Cyber security: threats, response and improvement

Technology

Cyberspace, or the Internet as an interchangeable reference, is the electronic medium of computer networks and systems in which onlinecommunicationand enterprise takes place. Originally, the Internet served to interconnect laboratories engaged in government research. However, since 1994, the decentralized Internet has expanded to serve millions of users and a multitude of purposes in all parts of the world. With this shift from government tool to general tool, the Internet has become a collective result of ideas, beliefs and initiatives.

Many aspects of our day-to-day lives can be traced along the Internet through some form of electronic function. In addition to its wide reaching powers with regards to the spread of information, the Internet has also become the most democratic and universal form of mass media ever known, since no one entity has a monopoly over the information available, thus making control close to impossible. Clearly, Internet usage in today’s world is no longer viewed as a nonessential luxury. Usage and content has exponentially risen to a level of unprecedented proportion that requires its own area of precautions and supervision.

The distal range of context that Cyberspace commands is the basis for a host of security issues and challenges that anyone that utilizes the Internet is made aware of daily. There is a growing awareness in today’s globalized world of the imminent dangers that may befell anyone that isn’t careful of their Internet usage. Cybercrimes such as theft, fraud and identify theft, to name a few, pose as ominous threats to the security of any individual or enterprise that engages the Internet at any given time.

Read thisChapter 2 – Why Security is Needed

Not only are these threats that individuals are subjected to, but also threats that the US government has been forced to acknowledge as it becomes increasingly dependent on the internet as a way of life. Based on the combination of the new widespread use of the internet, as well as governments and world’s dependence on the internet for daily life, cyber security has become the new face to American foreign policy, national security, military and defense strategies and economic stability.

As President Obama explained, the growing number of attacks on our cyber networks has become “ one of the most serious economic and national security threats our nation faces. ” This increased threat explains the increase in the cyber security field, task force work, watchdog groups and government agencies over the past decade. “ Cyber security,” as the field has been coined, is varied and ranges from the local, state and federal levels, all with the purpose of regulating and policing the ill effects of Cyberspace usage.

Responding to Threats. The increase of security threats has forced the United States government to meet these new challenges and implement strategies towards the safeguarding and integrity of its critical infrastructures, as well as against an extensive gamut of state and non-state actors that do not adhere to physical borders. The United States government is responsible for the supervisory control and data acquisitions (SCADA) of the entire nation. SCADA has seen a growing dependence of critical

infrastructures and industrial automation on interconnected physical and cyber based control systems.

There has been a growing and previously unforeseen cyber security threat to these systems, which include industrial control systems, computer systems that monitor and control industrial, infrastructure, or facility-based processes. These critical infrastructures include areas such as water treatment and distribution plants, wastewater collection and treatment plants, oil and gas pipelines, electrical power transmission and distribution generators, wind farms, civil defense siren systems and large communication systems.

Although most critical infrastructures are in the private sector, governments at various levels perform many key functions with regard to these infrastructures. Among those key functions are national defense, homeland security, emergency response, taxation, remittances to citizens, central bank activities, criminal justice, and publichealth. These functions and others now depend upon information networks and systems. Thus, it is the duty of the government by law to secure their information systems in order to provide essential services that is critical to the continuity of government. Government’s role in cyber security is warranted in cases where high transaction costs or legal barriers lead to significant coordination problems; cases in which governments operate in the absence of private sector forces; resolution of incentive problems that lead to under provisioning of critical shared resources; and raising awareness. ” 7 Policy Review Current cyber security policy has been adjusted to reflect the clear and present danger

associated with cyber warfare. The Obama Administration has identified several areas in which cyber security will be greatly impacted.

Its near term strategy, which in effect is the Administration’s immediate focus, is the most vigorous strategy, and includes the listing and identification of the designation of a cyber security directorate, establishes cyber security as a management priority, proposes a cyber security action plan that develops a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure.

The strategy also strives to provide the research community access to event data to facilitate developing tools, testing theories, and identifying workable solutions. 7 Cyber security and its safeguarding of critical infrastructure as we know it today came to pass The Homeland Security Act of 2002 (P. L. 107-296), which transferred and integrated several federal entities that play a role in cyber-security of control systems into the Department of Homeland Security.

These entities include the Critical Infrastructure Assurance Office, the National Infrastructure Protection Center, the National Infrastructure Simulation and Analysis Center, and parts of the Department of Energy’s Office of Energy Assurance. Additionally, the Homeland Security Act of 2002 created a new class of information, critical infrastructure information, which can be withheld from the public by the federal government.

In spite of the clandestine measures in place to ensure the integrity of privileged information, the cornerstone of America’s cyberspace security strategy is and will remain a public-private partnership. The government, working with key stakeholders, should design an effective mechanism to achieve a true common operating picture that integrates information from the government and the private sector and serves as the basis for informed and prioritized vulnerability mitigation efforts and incident response decisions.

From a federal government perspective, the proper and most efficient approach to ensuring the safety and integrity of its cyber security is through rigorous and cost-effective risk assessments. Industry Initiatives Since the field of cyber-security is a relatively new one, it will continue to experience its share of technical difficulties along the way. Initiatives that address the vulnerability of industrial control systems may be reduced and enhanced in a ‘ less is more’ approach through a range of federal actions.

Development standards by either a voluntary or mandatory process for cyber-security of control systems; identifying and addressing critical infrastructure interdependencies; developing encryption methods for control systems; identifying and establishing technologies to address existing vulnerabilities; funding long-term research into secure SCADA systems; providing for free exchange of risk information between the federal government, private industry, and other critical infrastructure sectors; and assessing federal activities in this area are all possibilities for negotiation.

Due to the severity of importance surrounding SCADA systems, federal actions may also create a more uniform process that would include “ the functionality necessary to protect industrial control systems, while providing for more secure operation. ” Preparedness and Resources America’s increasing dependence on informationtechnologyhas given way towards a greater protection of digital networks and infrastructures, however confidence in its current form is as delicate as ever despite renewed calls for better understanding, awareness and preparedness of critical infrastructures. “ Confidence in preparedness is variable.

Nearly a third of IT executives surveyed said their own sector was either “ not at all prepared” or “ not very prepared” to deal with attacks or infiltration by high-level adversaries. Among those who had actually experience such attacks, the lack of confidence rises to 41 percent. ” It is a generally held view by the cyber security community that the resources in place to secure networks are in adequate measure to respond to at-large threats. Overall, cost was most frequently cited as “ the biggest obstacle to ensuring the security of critical networks,” followed by “ lack of awareness of the extent of the risk. Such a daunting task of safeguarding these important resources can only be handled at the federal level, particularly in the military’s domain, yet even the federal government isn’t impervious to data breaches, nor is the military. The man currently responsible for overseeing US cyber security strategy is Deputy Defense Secretary of Defense William J. Lynn of US Cyber Command (USCYBERCOM).

Secretary Lynn cites the biggest threat to American cyberspace stems from the “ exploitation, disruption and destruction of our networks. In 2008, the

US was the victim of a cyber attack that penetrated top-secret classified files. The breach occurred when a foreign intelligence agent used a malicious flash drive to steal information from laptops in Iraq and Afghanistan. Lynn cites this unprecedented event as “ the most significant breach of U. S. military computers ever. ” 13 More recently in May of 2010, the US Secret Internet Protocol Router Network (SIPRNet) was breached by PFC Bradley Manning, which led to the highly publicized Wiki Leaks controversy.

USCYBERCOM will play the leading role in helping to integrate cyber operations into operational and contingency planning as outlined by the 2010 Cyberspace Policy Review and the Quadrennial Defense Review (QDR). According to the Cyberspace Policy Review, “[t] he nation’s approach to cyber security over the past 15 years has failed to keep pace with the threat. ” The QDR acknowledges that: There is no exaggerating our dependence on DoD’s information networks for command and control of our forces, the intelligence and logistics on which they depend, and the weapons technologies we develop and field.

In the 21st century, modern armed forces simply cannot conduct high-tempo, effective operations without resilient, reliable information and communication networks and assured access to cyberspace. It is therefore not surprising that DoD’s information networks have become targets for adversaries who seek to blunt U. S. military operations. Indeed, these networks are infiltrated daily by a myriad of sources, ranging from small groups of individuals to some of the largest countries in the world. The reality facing governments and private enterprise today with relation to yber attacks is to maintain a steadfast and cautious plan whose efficacy enables

them to respond to the incessant attacks by hostile governments and non-state actors alike.

Undoubtedly, these measures are costly, but a solid investment in the safeguarding of critical infrastructure and data. The alternative lies in damage control once an attack has been initiated, which when compared to an attack, is exponentially less than the warranted protection in aggregate. The average estimated cost of 24 hours of down time from a major cyber attack was U. S. $6. 3 million in 2010. 6 According to a study prepared by the Poneman Institute, a research center dedicated to privacy, data protection and information security policy, the smaller the gap between compliance and non-compliance costs, the lower the occurrence of compromised records for an organization. 17 According to Undersecretary of Defense Lynn, “ cyber attacks on our military networks have not cost any lives, not yet. But in a six month period, the Defense Department spent more than $100 million defending its networks ... and we spend billions annually in a proactive effort to defend our networks. ” 18 Future Action Plans

The interdependence of cyberspace means system networks are heavily dependent on varying infrastructures in order to function at optimum capacity. The US Department of Defense has acknowledged that in order to meet the demands of today’s cyber security threats, they must collaborate with private enterprise in order to coordinate responses to cyber attacks. The Cyber Policy Review states that, “ implementation of this framework will require developing reporting thresholds, adaptable response and recovery plans, and the necessary coordination, information sharing, and incident reporting mechanisms needed for those plans to succeed.

Moreover, the QDR supports the Cyber Policy Review by stating that, “ this mutual assistance includes information sharing, support for law enforcement, defense support to civil authorities, and homeland defense. In particular, DoD will strengthen its cooperation with DHS, which leads the national effort to protect federal information systems. ” 19 Collaborative Effort and Hierarchy While cyber security is currently evolving and become a growing trend in the digital age with relation to national, military and economic security, overnment-sponsored cyber security cooperation varies widely among owners and operators of critical infrastructure in their respective arenas. 20 The advent ofglobalizationhas spawned a new age of interdependence and the integration of markets, nation-states and technologies. 21 While there is no question as to the federal government’sresponsibilityin pooling its resources together for its own security, the question remains insofar as to how the US’ allies and partners will collaborate in areas of mutual interest with relation to cyber security.

As with any other venture that requires circumspection, the tendency for information sharing not only at the federal level, but international level as well may very well be a one-way street; from bottom, up. While U. S. cyber security policy aims at having a partnership with private enterprise, resistance from the private sector arises from an impending gamut of legislation and regulation. Three areas in particular are a concern for IT professionals: * Lack of faith in the understanding officials have about the way a sector works. Clumsy regulation may “ level-down” security in very diverse sectors. * The risk that mandatory disclosure of security incidents—for example the compromise of personal data—can drive policy and

resources in counter-productive directions. 22 These concerns are well founded and derive from the legislative branch’s inability to often time analyze, understand and process information in a timely fashion. Improving Cyber Space It will remain an arduous task for anyone and everyone who utilizes cyberspace as a medium for information and data sharing to maintain a relative form of security comfort.

Cyberspace in its current form is unregulated by most countries around the world. China is an exception; due to their system of government, the Chinese see it as a strategic interest to hide certain areas of public internet usage. While there are steps in place to promote a healthy relationship in cyberspace from the government on down to private individuals, cyberspace and its capabilities are its infancy in terms of technology, systems and infrastructure. The ceiling is limitless with relation to advancements in all three of these phases.

In the short-term, information placed in cyberspace must be carefully weighed for its content value and varying degree of sensitivity. There is a growing demand and shift towards internet usage that has secured access. For example, most websites that handle financial transactions and safeguard personal information have moved towards the “ https://” coding for secure connectivity. Firewalls are an important component as well in handling any would-be hacker or virus from penetrating encrypted data.

Such measures are an important step towards maintaining a harmonized cyberspace. The need and demand for privacy is another area of interest in maintaining a safeenvironmentwithin cyberspace. There’s a profound

difference between the location of a terrorist cell on a network server in the Pentagon and an individual’s latest update on asocial mediasite. While both are important for differing reasons, privacy and security are of the utmost importance to maintaining the Internet and its users as safe as possible.

Many cyber vulnerabilities exist because of a lack of cyber security awareness on the part of computer users, systems administrators, and technology developers, Such awareness-based vulnerabilities present serious risks to critical infrastructures. 23 Safety and improvements to cyberspace is everyone’s responsibility. With no single governing body in charge of securing and improving cyberspace, it becomes increasingly more important for all users to heed the caveat lectors of their own due diligence and to point out potential trouble areas and vulnerabilities.