International Journal of Advance Research in Science and Engineering
Vol. No.4, Special Issue (01), November 2015
www.ijarse.com
IJARSE
ISSN 2319 - 8354

EXPLORATION OF CYBER SECURITY AWARENESS AND ITS SERIOUS IMPLICATIONS

Mrs. Jyoti Nawade [1], Dr. Balaji D [2], Mr. Pravin Nawade [3]

[1] *Lecturer, JSPM'S Bhivrabai Sawant Polytechnic, Pune (India)*

[2]*Assistant Professor,* [3]*Assistant Administrative Officer, SIBM-H, Hyderabad (India)*

ABSTRACT

Cyber criminals are primarily targeting the human aspect of security since end users are soft targets to manipulate. The use of internet has made people and organizations helpless from the outside attacks, Cyber issues mainly affect information systems with different types of nasty attacks such as spyware, virus and social engineering etc. Currently Social Networking sites are more popular medium of interaction and communication with users. These sites provide the ability to run applications to users' knowledge. The popularity of social networks makes it an ideal tool through which awareness can be created on existing and emerging security threats. Information of Cyber Security is still severe challenge to spoil the threats due to lack of control on security breaches and awareness in the society. Risk is formally defined as "the effect of uncertainty on objectives". Risk is often characterized by a probabilistic analysis involving both the likelihood of potential events and their consequences on the organizational objectives. The economy, the infrastructure, the safety and the security of the United States, as well as much of the rest of the world, depend upon the Internet for the transfer of electronic data. The threats and risks are real and increasingly frequent, with high potential to critical energy infrastructures.

Keywords: Cyber Security, Social Networking, Internet, Organizational Objectives.

I. INTRODUCTION

Day by day we are losing our battle against Cyber security. We are heavily depends upon technology as the main defense, instead of recognizing that the easiest attack vectors are the people who operate the various software and application in current decades. The ordinary users do not understand the decisions they make each and every day have security implications for themselves and to their projects and companies. Network outages, data compromised by hackers, computer viruses and other incidents affect our lives in ways that range from inconvenient to life-threatening. As the number of mobile users, digital applications and data networks increase, so do the opportunities for development. Cyber criminals are primarily targeting the human aspect of security since end users are soft targets to manipulate. The use of internet has made people and organizations helpless from the outside attacks, Cyber issues mainly affect information systems with different types of nasty attacks such as spyware, virus and social engineering etc. since these people are primary target, education is one of the reliable weapon in the Cyber Security. Further, if everyday users are the targets, then not only general public but also technical staff needs training and education in Cyber security. I believe that cyber security is not only the

next step in cyber security defense; it may be one of the most important steps we can take. Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from an unauthorized access, change or destruction. Through public general awareness we want to encourage the profession to reach out to the populous and help make them security literate. The goal of this research is to provide an alternative approach to learning more about Cyber Security awareness, it will help user in their lives. Traditional methods such as intrusion detection system and prevention system cannot effectively deal with insider attack problems because they lack of dynamic inference capability to acquire and understand cyber situational awareness.

II. CYBER SECURITY AWARENESS

Cyber Security awareness among general user easily can be created by Social networking sites, Cyber defense Competitions, Seminars, workshops and Public protection and disaster relief operations programs etc. A comprehensive cyber security plan needs to focus on three key areas, these are

a) **Prevention:** it includes solutions. Policies and procedures need to be identified to reduce risk of attack.
b) **Resolution:** In case of computer security breach, plans and procedures need to in place to determine the resources that will be used to remedy of threat.
c) **Recompense:** Companies need to be prepared to address a security threat with their employees and customers to ensure that any loss of business is minimal.

As like above three key areas cyber security plan there are various models of Cyber security these are

a) Prediction Model-Basically this model work on impact of an attack based on significant factors that influence cyber security.
b) Maturity Model-This model provides a structure for organizations to baseline current capabilities in cyber security workforce planning, setting a foundation and consistency of evaluation.
c) Industry Competency Model-The model incorporates competencies identified in the Industry and complements the Framework by including both the competencies needed by the average worker who uses the Internet or the organization's computer network, as well as cyber security professionals.

Currently Social Networking sites are more popular medium of interaction and communication with users. These sites provide the ability to run applications to users' knowledge. The popularity of social networks makes it an ideal tool through which awareness can be created on existing and emerging security threats. Information of Cyber Security is still severe challenge to spoil the threats due to lack of control on security breaches and awareness in the society.

III. INFORMATION SECURITY

The U.S. Code defines Information security as a means of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

- Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;

- Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- Availability, which means ensuring timely and reliable access to and use of information.

Risk is formally defined as "the effect of uncertainty on objectives". Risk is often characterized by a probabilistic analysis involving both the likelihood of potential events and their consequences on the organizational objectives. Risk management involves "coordinated activities to direct and control an organization with regard to risk" (ISO 73 2009).Historically, risk management is a highly introspective knowledge acquisition process that yields benefits not only in the ability to reduce uncertainty in the outcomes of objectives, but also provides the prerequisite knowledge necessary to proactively develop contingency plans which can be placed into action should a risk materialize. Organizations typically use a risk management process to identify and mitigate risks to assure their organizational mission. Risk management provides a documented, structured, and transparent process to identify critical resources, estimate threats, and vulnerabilities. The intersected set of threats and vulnerabilities cause harm (risks) to those identified resources. Moreover, the process estimates the likelihood of risk occurrence and evaluates tradeoffs among control measures used to mitigate the risks, and periodically revisits the analyses as needed. However, the value of the analysis is a strong function of the accuracy of the inputs to the process.

IV. RELATED WORK APPLICABLE TO INVESTIGATION

Organizations typically implement an IT focused risk management process to identify and mitigate IT related risks in order to assure their organizational mission. These enterprises span industries and infrastructures listed in the next several paragraphs. The European Network and Information Security Agency (ENISA) have generated an inventory of risk management and risk assessment methods. A total of 13 methods were considered. Each method in the inventory has been described through a template. The template used consists of 21 attributes that describe characteristics of a method. The inventory website also provides for the comparison of the risk management methods and also the risk management tools. In the context of applying these techniques to an application space, a critical infrastructure is, "an infrastructure so vital that it incapacity or destruction would have a debilitating impact on our defense and national security". With respect to various subject domains, the associated critical infrastructure consisting of 11 sectors (agriculture and food, water, public health, emergency services, defense industrial base, telecommunications, energy, transportation, banking and finance, chemical and hazardous material, and postal and shipping), and 5 key assets (national monuments and icons, nuclear power plants, dams, government facilities, and commercial key assets) have been identified. Vulnerability analysis of these critical infrastructures is well documented, using traditional techniques. Recently this list is expanding and the electric power industry is applying similar techniques to SCADA (supervisory control and data acquisition) equipment, cyber threats, cyber security, the Internet, and the Smart Grid. The oil and gas industry in particular and the chemical process industry in general store and transport hazardous and energetic chemicals, and operate processes under extreme conditions of temperature and pressure. Terrorists or disgruntled employees may exploit these conditions, which may then lead to toxic release, fire and explosion resulting in mass casualties, property damage, and economic and environmental impacts. Newer approaches are emerging that apply information security techniques of easing the complexity of creating tree and graph

structures and deriving probabilistic defense graphs from network architectural models. Further refinements have recently been documented and additional methodologies have been applied dealing with enhanced dynamic decision making.

V. CYBER SECURITY ECONOMETRICS SYSTEM (CSES) MOTIVATION FOR CURRENT INVESTIGATION

The Roadmap for Cyber-security Research articulates that information technology has become pervasive in every way from our phones and other small devices to our enterprise networks to the infrastructure that supports our economy. Improvements to the security of this information technology are essential for our future. As the critical infrastructures of the United States have become more and more dependent on public and private networks, the potential for widespread national impact resulting from disruption or failure of these networks has also increased. Securing the nation's critical infrastructures requires protecting not only their physical systems but, just as important, the cyber portions of the systems on which they rely. The motivation for this work is highlighted by existing and emerging technologies that complement the Roadmap in the context of the survivability of time-critical systems. The President's Comprehensive National Cyber-security Initiative also emphasizes the need for leap-ahead improvements in security of cyber physical systems. A failure is inclusive of random events, design flaws, and instabilities caused by cyber (and/or physical) attack. One such domain, optimizing investments in critical infrastructure protection, is applicable to the use of the Cyber Security Econometrics System (CSES). We discuss the workings of such a system in this context of the need for optimizing investments, the CSES mathematical foundations, the linear cascading of linear models, and the implications of this computing architecture, in particular, with respect to our nation's critical cyber infrastructure and key resources. Combining the subject domains of information security, and risk management, CSES is a methodology for estimating security costs to stakeholders as a function of possible risk postures. In earlier works, we presented a computational infrastructure that allows an analyst to estimate the security of a system in terms of the loss that each stakeholder stands to sustain as a result of security breakdowns. More recently, we presented how this infrastructure can be used in the subject domain of mission assurance. Additional work has applied CSES to specific business cases. The current state-of-the-art of CSES addresses independent events. In typical usage, analysts create matrices that capture their expert opinion, and then use those matrices to quantify costs to stakeholders. In situations where the underlying events exhibit significant dependencies, the current approach is not appropriate. Unfortunately, significant dependencies are likely to arise with any detailed modeling of a complex system of components, such as an enterprise network.

VI. CURRENT METHODS OF VULNERABILITY & THREAT DETECTION

There are currently two common ways in which a wireless threat can be detected: a technique known as war-driving and use of wireless intrusion detection systems (WIDS). WildCAT is based on war-driving. Wardriving is a technique for collecting wireless network data that involves driving around in a vehicle collecting information about the wireless network traffic that is detected. Wardriving requires a laptop running a wireless discovery program such as Kismet, NetStumbler or Flying Squirrel, a GPS device, and an antenna. This

technique usually lacks realtime threat detection because it requires further analysis that cannot be performed while driving. It is also a time-consuming process, requiring specially trained staff in order to perform the collection and vulnerability analysis. A WIDS consists of a system of sensors, which collect 802.11 data and forward it to a central management system where it is processed and stored. Although WIDS are effective, they are expensive, difficult to deploy and maintain, and limited to the boundaries of the sensors. Both WIDS and wardriving techniques do have some documented problems with unreliable hardware performance and high false alarms rates. Due to the pervasiveness of wireless networks, both wardriving and WIDS collect an overwhelming amount of data. It is difficult to identify relatively infrequent security risks amidst the massive amounts of information collected. Cyber analysts are specially trained to parse through this data to quickly identify and respond to any wireless threats. The WildCAT approach maximizes the time spent by cyber analysts on threat analysis by removing the need for them to conduct wardrives.

VII. POTENTIAL APPLICATIONS

Wireless communication is continuing to expand in industrial, residential, and government sectors as many people value the mobility and installation ease that wireless networking enables. However, an easy persistent method of monitoring wireless threats is needed to mitigate attacks to critical infrastructure through wireless vectors. WildCAT is designed to offer a flexible, low-cost, and easy method of wireless monitoring with existing patrol fleets.

A. Continuous Sustained Surveillance High-value targets such as ports, power generation facilities, refineries, embassies, and organizations interested in protecting confidential data and critical infrastructure can use WildCAT to continuously monitor their wireless networks. The visibility of wireless activity can be increased by instrumenting WildCAT sensors into any roving vehicle (maintenance, security, delivery, etc.). If an unauthorized, or rogue, device is attempting to connect to known, authorized wireless access point, security forces should be notified immediately.

B. Targeted Monitoring and Tracking Law enforcement needs the ability to link a client device and person responsible for illegal traffic observed at the ISP or IP level. With courts now recognizing that an IP does not link network activity to a person, it is crucial to collect evidence that can geo-locate a Wi-Fi client and record the network traffic being exchanged with an access point. Such evidence can successfully link a child pornographer or copyright infringer to their wireless network traffic. WildCAT is designed to be a rapidly deployable, shared resource within a group (grab & go-type device that requires little to no user training), or as silently vigilant standard vehicle equipment that is always monitoring and reporting its findings.

C. Multiple Site Security Instead of configuring a WIDS at each and every location, security professionals can use WildCAT as a low cost roving sensor that travels between sites. Alternatively WildCAT sensors can be mounted to vehicles and rotated between sites.

D. Extend WIDS Coverage WildCAT can reach areas that are not typically covered by fixed WIDS sensors such as parking lots, thereby adding visibility beyond a WIDS. Wireless APs can be connected to a wired LAN and as a result expose an organization to attack outside the range of deployed wireless access points and WIDS sensors.

The recent cyber attacks by Russia against Georgia in August 2008, along with attacks on Estonia in 2007, Lithuania in 2008, and Kazakhstan in early 2009, have greatly increased the visibility of the international problem of cyber security. The cyber attacks were closely timed with actual Russian military operations against Georgia. Social networks operating on the Internet were used during the attacks and prior to the attacks for the recruiting of attackers. The cyber attacks appear to have been orchestrated by Russian organized crime working with the Russian government. The cyber attacks began with botnets, which consisted of denials of service and website displacement. Though they appeared minor in nature, the attacks significantly impeded the ability of the Georgian government to deal with the invasion. If more international cooperation had taken place, someone could have potentially warned Georgia of the pending attacks.

VIII. CYBERSPACE ENABLED ECONOMY

The economy, the infrastructure, the safety and the security of the United States, as well as much of the rest of the world, depend upon the Internet for the transfer of electronic data. The nation's critical infrastructures use the Internet as the primary means to interconnect. As the Director of National Intelligence (DNI) recently testified before Congress, "the growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures". The American and international public, businesses, and governments have become increasingly dependent on automated information systems. These systems have also become extremely interconnected worldwide with the entire critical infrastructure. The cyber critical infrastructures are attractive targets for individuals and organizations that seek monetary gain, intelligence, or just the pleasure of doing damage to individuals, industry sectors, and even countries. Attackers use a variety of tools and techniques to identify and exploit system vulnerabilities and to collect information passing through the networks. As the sophistication of the attacker tools increase, the need for required complex knowledge is less important. As it becomes easier to attack network systems, the numbers of attacks increase, as does the potential damage increases. The computing environment is transitioning to a globally integrated information structure and a worldwide effect will be felt across all sectors if a catastrophic event happens to the major networks. Many systems would feel the cascading effects as those effects ripples through the critical infrastructures of the developed countries. Attackers have stolen, modified, and destroyed both data and software. They have shut down entire systems and networks, thereby denying service to users who depend on automated systems to help meet critical needs. Some of the more common threats are listed and described below. Many are experienced at the same time. Zero day vulnerability is commonly observed, which is where a flaw in software is discovered, but not quickly corrected. Flaws in the system will continually be exploited until they are corrected or bypassed.

IX. CYBERSPACE VULNERABILITY

There is no doubt that America and the rest of the developed world's critical infrastructure networks are under constant threat. Pervasive vulnerabilities of hardware and software and the connectivity of these mechanisms to the Internet make the multi-layered lines of defense, meaning anti-virus, firewall, and intrusion detection,

relatively ineffective. The last 5 years have seen a dramatic increase in the number of Web application vulnerabilities. Both businesses and consumers are at risk; attackers target businesses with sensitive and valuable data, and consumers for their personal information, banking details, or simply their computer resources to create Botnets. Many of the risks and vulnerabilities face in cyberspace seem to be because of a lack of planning, coordinating with different agencies, and being reactive instead of proactive. Networks are vulnerable because of inexperienced and untrained IT personnel and individuals using weak passwords. Moreover, identified weaknesses often go uncorrected for financial or time reasons. Another problem is that incidents are not reported to the appropriate authorities for dissemination to others. Part of this lack of reporting is because there is not a clear line of responsibility. This lack of a clear line of responsibility is discussed in the Section on governance. Lightening, power fluctuations, surges, blown fuses and other power outages all disable computer systems, since they rely on an electrical source. Developments in Information and Communication Technology have created a desire to have meters installed for household electricity monitoring and interfacing. There is now a capability to remotely monitor electric, water, and gas consumption for an individual's homes. There are a lot of benefits associated with the upgrade, such as improved efficiency, quicker response to problems, and more accurate billing. The data are sent over computer networks, however, this makes the system vulnerable to intercept and malicious attacks. The data could also be used by an intruder, to determine when the homeowner is home, based on electricity usage. With any new technology come new risks and vulnerabilities, which need to be identified and mitigated. The electric companies need to assure information security and prevent malicious attacks on the system. Electricity plus Information, features, such as electricity transmission, distribution, and billing are all integrated with information networks. The technology has enhanced the performance part of the system with monitoring and controlling the system, but the openness of the networks creates threats and makes the system and the electrical system vulnerable to malicious attacks. The security of the system, along with the issue of maintaining the confidentiality and integrity of data on the networks, is a major concern. There are also failures caused by worms, or viruses, which can be attributed to terrorism, espionage, and other hacker activity. There are risks of computer and / or SCADA system failures. SCADA systems are used for process control in manufacturing and utilities. These systems are used to control refineries, power plants, factories, and other highly complex environments. SCADA faces vulnerabilities to security and stability issues. There needs to be better security technology with protocols, firewalls, and an audit/assessment of security administration. According to the National Vulnerability Database and nCircle VERT (Vulnerability and Exposure Research Team), "Web application vulnerabilities have increased from 1.9% of all published vulnerabilities in 2006 to over 52% in 2009 (projected based on Q1 and Q2 growth rate). It is important to note that these figures only represent web application vulnerabilities in libraries, languages, frameworks and canned web applications; they do not account for the numerous custom Web Applications that contain their own web application vulnerabilities". Applications seem to be more attractive, since they are not as effectively secured as operating systems. Specifically, there are fewer venders of operating systems, they pay more attention to the systems, and they send patches correcting identified problems quicker. According to the Sans organization, during the last few years, the number of vulnerabilities being discovered in applications is far greater than the number of vulnerabilities discovered in operating systems. As a result, more exploitation attempts are recorded on application programs. The most "popular" applications for exploitation tend to change over time since the

rationale for targeting a particular application often depends on factors like prevalence or the inability to effectively patch. Due to the current trend of converting trusted web sites into malicious servers, browsers and client-side applications that can be invoked by browsers seem to be consistently targeted. Information and Communication Technology (ICT) is so complex that the many different interdependent components make assessing the vulnerabilities difficult. There are so many possible unpredictable combinations that it makes security of the system difficult. There are available models that can generate an attack model graph. Variables, such as the network security policy, vulnerabilities of the system, and topology of the network, are input into the model. A cost benefit analysis can be conducted to assess the most likely behavior of the attacker. Cost ratings can also be based on the severity ratings given by CVSS or US-CERT. The Model can help to determine what processes, or components, are most in need of improvement.

X. CONCLUSION

The task of preventing unauthorized users from compromising the confidentiality, the integrity, or the availability of sensitive information is increasingly difficult in the face of the growth in Internet use, the increasing skill level of attackers, and the technological advances in their tools and methods of attack. The threats and risks are real and increasingly frequent, with high potential to critical energy infrastructures. The Department of Homeland Security needs to have a clear plan in place to help better mitigate the problems faced with cyber security. The Unites States needs to work with its international allies to help establish/improve the current governance for cyber security issues.

REFERENCE

[1] L. Pipkin, Information security protecting the global enterprise:Hewlett-Packard Company, 2000.

[2] Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems, recommendations of the national institute of standards and technology," National Institute of Standards and Technology, U.S. Department of Commerce, Gaitherburg, MD NIST Special Publication 800-30, 2002.

[3] C. Woody, J. Coleman, M. Fancher, C. Myers, and L. Young, "Applying octave: Practitioners report," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA CMU/SEI- 2006-TN-010, 2006.

[4] COBIT, "Control objectives for information and related technology," Governance, Control and Audit for Information and Related Technology. IT Governance Institute / ISACA / ISACF, 2011.

[5] R. T. Marsh, "Critical foundations: Protecting america's infrastructures - the report of the president's commission on critical infrastructure protection," The White House, Washington, DC 1997.

[6] Srivastava and J. P. Gupta, "New methodologies for security risk assessment of oil and gas industry," Process Safety and Environmental Protection, vol. 152 in press, p. 6, 2010.

[7] T. Sommestad, M. Ekstedt, and P. Johnson, "Cyber security risks assessment with bayesian defense graphs and architectural models," in 42nd Hawaii International Conference on System Sciences, Waikoloa, Big Island, Hawaii, 2009, pp. 1-10.

[8] T. Sommestad, M. Ekstedt, and P. Johnson, "A probabilistic relational model for security risk analysis," Computers & Security, vol. 29, pp. 659-679, Sep 2010.

[9] M. R. Grimaila and A. Badiru, "A hybrid dynamic decision making methodology for defensive information technology contingency measure selection in the presence of cyber threats," Operations Research: An International Journal, 2011.

[10] T. Sheldon, R. K. Abercrombie, and A. Mili, "Methodology for evaluating security controls based on key performance indicators and stakeholder mission," in Proceedings of 42nd Annual Hawaii International Conference on System Sciences (HICSS-42), Waikoloa, HI, 2009, pp. 1-10.