of TOP SECRET, called Sensitive Compartmented Information (SCI) that not everyone was allowed to see just because they were cleared to that level. There were thousands of these. There were some Special Access Programs that only certain people with SCI Access could see. So not only did you have to figure out how to give access to people who were cleared, but they also had to be authorized into the compartment. These were called access authorizations and there were some for SECRET too. There were so many variables to this that it was not easy to map them out, but that is what they were doing; then, they would figure out

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

what had to be done to implement these through security mechanisms at every level of the network. It was complicated and they had no idea how it could be done. This was interesting security, but as it turns out, nobody could do it. After thirty years, we are still building the Internet but we can't do the security that was envisioned at the time, though it certainly is not a technical problem. The basic hurdle always has been that, given the number of checks that had to be made on access authorizations, it took so long to make a decision about whether a person could have access, that a system was too slow to be useful. It was, at the time, the silver bullet of cyber security. If we could just get a system to do multilevel security, the world would be safe again.

Twenty years later, we had a meeting in the Ballistic Missile Defense Organization (BMDO is now the Missile Defense Agency) about the same issue. One of our senior military men was spending quite a bit of money to try to reinvent multilevel security for our programs, using a small subcontractor that he favored for work. We got into a heated argument about his program's merits. I told him he was throwing money down a rat hole that the National Security Agency (NSA) had already spent millions trying to do unsuccessfully. He said he had the matter under control and could handle it. This is Bureaucrat-speak for, "Leave me alone – I am doing this whether you like it or not". He forgot, for just a minute, that he was spending part of my budget.

I went to see one of the senior executives about it. I told her what was happening and she didn't even mull it over; she cut off the funds that day. It seems she knew the history of Multi-level security and the amount of money the NSA had poured into trying to make a whole series of products that would eliminate evil in every computer network. From 1990 until 2000 they spent hundreds of millions of dollars trying to reach this holy grail of cyber security and hardly accomplished a thing. The programs were called MISSI, the Multi-level Systems Security Initiative. We were mandated to buy computers with built-in interfaces for MISSI cards that would encrypt every transmission made over any systems that used it. If it had worked, we wouldn't be worried about the Russians or Chinese getting into our networks. It has come to symbolize the waste that has gone into searching for a silver bullet that will make systems secure.

In January 2008, President George W. Bush was persuaded to sign National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23) which was intended to correct some basic vulnerabilities identified in our interconnected set of networks. It is supposed to do the following:

> **To establish a front line of defense against today's immediate threats** by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the Federal Government—and ultimately with state, local, and tribal governments and private sector partners—and the ability to act quickly to reduce our current vulnerabilities and prevent intrusions.
>
> **To defend against the full spectrum of threats** by enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies.

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

> **To strengthen the future cyber security environment** by expanding cyber education; coordinating and redirecting research and development efforts across the Federal Government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace.

There are twelve initiatives included in the implementation of this Directive and two of them define the Federal Enterprise as a single network to be defended, two of them direct the placement of sensors on that Enterprise, and the others are to get agencies to cooperate better. From the standpoint of ownership, this seems like a good thing to do. We have identified the Federal enterprise as a single entity that is owned by the Federal government and not the Federal agencies.

There are two new silver bullets, automated sensors on the networks, and something called "situational awareness" which, like pornography, few can define but all can know when they see it. It is an attempt to visualize the complex set of attacks that go on through out the world and it is a preoccupation of government leaders. Nearly every Federal agency has established a center where information [collected from every source they can get access to] is collected, analyzed and displayed – the larger the screen, the better. The only useful purpose of duplicating capabilities across the agencies is the feeling that someone has their finger on the pulse of what is happening in cyberspace. It leads to some bizarre situations where the collection of the information is more important than how it is used.

The Operations Center of the Department of Homeland Security (DHS) is a typical government center. It follows the examples of many such places like the National Critical Infrastructure Protection Center, the National Threat Operations Center at the National Security Agency (NSA), National Cybersecurity and Communications Integration Center at DHS, the Joint Interagency Task Force/Global Network Operations and hundreds of others established for each agency of the government. We once looked at the number of "operations centers" in the different services and agencies and found over 100, all doing similar types of work. You only have to read a little of the statements published about these places to know that they are each in charge of the Federal effort to collect and analyze information about the operational status of our national networks and to fight people trying to get into them. There are so many of these centers that none of them are in charge and they spend more time fighting each other than getting control of the hacking of our networks.

The Director of National Intelligence (DNI) tried to get them to cooperate, without much success. Having the Intelligence Community managing this type of initiative made the civil agencies less trustful of the whole process and the National Security Agency (NSA) was not making it any easier to do. Private contractors and government civil agencies were submitted reports on incidents they discovered, only to have NSA classify them by adding information. This prevented many of those sending the reports to ever see them again. Many of the contractors did not get the classified analysis nor see other reports that were similar to their own. Neither the civil agencies nor commercial contractors who reported the events liked this very much, but neither could we get DNI to change the way

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

NSA did business. It was over-classifying the entire reporting structure and making exchange of information more difficult.

For several months, we had worked on getting enhancements done to the DHS Center to try to make it ready to coordinate another part of its mission, natural disasters, such as those it was about to face during two hurricanes, Katrina and Rita. The IT staff at Homeland Security seemed to have a different idea of what types of enhancements were required to make an Operations Center more effective. They wanted to develop more ways to integrate and display large volumes of information which would come in from all the agencies in the government universe. It is as if the data display will result in "situational awareness" that will allow persons to make decisions they could not have made without those displays. The first thing DHS did, last year, with millions of dollars in money that came from another CNCI initiative, was to build a new operations center to support the one they already had. During hurricanes Katrina and Rita, the agency actually had to use this information to manage an event.

Almost a year before Katrina actually hit New Orleans, the Intelligence agencies were coordinating to have satellite imagery available so the analysts would have before-and-after images of any emergency situation that might occur. This would give the analysts some means of comparing what the ground looked like before it was flooded, bombed or contaminated with a chemical. This is not as easy to do as it might first appear, since imagery from US spy satellites cannot normally be taken over our own territory, without an exception by the President. There is nothing sinister about this. It is illegal to allow US Intelligence assets to "spy" on the US, even though it is clear why they would be doing it. This was a complicated process that was concluded in plenty of time to get the data before the first hurricane hit.

What we didn't know at the time was the DHS Center could not download the data directly from the intelligence sources. They didn't have the right kind of equipment or the infrastructure to handle large volumes of formatted data, let alone display it. The National Geo-Spatial-Intelligence Agency (NGA) which was processing the data, had to download it to CDs and hand-carry it to DHS. It was a little hard for us to imagine how this process would work in a middle of a dirty bomb exploding or a widespread disease outbreak. When it was received, there was more data than they had anticipated and they did not have adequate storage for all of it. They did not have the right software to process the data in the formats that intelligence data comes in, nor the training to operate the systems when the data came in.

Every plan that is written for emergency response, every scrap of policy and operational procedure, said the Operations Center was going to use data, supplied by other parts of the government, to analyze the events and direct actions of first responders. Yet it was clear the basic infrastructure to download the data, store it, and process it was not there. They simply had other priorities.

When Katrina hit the coast, it did not take long for the White House to start asking for some analysis of the damage. The Operations Center had nothing to give them. The first

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

images they were able to provide to the senior White House leaders were cut and pasted from Google, which had the only ones DHS was able to access and manipulate. We decided the best course would be to download commercial imagery from a local company that already had a contract with the federal government. This would give the Center the data they needed in a format they could manipulate. The commercial company was very cooperative and tried to get the data to us as quickly as possible. It was already paid for, so any government agency could download it if they had the ability and passwords from the vendor. It would have been better if we had just given it to Google.

Our liaison gave the passwords to the Operations Center and was ready to help with the analysis as the data came in. DHS was trying to download it, but could not. The imagery contractor thought there might be something wrong with the DHS end of the transaction since they seemed to be able to give the data to other government agencies without a problem like the one we were having. One of our engineers checked the circuits and found nothing wrong with them, but they were too slow to do a normal download of a size that was needed for such a huge amount of data. He had a solution to the problem. He went to his home and downloaded the data on his personal computer, copied it off to DVDs and brought them back to the Operations Center.

We had run exercises with this Center on biological and nuclear attack scenarios that depended on accurate and timely data being analyzed and sent to first responders and it was difficult for us to believe that none of the capabilities ever really existed. If the incidents had been as real as these hurricanes, it would not have taken long to find out how poorly these systems performed.

What it illustrates more than anything is the lack of accountability for money being spent on our national networks. Government agencies do not seem to care very much about what the money is allocated for; once they have the money, they spend it on whatever suits them. Collectively we spend billions of dollars on IT for the Federal government, and according to many of the GAO and Inspector General reports of the last 20 years, much of it is wasted. For the most part, it is because people have spent it on whatever they want to do and not on what they said they would do with it. DOD is generally cited as the best example of this but it wasn't DOD; it was just a small part of it, the Army.

In 1996, the Ballistic Missile Defense Organization (BMDO) funded a large percentage of the information technology budgets of Redstone Arsenal, Huntsville, Alabama which had the major military components of Army that built and maintained missile systems needed for command and control, business systems, and design capabilities for contractors. We had advised them the year before that we wanted to do a regional assessment of security of their networks, looking at contractor and government systems, so they were especially interested in being ready for that assessment. After all, we controlled their money.

We noticed a substantial number of programs asking for additional money for security of their IT systems. At first, we did not pay a great deal of attention to this because we were already paying for security in the budget lines of most of the programs that were requesting the additional money. But, they kept coming and were getting more and more

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

urgent. We started looking at the individual program budgets and trying to find out what parts of the budget were actually devoted to security of the systems and it turned out to be harder than we thought. Some programs rolled the money into IT as a whole; some had separate line numbers for these items; some had no reference to anything for security of information systems but included that in their budget for overall security, which included physical, administrative and personnel security matters. It was impossible to separate those relating only to security of computer systems.

By coincidence, the Army was due to present its budget for Information Assurance to the Department of Defense budget process which would vet it, combine it with all the Services and Agencies in DoD, and forward it up through the federal system. BMDO had to do the same thing, so all the agencies were together for a meeting where these briefings were given. When the Army representative gave his briefing, it included a number of broad security initiatives for all of the major Army networks and several for advanced programs. It sounded pretty good.

Because we were having such a difficult time with understanding how the Army allocated these funds to levels below the senior staff, I asked a couple of questions about how that was done. The responses were somewhat confusing, because they weren't pointing to a rollup of funds based on inputs from the field, as the other agencies did, and the Army person was getting flustered. I thought it might be easier for us to understand if we started from the top view and worked down, so I asked him how much of his program was funded as baseline. He said, "None of it." Several of us looked at each other to be sure that we had heard what we thought we heard. He confirmed it by adding that the entire Army program for Information Assurance was an "unfunded requirement" that was submitted as a part of the overall Army budget, but was not included in it for funding. As time went on through the year, the Army would get funds from various places and give them to the IA Office. Incredible as it sounds, the Army still does security of its computer systems the same way today.

We set out to find out where all the money we had been supplying through our budget was going. It was not easy. We matched up what we had given to the Army for missile defense and identified where there were requirements for security included in that funding. The total amount was about $250 million dollars a year. Then, we went to each of the agencies that were supposed to receive the money and figured out how much they actually got to do the work. It was less than half of the money we had given them. At least part of it had been reallocated to expand a military golf course in Atlanta. The rest of it was even harder to figure out and we never did determine where it had gone. The findings put us on a collision course with the Deputy Undersecretary of Defense for Acquisitions and the Army Chief of Staff.

We decided to try another approach. We were going to include the Army funding for cybersecurity (then called Information Assurance) in our budget and fund it directly to the people doing the work. No middleman. The Army did not like that idea and they thought we could never get this concept through the senior leadership in the Pentagon. Because we were taking a long view, we decided to collect our information and ask for the money in the following year's budget. That gave us about nine months before anyone would know what we were trying to do.

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

In the meantime, we started asking that every program include a separate line number in their budget for cybersecurity. This was so we could track these requests and total them. Most of them began to do that and the numbers rose considerably. They were still not exact, but they were into the $300 million range. BMDO was used to numbers like that, so nobody seemed excited by our totals. When the time finally came, we had a chance to present our budget for the next year and we included any Army system funded by BMDO, and we asked the Army to reduce their budget request by the same amount. Instead of a firestorm, we got a few interested glances but nothing more. Not one person objected.

At the next level up, the budget requests for cybersecurity get consolidated and presented as a total. I had never been to a meeting like this and had never been asked to brief such a big group. Most of the time our budget request was so small, it never made the "drop in the bucket" analogy. This time it did.

I got to the meeting early so I could get a seat near the Budget Director, at the far end of a long conference table and wait my turn. As they attendees started to show up, I was surprised to see so many stars on the shoulders of the people sitting with me. The fellow next to me was the Surgeon General of the Army and had 3 stars and the one who came with him did too, but I had no idea what he did. By the time they all came in, nobody except me had less than 3 stars. I was pretty sure I was at the wrong meeting. A person in civilian clothes came and sat at the head of the table at the other end and everyone quieted down.

As we went on, it was fairly obvious that they were waiting for something and I figured it was our briefing, but I was wrong. A young Colonel got up to brief the budget request of the Defense Information Systems Agency (DISA) and the General next to me turned to his partner and said, "OK, this is it." DISA was asking for 125 people, to be drawn from the other services in the Department of Defense to set up a group to do IA in all of the Defense Department. This confused me, when this was presented, because I had come from that organization ten years before, and had been part of a group of the same size that did the same thing. DISA broke it up and scattered it all over the organization, and now they were asking for another group of people to do the same thing. There were a lot of questions from the floor and I was afraid to say much until all these senior people got finished asking theirs. But I finally got and opportunity and raised my hand. "What happened to the 125 billets you had in the Center for Information Systems Security?" I asked him. Everyone knew, right at that moment, that he didn't have any idea about any such organization, let alone that it was in DISA. I had to explain the background of the question. The Chairman asked if the matter could be investigated further before consideration of DISA's budget was made, and the Colonel agreed and sat down. The General next to me turned to me and said, "Good job son. We sure didn't want to give up anymore people to those folks."

I was next and gave my briefing. Nobody seemed to care much about it, now that the real issue of the day had been resolved, but the Army representative said he objected to the duplication this could cause and he wanted to be sure we had coordinated this accurately with Army. The Army would agree to establish a separate budget request for IA for the systems missile defense funded, if BMDO would agree to arbitration of their request to

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

make sure there was no duplication of requests. We hadn't expected this, but we agreed that it sounded reasonable and we would finish our joint requests in two weeks.

The meetings with the Army office were exhaustive and we went back and forth on the numbers, right up to the deadline. The Army had agreed to a request for a sizeable sum, and we agreed to $7 million for our systems operated by Army. These numbers were fairly equal to what should have been requested in years past, so we agreed. We got the requests to be adjudicated and they were passed up the chain for inclusion in the higher-level budgets of both agencies.

We thought we had an agreement that would change the way Information Assurance was being done in the Defense Department, but we were not very familiar with the way the Pentagon actually worked. When the Army request got to the next level, it was withdrawn without ever being presented for funding, exactly the same way they had always done it. BMDO was directed to give the Army the $7 million we had requested for Army programs. Once it went to them, it could be used for another addition to that golf course, or anything else the Army wanted it for. It was a very expensive lesson for all of us. Though all the professionals agreed on what to be done, the people at the top of those chains do not necessarily believe that it is important and don't want to change.

The CNCI money is doing very much the same thing, in almost exactly the same way. It represents additional monies that have been added to agencies to do what they should have been doing all along, with the hope that they will act as "seed money" to establish programs in "baseline funding" i.e. those that are independently funded by the agencies. Only the agencies are not doing that. They take the money and, for as long as the programs last, they spend it, but they don't put it into their baselines and it ends when the funding stops. The Intelligence community is much like the Army or Department of Homeland Security, in that it decides how its budget is going to be spent and rates various programs in a stack. It looks down that stack and draws a line at the point where it believes the budgets will be funded. Anything falling below that budget line is not funded. So, often, the programs that are being funded by CNCI money were things that the government agencies could have done had they funded security of their own systems. Congress is not managing the programs well and the Joint Interagency Task Force set up to coordinate it has not been effective.

Congress has to do a better job of overseeing the money they spend for security of cyberspace, and put someone in charge that can execute those funds. By the time it gets into an agency, the purpose of it is lost and the federal agencies divert it, or throw it around like play money into project after project that does nothing for the protection of our networks. In the meantime, we have a new type of incident every week where someone from Estonia or some other little country is working with someone in Belarus to install the Zeus Trojan on our systems so they can get into financial accounts that are in our banking system.[9] It never stops.

---

[9] Bray, Chad/Cassel, Bryan-Low/Gorman, Siobham, *Accounts Raided in Global Bank Hack*, The Wall Street Journal, http://online.wsj.com/article/SB10001424052748704483004575523811617488380.html

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

© 2011 SANS Institute, Author retains full rights.

© 2011 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced