WHITE PAPER

Government Policy + National Cyber Security

March 2

2013

This white paper presented by SDV INTERNATIONAL helps readers understand the importance appropriate U.S. cybersecurity policy to protect our industries and provide national security in response to advanced persistent cyber threats. It is important that American governmental and industrial information systems be protected with a high level of assurance through sound security measures, practices, procedures, and enterprise architecture policies.

.:. SDV INTERNATIONAL, LLC .:.
.:. Phone: (202) 455-6554 .:.
.:. Email: info@SDVInternational.com .:.
.:. Website: www.SDVInternational.com .:.

INTRODUCTION

It is critical that the United States sets appropriate cybersecurity policy to protect our industries and provide national security. The U.S. is facing a wide range of advanced persistent threats from adversaries with sophisticated expertise and extensive resources, and which utilize a multitude of attack vectors. It is important that American governmental and industrial information systems be protected with a high level of assurance through sound security measures, practices, procedures, and enterprise architecture policies.

Modern society, especially the U.S., has become more dependent on information systems than ever before. Critical infrastructure, including water treatment facilities, the power grid, municipal damns, natural gas lines, and air traffic control systems all depend on information systems that require appropriate cybersecurity. Critical infrastructure attacks have already occurred abroad, such as in the case of the Saudi Arabian power company, Aramco. Aramco's many computers were infected with a virus that erased data and left users with a screen displaying an image of a burning American flag (Perlroth, 2012). Unfortunately, cybercrime and cyber terrorism is proliferating as more sophisticated tools become available to malicious actors. Ironically, the sophisticated tools are becoming easier to use, by offering graphical user interfaces and simple tools that enable hackers to learn to become capable of being destructive, more quickly than ever before.

America is extremely dependent upon the well being of cyberspace. Cyber attacks are occurring at level never seen before, as this report explains, and it is critical that we maintain, protect, and defend the use of cyberspace from threat sources.

GOVERNMENT INFLUENCE ON CYBERSECURITY POLICY

Because a strong functioning American government requires stable critical infrastructure, it is important that government policy addresses cybersecurity. Cybersecurity policy is a formal high-level plan that embraces general goals, objectives, and acceptable procedures related to cybersecurity (Guel, 2007). Cybersecurity policymakers may choose from a variety of frameworks when crafting cybersecurity policy. For example some organizations might prefer to utilize the International Information Systems Security Certification Consortium's (ISC^2) Certified Information Systems Security Professional (CISSP) information security framework, which includes ten (10) domains in which policy can be addressed. Other organizations, such as the U.S. government, utilize policy set forth by the Secretary of Commerce, following the guidance from the National Institute of Standards and Technology (NIST), which is thoroughly described in its publications. Yet other organizations may choose an International Standards Organization (ISO) framework through which policy is crafted. Ultimately, an organization's cybersecurity policy framework should be selected based on what works best for each organization, the organization's culture, the organizations regulatory requirements, the organizations mission, and the resources it has available (Guel, 2007).

Legislative efforts have expanded significantly in recent years. When requesting an increased budget for cybersecurity programs at the Department of Homeland Security in 2012, Secretary Janet Napolitano found the Congress was willing to strongly support increases in the DHS budget for cybersecurity, with an increase of $325 million to a total of $770 million in 2013 (Jackson, 2012). There are a myriad of policy efforts in the U.S., some of which have had fits and starts in the Congress; such as the Cyber Security Enhancement Act, the Cyber Security Act of 2012, the Health Information Technology for Economic and Clinical Health Act (HITECH), and others (Armerding, 2012). In addition, President Obama is focusing on cybersecurity and computer crime. In a recent memorandum, the president has emphasized the nation's need for

new cybersecurity policy and enforcement guidelines that meet new challenges posed by new threat sources (Wayne, 2012).

Current Government Guidance to Industry

The U.S. government has created policy that helps it defend against malicious actors and protect national security through a variety of measures, including but not limited to: the E-Government Act of 2002, which includes the Federal Information Security Management Act (FISMA); the Computer Fraud and Abuse Act (CFAA), and; the Foreign Intelligence Surveillance Act (FISA).

FISMA has received the most attention, as it has required the U.S. government to develop standards and guidelines, which are provided by the National Institute of Standards and Technology (NIST), in coordination with the Office of the Director of National Intelligence, the Committee on National Security Systems, and the Department of Defense, to establish a common framework for information security across the federal government (NIST, 2011).

To help standardize government information security practices, NIST has provided a series of special publications that cover a wide range of guidelines, standards, and even step-by-step processes for government and industrial stakeholders to follow. Beginning with *An Introduction to Computer Security: The NIST Handbook*, and up to the *Draft Guidelines on Hardware Rooted Security and Mobile Devices*, NIST has been providing such publications to the American government and industrial stakeholders since 1995 (NIST, 2013). While U.S. government agencies are required to follow the NIST guidelines and standards, heretofore not all industrial stakeholders have been required to do the same.

Analyzing Consequences of Government Intervention – Federal and State Government Examples

As in the analysis of other government regulations, there are stakeholders who believe that government cybersecurity policy ought to be mandated, and there are those who believe that the government should not interfere with industrial or private cyber practices.

Civil liberties are one area of concern for opponents of enhanced government cybersecurity policy. For example, some are concerned that civil liberties may be violated by government policy that might allow the government or other stakeholders to monitor the activities of citizens of the United States.

At the federal level, some criticize the Patriot Act as an example of how the federal government overstepped its role when it was authorized to monitor American citizens who are suspected of being involved in terrorist activities (Gorham-Oscilowski, 2013). At the state level, some argue that the California government overstepped its bounds when the City of San Francisco shut down cellular phone service in its subway stations to prevent citizens from communicating about a planned protest (Smith, 2011). As another example of state-level cybersecurity policy concern that dates back to 2004, New York Governor Pataki aggressively sought to enhance New York State Law to provide 750,000 state and local law enforcement officials with the same level of cyber investigatory authority leveraged by their federal counterparts (Albanesius, 2004).

The application of cybercrime laws vary from state to state. For example, the Computer Fraud & Abuse Act (CFAA) is interpreted differently in different circuit courts. In the case of *United States versus Nosal*, as described in the Florida Bar's Journal article, *Federal Computer Fraud and Abuse Act: Employee Hacking Legal in California and Virginia, But Illegal in Miami, Dallas, Chicago and Boston*, some states considered the defendant's use of his former employer's

customer data as a cybercrime under CFAA, while other courts did not because they did not view his collection of the information as a computer "hack" because he exercised rightful use of the information at the time he collected it, even if he improperly used it later, thereby violating other laws (Kain, 2013).

Unintended consequences of federal and state policy may occur. For example, some argue that the Patriot Act, which was intended to allow the Federal Bureau of Investigation (FBI) to build cases on terrorism suspects by using National Security Letters (NSL) to seek consumer information from industry to analyze suspect behavior patterns, went too far and ultimately violated the First and Fourth Amendments of the U.S. Constitution by reaching into the communications and financial lives of ordinary Americans (Gorham-Oscilowski, 2013).

Another example of unintended consequences, related to military applications of cyber weapons, is in the use of autonomous weapons, where there is the risk of impacting unintended targets (e.g., American federal and state government information systems) (Leithauser, 2012). Further, in his recent Executive Order, President Obama emphasized a need for government to communicate more of its sensitive information with industrial stakeholders (Obama, 2013). A possible unintended consequence of sharing too much information with industrial stakeholders, who have not been cleared by the U.S. government as being loyal to American interests, could be the leakage of sensitive government information to U.S. adversaries. Another unintended consequence might come in a shift of responsibility for comprehensive background investigations from government authorities to the private sector; a change that could lead to many new vulnerabilities.

Some say any degree of government intervention in cyber freedom violates American civil liberties, while others find civil liberty concerns to be overstated and unrealistic because of the sheer volume of information that exists in cyber space, and the fact that the government has enough *real* threats on which to focus, and no directive to monitor law abiding Americans.

Americans have seen government regulations in many other areas of their lives. Consider gun laws, tax laws, drug and alcohol laws, carbon emissions laws, Sarbanes-Oxley compliance regulations, Generally Accepted Accounting Principles (GAAP) guidelines, and many other government regulations that affect the way industry does business, and the way Americans live. The bottom line is that the U.S. must have a secure critical infrastructure, and much of that critical infrastructure is supplied and maintained by the private sector. Therefore, it is incumbent upon the government to enforce some degree of cybersecurity policy compliance in industry. More policy will unfold in the coming years, and the degree to which industry will be required to comply is yet to be seen.

GOVERNMENT POLICY & ITS IMPACT ON NATIONAL SECURITY

The government's purpose is to go about setting regulations that foster opportunities for Americans, and to provide national security. In its determination of regulatory requirements, the U.S. considers cybercrime and cyber terrorism important factors. The U.S. regulatory system, including many efforts led by the Department of Justice, is focusing on creating new law enforcement guidelines to meet new challenges for national security (Wayne, 2011).

It is important to understand the threats that exist in cyberspace. Cybercrime is not unique to this decade. Consider that the Department of Justice arrested more than 150 people in an organized law enforcement program in 2004, where criminals were charged with a variety of cybercrimes, including identity theft, fraud, and other intellectual property crimes (O'Rourke, 2004). What makes things different in this decade is that now relatively novice hackers can use tools to cause significant damage to information systems, thereby exponentially amplifying the potential of new threat sources around the globe.

It is important that our legal system applies proper punishments to cyber criminals who are apprehended and convicted. Examples of previous cybercrime sentences include: two-and-a-half (2.5) years of imprisonment for breaking into the computer systems of businesses to obtain copies of legal documents, financial information and other types of information; three (3) years of imprisonment for gaining unauthorized access to a government banking system and transferring money to a personal account (Shultz, 2005). Many cybersecurity professionals have read the stories of Kevin Mitnick, the phone phreaker (i.e. phone system hacker) and computer hacker who was convicted of more than twenty-five (25) crimes, although arguably without significantly hurting his targets, and served five (5) years in prison (Mills, 2012). Hector Monseguer, one of the arrested LulzSec hackers, may serve over one hundred (100) years for his cybercrimes, despite working as an informant for the Federal Bureau of Investigation (FBI) before he was effectively taken off line (Mills, 2012).

Matters of cybercrime become more challenging when dealing with transnational issues, such as extradition treaties and multilateral agreements. In the case of LulzSec, one of its ring leaders who worked with Monseguer was arrested by English police in the remote Shetland Islands. In the case of Julian Assange, the WikiLeaks founder who disclosed classified military information (e.g., U.S. diplomatic cables, U.S. military operations documents) to the public, he has been taking asylum in an Ecuadorian embassy in London since June of 2012. Once he leaves the embassy, the British government plans to extradite Assange to Sweden where he faces sexual assault charges, and he may subsequently be extradited to the United States to face espionage charges (Bruner, 2012).

Cyber terrorism and asymmetric attacks could lead to more devastating consequences than the U.S. has seen in the past. Cyber terrorists may attack critical infrastructure from an unknown location, anywhere in the world, and disappear through obfuscated dark web back alleys without leaving a trace (Jaeger, 2006).

When nongovernmental organizations are victims of attacks, the Department of Justice is available to provide forensic and legal assistance, in some cases, when the appropriate stakeholders are operating in America. However, with consideration of the enormous volume of hacking cases every day, as well as the relative shortage of available cybersecurity experts, it is unlikely that the justice department can help everyone; therefore, it is incumbent upon industry and the general population to learn how to follow sound guidelines and standards that the government provides to the public, through programs such as the *Stop. Think. Connect.* campaign that is featured as part of the Department of Homeland Security-sponsored National Cyber Security Awareness Month (NCSAM) (Daniel, 2012).

When Industry Does Not Comply with Government-Recommended Cybersecurity Guidelines and Standards

Advanced persistent threats are continually pillaging industrial information systems. Intellectual property is leaving America faster than ever before (Forman, 2012). If industry does not apply adequate cybersecurity in its ecosystem, America faces both short-term and long-term threats that may be strategically devastating to U.S. interests.

Apple, Inc., for example, publicly announced that it was the victim of a cyber attack after claiming for many years that it was not as vulnerable as other computing systems (Lessin, 2013). As professionals who work in this field understand, many organizations do not publicly report when they have been hacked, for many reasons, including public reports which may cause hacker organizations (i.e. Anonymous) to jump on the proverbial bandwagon and increase the number of attacks. Therefore, this announcement by Apple, Inc. is significant and indicates the company's noteworthy concerns.

Although consumer products companies with significant market share are important, critical infrastructure owners and operators are currently a primary concern for the U.S. government.

In his recent Executive Order that focuses on proving critical infrastructure cybersecurity, President Barack Obama has asked that the Director of National Intelligence, the Secretary of the Department of Homeland Security, and the Attorney General to issue instructions consistent with their authorities that identify, in unclassified reports, information about threat sources that are targeting specific U.S. entities (Obama, 2013). The president has also asked that agencies to coordinate with industries in their sector, to encourage future voluntary industrial critical infrastructure cybersecurity program participation (Obama, 2013).

When Industry Meets Only Minimum Government-Recommended Cybersecurity Guidelines and Standards

When industrial stakeholders meet only the minimum requirements set forth in government guidelines and standards, they may be vulnerable to evolving threats; many of which adapt every day. Cyber laws, standards, and guidelines cannot maintain the same evolutionary pace that technical innovation keeps; a comparison of months or years versus days or hours. Meeting only minimum guidelines and standards, while good, might only be as good as meeting *yesterday's* threats.

How Industry Benefits by Exceeding Minimum Government-Recommended Cybersecurity Guidelines and Standards

Industry has an opportunity to benefit by exceeding the minimum requirements set forth by the U.S. government cybersecurity guidelines and standards. The U.S. government has made it easier in recent years for organizations determined to maximize cybersecurity protection by providing extensive publications under FISMA. Private sector stakeholders can evaluate and apply a wide range of NIST publications in a manner that is appropriate to their organizations. When the private sector applies an organized and methodical approach to providing cybersecurity, it has a better chance of defending against cyber threats. For example, as an

enhancement to its Publication 800 – 37, NIST has provided industry with special publication 800 – 137, which provides guidelines and standards for Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (NIST, 2011). These guidelines and standards are readily available for industry to adopt and utilize.

Those companies with the best chance of defending against cyber threat streams are those which consistently monitor and adapt to advanced persistent threats. This typically means having internal or external resources that focus solely on cybersecurity. With successful cybersecurity defenses, industrial stakeholders can realize benefits that are critical to their survival, such as the protection of trade secrets.

Conclusion

The U.S. government plays a very important role in protecting American interests. As U.S. legislators and government executives realize, it is very important that they develop policy that is good for industry, good for government, and therefore ultimately good for the prospects of America. It is incumbent upon both industry and government stakeholders with responsibility for maintaining secure cyber space to do everything possible to preserve the very infrastructure on which our civilization now depends.

Sources

Albanesius, C. (2004) N.Y Seeks Enhanced Security. *Congress Daily AM, P.19.*

Armerding, T. (2012) Demise of Cybersecurity Bill Means Executive Order on the Way. *CSO Online.* Retrieved from www.csoonline.com

Bruner, E. (2012) Ecuador Grants WikiLeaks Founder Julian Assange Political Asylum. *ABC News.* Retrieved from www.abcnews.com

Daniel, M. (2012) Blog Post: Staying Safe Online. Retrieved from www.whitehouse.gov.

Forman, G. (February 21, 2013) U.S. Ups Ante for Spying on Firms. *Wall Street Journal, Vol. CCLXI No. 42.*

Gorham-Oscilowski, U., & Jaeger, P. (2013) National Security Letters, the USA Patriot Act, and the Constitution: The tensions between national security and Civil Rights. *Government Information Quarterly, 25625-644. doi:10.1016/j.gig.2008.02.001*

Guel, M. (2007) A Short Primer for Developing Security Policy. *The SANS Institute.* Retrieved from www.sans.org.

Jaeger, C. (2006) Cyberterrorism and Information Security. *Handbook of Information Security.* Hoboken, NJ: John Wiley & Sons.

Leithauser, T. (2012) DoD: 'AUTONOMOUS' WEAPONS NEED PROTECTION FROM CYBER ATTACKERS. *Cybersecurity Policy Report, 1.*

Kain, R. (2013) Federal Computer Fraud and Abuse Act: Employee Hacking Legal in California and Virginia, But Illegal in Miami, Dallas, Chicago and Boston. *Florida Bar Journal. 87(1), 36-39.*

Lessin, J. (February 20, 2013) Apple Gets Hit by Hackers. *Wall Street Journal, Vol. CCLXI No. 42, Marketplace Section, B1.*

Mills, E. (2012) Crime and punishment: Harsh fate for accused LulzSec hackers? CNET News. Retrieved from www.cnet.com

NIST. (2011) Information Security Continuous Monitoring (ISCM) for Federal Information Systems and organizations. *NIST Special Publication 800-137.* Retrieved from www.NIST.gov

NIST. (2011) Guide for Conducting Risk Assessments. *NIST Special Publication 800-30, Revision 1.* Retrieved from www.NIST.gov

NIST. (2013) Special Publications (SP) – (800 Series). National Institute of Standards and Technology (NIST). Retrieved from www.nist.gov

Obama, B. (2013) Executive Order -- Improving Critical Infrastructure Cybersecurity. Retrieved from www.whitehouse.gov

O'Rourke, M. (2004) Operation Web Snare. *Risk Management, 51(11), 8.*

Perlroth, N. (2012, October 24) Cyberattack on Saudi Firm Disquiets U.S. *New York Times*. p. 1.

Schultz, E. (2005). Update in the war against cybercrime. Computers & Security, 24(1), 2-3.

Smith, J. (2011) Taming and Reining in Cyberspace. *National Journal, 1.*