ISSN: 2379-3686 International Journal of Science Research and Technology
Volume 2 Issue 1, p p 42-44, 25th March 2016

SURVEY ON CYBER THREATS AND MANAGEMENT POLICIES

Prof. Debalina Nandy
Assistant Professor, Computer Engineering Department, Atmiya Institute of Technology & Science, Rajkot, Gujarat

Prof. Renish Padariya
Assistant Professor, Computer Engineering Department, Om Engineering College, Junagadh, Gujarat, India

Abstract - *Human-centric and machine-centric approaches are insufficient for defending the security of today's increasingly complex computer infrastructures. Current cyber defense systems involve humans at multiple levels, but people are often far down in the control structure, requiring them to make too many time-critical decisions. Information flow between humans is slow and frequently asynchronous. In a crisis, humans may be unable to cooperate because of culture, language, legal, proprietary, availability, or other obstacles. Such systems cannot adapt to the Internet speeds of cyber threats. Consequently, effective cyber defense requires a framework that simultaneously capitalizes on the adaptability of humans and the speed of machines. In other words, humans must be put in the right loop to maximize their effectiveness while preserving their legal responsibility for the actions of their autonomic systems.*

***Key Words*:** Cyber Threats, Definition, Risk Analysis, Policies

1. INTRODUCTION

The commonly accepted definition of cyber security is the protection of any computer system, software program, and data against unauthorized use, disclosure, transfer, modification, or destruction, whether accidental or intentional. Cyber attacks can come from internal networks, the Internet, or other private or public systems. Businesses cannot afford to be dismissive of this problem because those who don't respect address, and counter this threat will surely become victims. CID will enable cooperative defense of infrastructure through situational awareness using visualization, security policy dialogue between humans and agents, shared initiative in solving cyber problems, and a foundation for building trust between humans and agents within and between organizations. Cyber security exercises are a very effective way of learning the practical aspects of information security. But designing such exercises is not an easy task and requires the work of several people. CID is designed to be a scalable, dynamic, and robust framework for securing increasingly complex computational infrastructures. CID makes humans an intrinsic part of the solution, engaging them without requiring them to directly control and enables diverse

organizations within an infrastructure to cooperate in an adaptive cyber defense.

1.1 History of Cyber Threats

Everywhere Cyber-crime is on the rise. On average, there has been a reported cyber security event every single day since 2006. If there's a transaction that involves a card with a magnetic strip and a swipe, there's a transaction that involves a risk. And if there's a computer system with software designed to allow access by multiple users (e.g. by franchisees, vendors, or other providers) without security in mind, then there's a major risk of being hacked for malicious or competitive purposes. Mobile devices, often containing sensitive data, are lost or stolen every day. In the cyber security world, there are only two kinds of computer systems: those that have been hacked and those that will be hacked. And just because people are computer savvy does not mean their data are safe. Like an AIDS test,

penetration testing in the cyber security arena offers assurance and protection only as of the date of the testing. So once is not enough. Penetration testing must be done regularly and thoroughly to maintain its value or it becomes worth no more than a cancelled subscription.

1.2 Cyber Policies / Procedures

Organizations are well advised to have policies in place with respect to data protection, data retention, data destruction, privacy, and disclaimers to customers. And, if a security breach occurs, the company should expect, and be prepared for, a regulatory investigation during which the company will have to show that its policies were well documented, updated as business processes change and observed, or risk significant fines, agency oversight, or worse. The policies must be more than mere window dressing, failure to conform to a company's own stated, internal policies may be worse than having no policies at all.

2. CYBER RISK ANALYSIS

There has been formulated a "Scale of Cyber In-Security" based on the potential harm that can be caused:

Low risk: Hacker has gained entry to system but minimally. Minor risk of business disruption, but access can aid attackers in information gathering and planning future attacks.

Medium Risk: Malware has been implanted in the company's network, which could cause malfunctions and mischief. There is a significant risk of a business disruption that could result in financial loss and/or damage of goodwill.

Medium-to-High Risk: Using sniffers or other equipment, hackers have obtained personally identifiable information (PII) from point of sale (POS) systems. There is a significant risk of a business disruption that could create financial loss and/or damage of goodwill.

High Risk: Inside job: data stolen by disgruntled employee. There is a potential risk of business disruption, resulting in financial loss and damage of goodwill. PII may be taken, as well as company's confidential information and financial information.

Critical Risk: Hackers have gotten into the system and can access company's financial information and confidential information. There is a severe risk of business disruption, financial loss, damage of goodwill. System, application, and database have been compromised.

Major liability may be incurred from, individual litigation, class litigation, regulatory investigation, contract dispute, loss of customers, reputation damage, data theft, denial of service, cyber-terrorism.

3. CYBER CRISIS MANAGEMENT

Though cyber attacks may be inevitable, companies can mitigate the resulting damage through effective crisis management. Preparing for cyber incidents and managing crisis communications effectively are essential to minimizing the impact of significant cyber incidents.

Before a crisis occurs, business leaders can continuously improve their organizations' ability to respond by assessing capabilities, planning, and preparing through custom-made executive tabletop exercises. Good Harbor helps clients develop crisis management plans and also designs, coordinates and leads realistic tabletop exercises for chief executives and other senior corporate officers to help them achieve three key objectives:

1. Evaluate assumptions, capabilities, and the effectiveness of existing response planning;
2. Strengthen the awareness of senior leaders and crisis management teams of response plans and the importance of crisis preparedness and response; and,
3. Improve the ability of multiple teams from across the organization to communicate and work together quickly and effectively in a real crisis.

When a cyber incident has already happened, the stakes of crisis management and communications are high. The impact of poorly handled communications can be worse than the impact of the breach itself. Consequences include loss of

shareholder or customer confidence, financial impacts, and damage to a company's hard-earned reputation.

With so much on the line, companies turn to Good Harbor to be a trusted advisor and to help navigate the crisis environment. Good Harbor brings together cyber risk and crisis management expertise to help clients accomplish the following:

1. Develop and implement a tailored strategy for managing the cyber incident and crisis communications
2. Navigate relations and disclosure requirements with investors, clients, employees, and government agencies; and,
3. Protect and enhance reputation through diligent crisis management and communications.

3. CONCLUSIONS

The risks of cyber crime are very real and too ominous to be ignored. The human factor is the weakest link in any information security program. Communicating the importance of information security and promoting safe computing are key in securing a company against cyber crime. Communicate/educate with employees and executives on the latest cyber security threats and what they can do to help protect critical information assets. Secure all mobile devices when traveling, and report lost or stolen items to the technical support for remote kill/deactivation. Educate employees about phishing attacks and how to report fraudulent activity. At the very least, every company must conduct a professional analysis of their cyber security and cyber risk, engage in a prophylactic plan to minimize the liability, insure against losses to the greatest extent possible and implement and promote a well-thought out cyber policy.

REFERENCES

[1] Lance J. Hoffman, Daniel Ragsdale: Exploring a National Cyber Security Exercise for Colleges and Universities, IEEE Security and Privacy, Volume 3, Issue 5 (September 2005).

[2] Wayne Schepens, Daniel Ragsdale, John Surdu, the Cyber Defence Exercise: An Evaluation of the Effectiveness of Information Assurance Education, the Journal of Information Security, Volume 1, Number 2. July, 2002.

[3] Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace, ABC-CLIO, 2010.

[4] Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

[5] Frincke, D., Wespi, A., Zamboni, and D: From Intrusion Detection to Self-Protection, Computer Networks 51, 1233--1238 (2007).

[6] Karat, J., Karat, C.-M., Brodie, C., Feng, J.J.: Privacy in Information Technology: Designing to Enable Privacy Policy Management in Organizations Int. J. Human.-Computational Studies, 63, 153--174 (2005)

[7] Axelsson, S the base-rate fallacy and the difficulty of intrusion detection. ACM Trans. Information and System Security, 3(3):186–205, 2000.

[8] Rao, A.S., Georgeff, M.P.: BDI Agents: From Theory to Practice. In: First International Conference on Multi-Agent Systems (ICMAS-95) pp. 312—319, AAAI Press, Menlo Park, CA, USA (1995).