AMERICAN CHRONICLE

Wednesday, June 17, 2009 9:47:03 AM

A Call for Action in Addressing Cyber Security

June 17, 2009 *Ed Dickson*

President Obama has addressed the nation on the importance of securing cyberspace and the reasons why it could be a danger to both our economy and national security. He also has used the term, "weapons of mass disruption" and announced that he will appoint a cyber security czar.

The speech where he addressed this issue highlighted a **60-day study** conducted at his direction, designed to take a look at how vulnerable we are to cyber attacks that could drastically change the whole way we exist.

Is this a far cry from reality? Perhaps not; if you can take command and control of the computer that controls something we use, you can do pretty much anything you want with it. This might be anything from a banking system to the system that controls an electrical grid or a sophisticated weapon. If you really think about, computers control just about everything nowadays.

As I was considering this, it reminded me that there are already millions of computers where some hacker has gained command and control of and formed into a botnet (essentially a supercomputer). All it took to do this was a little social engineering to trick someone into downloading some malicious code on a machine. While some of us might write this off as stupid people doing stupid things, people have even been tricked into doing this at government agencies and Fortune 500 companies. Trust me, not all the people who fall for some of this stuff are stupid. Social engineering is known to cause people to do things they normally would not!

While it takes a little technical sophistication to write malicious code, a person doesn't necessarily have to be a technical whiz to get their hands on it. They can buy it right on the Internet, complete with a do-it-yourself (DIY) kit to execute their intended misdeed. While most of the "misdeeds" seen in the wild have a financial intent, the intent is dictated by the person committing the act. In other words, the intent might be different depending on the person who is executing the deed.

Also mentioned, both in the **report** and in the speech, was cyber-warfare. For years now, the **Chinese** have been accused of hacking into government systems, although they always deny it. Also mentioned was an actual use of cyber warfare, or the Russian attack on Georgia that happened in the not very distant past.

Please note that botnets, which I mentioned above, were used to **cripple** the Georgian infrastructure. The zombie computers used in these botnets didn't come out of Russia, either. Some of them were traced right back to this country. In the current environment, you don't need to be in a physical location to take command and control; it might happen from anywhere.

The report also mentions attacking electrical grids and that the CIA has intelligence that this has already occurred in other countries. Just last month, the Wall Street Journal issued an **article** stating that Russian and Chinese hackers had mapped the U.S. power grid and left behind software that in theory could be used to attack our electrical grid. The article quoted unnamed officials from within the government. This set off a flurry of articles and in the end, most of the **experts** concluded that the threat, although real, wasn´t as bad as it was hyped up to be. Nonetheless, hacking certain utilities, such as electricity, water, and sewage could cause a lot of serious problems and there is evidence it has been accomplished in other countries.

While cyber warfare is an ominous subject, the report points out that we have already seen some pretty major events when financial systems were successfully attacked. Examples given were the TJX data breach (45 million payment cards compromised) and the more recent WorldPay payment card breach where a 30 minute exploit netted nine million dollars. This **highly coordinated scheme** took place all over the United States, Montreal, Moscow, and Hong Kong in a very short time-frame.

There is tangible evidence that so much personal and financial information has been stolen that the laws of supply and demand are driving prices down. Interestingly enough, a lot of this information is traded right over the Internet in anonymous forums using hard to trace forms of payment.

Two recent reports point to this. Symantec released a pretty interesting **report** on the underground economy and shortly afterwards, Verizon issued another report on the state of personal and financial information being stolen. The Verizon **report**, pointed out that the 285 million "known" records stolen in 2008 amounted to more than what was recorded in the previous three years. The Symantec report, which breaks down the going prices for information noted that the practice of spoofing (impersonating) financial institutions to steal information grew from 10 percent in 2007 to 29 percent in 2008. The Symantec report stated that 90 percent of the attacks being launched via botnets were designed to steal information and that the number of infected computers had grown 31 percent in 2008 over 2007, also.

Also cited in the report and in the speech was an estimated $1 trillion dollar loss per year in intellectual property. In recent years, the FBI has been busy catching **numerous people** stealing technology secrets and exporting them out of the country. This brings up another variable in the problem or if a person is given access to a system it is relatively easy to compromise it.

Recently, it was even disclosed that computers in Congress were **hacked**. It appears that even government intellectual property is being targeted.

When it comes to intellectual property theft, often we do not know what the motive is. Again, the intent is largely dictated by the end user. If you wanted to see a real world example, you might take a look at software piracy. The Business Software Alliance puts **worldwide losses** at over $50 billion, yearly. If you were to look at counterfeiting in general – which can involve the theft of intellectual property – the International Anticounterfeiting Coalition estimates the losses at **$200 to $250 billion** just in the U.S., every year.

The report, which is posted on **WhiteHouse.gov**, also addresses the growing problem of privacy in the digital world. Personal and financial information is worth a lot of money to businesses and criminals alike. Unfortunately, because of this, a lot of people are leery of putting in controls that might make it harder to profit from information. Because of this, a lot of people´s personal and financial information has gone missing.

The American Library Association, the Cato Institute, the Center for Democracy and Technology, Carnegie Mellon University, Consumer Action, the Center on National Security Studies, Cornell University, the Electronic Frontier Foundation, the Electronic Privacy Information Center, George Washington University, Harvard University, Indiana University, Johns Hopkins University, OMB Watch, Ohio State University, the National Security Archive, the University of California-San Diego and the American Civil Liberties Union were all consulted in the initial 60-day report.

While the report isn't clear on how privacy will be dealt with, it nonetheless is calling out that a problem exists. The problem is too much information being stored in too many not very well secured places.

For a real example here, one could refer to the **DATALOSSdb Open Security Foundation**, which tries to document all the known data breaches. The problem is getting worse all the time, and although some might argue that greater transparency is the reason for this, there are probably many more unknown data breaches that occur out there. After all, it´s unlikely that the hackers or other criminals stealing the information are going to come right out and tell us where they are getting it from. From a business perspective, it isn´t in their best interests.

The real casualties in this part of it are the individual victims, who suffer a lot when their information is used after it stolen. With the sheer amount of victims out there, some could argue we are facing an identity crisis.

To add to the problem, technology is now also being used to produce high-quality counterfeit documents and financial instruments in places, such as garages. This makes the information being stolen all the more dangerous, or easy to abuse.

Another thing the report addresses is the need for education and that laws need to catch up to the technology we are using. An interesting section at the end of the report highlights the history of modern communication technology. There is little doubt that as technology grows at a rapid pace; it is hard for the legal community to keep up with it.

In the end, in my humble opinion, the study is the first step in a positive direction. We have already seen too many examples of the abuse of technology, which has a lot of potential for good, too! The problem is how to deal with those

who abuse it. The good news is that a large part of solution can be achieved by using a little more common sense and the clean slate approach (mentioned in the report) will go a long way towards making this a viable effort. In the end, a responsible balance is the key, and this is what it seems the report seems to be calling for.