



NATIONAL CYBERSECURITY INSTITUTE JOURNAL

Volume 2, No.1



© Excelsior College, 2015

ISSN 2375-592X

National Cybersecurity Institute | 2000 M Street, Suite 500 | Washington, D.C. 20036
Excelsior College | 7 Columbia Circle | Albany, NY 12203-5159

National Cybersecurity Institute Journal

Volume 2, No. 1

Founding Editor in Chief:

Jane LeClair, EdD, National Cybersecurity
Institute at Excelsior College

Associate Editors:

Denise Pheils, PhD, Excelsior College
Michael Tu, PhD, Purdue University

5. Intrinsic or Opportunistic: Chinese Cyber Espionage Strategies

Miguel Alberto Gomez

13. War Against Identity Cyber Assault in a Social World

Sharon L. Burton
Dustin Bessette

**21. Regulation of Cybersecurity in the Financial Sector:
Now Modeled on the Emergency Preparedness Cycle**

Ken Lerner
Matthew Berry

**37. Cybersecurity Graduate Training Reveals Security-by-
Obscurity Vulnerabilities in Website Authentication**

Gordon W. Romney
Dustin L. Fritz

**51. The Exclusiveness of Malicious Software Called
Spyware and Exploring Mitigating Techniques**

Aron Schwartz

**69. Bibliometric Analysis of the Scientific Literature on MOOC's
Self Directed Learning (SDL) and Educational Taxonomies**

Teresa Ferrer-Mico
Miquel Angel Prats-Fernandez

79. Security in Cyberspace: Part II: NCI Cyber Symposium Series

Jane A. LeClair, EdD
Matthew Flynn, PhD

EDITORIAL BOARD

Founding Editor in Chief

Jane LeClair, EdD, National Cybersecurity Institute
at Excelsior College

Associate Editors

Denise Pheils, PhD, Excelsior College
Michael Tu, PhD, Purdue University

PEER REVIEWERS

The *National Cybersecurity Institute Journal* gratefully acknowledges the reviewers who have provided valuable service to the work of the journal:

Peer Reviewers

Mohammed A. Abdallah, PhD,
Excelsior College/State University of NY
James Antonakos, MS,
Broome Community College/Excelsior College
Barbara Ciaramitaro, PhD
Excelsior College/Walsh College
Kenneth Desforges, MSc, Excelsior College

Amelia Estwick, PhD, Excelsior College
Ron Marzitelli, MS, Excelsior College
Kris Monroe, AOS, Ithaca College
Sean Murphy, MS, Leidos Health
Lifang Shih, PhD, Excelsior College
Michael A. Silas, PhD, Excelsior College/Courage Services
Michael Tu, PhD, Purdue University

NATIONAL CYBERSECURITY INSTITUTE JOURNAL

The National Cybersecurity Institute at Excelsior College is a research center based in Washington, DC, dedicated to increasing knowledge of the cybersecurity discipline and its workforce demands. Published three times a year, the peer-reviewed *National Cybersecurity Institute Journal* covers topics that appeal to a broad readership within the cybersecurity discipline, with a particular focus on education, training, and workforce development. The manuscripts submitted to the journal are reviewed for their contribution to the advancement of applied research in the area of cybersecurity.

Submission guidelines for authors can be found at www.nationalcybersecurityinstitute.org/journal/.

FROM THE EDITOR

Greetings and welcome to the 4th issue of the National Cybersecurity Institute Journal (NCIJ). As the ever expanding cybersecurity community is now fully aware, our mission at NCI is to continue to increase the awareness and knowledge of the cybersecurity discipline, and assist the government, industry, military, and academic sectors to better understand and meet the challenges in cybersecurity policy, technology, and education by offering a peer-reviewed venue for current events, quality research, and applicable topics. In past issues of this journal we strove to provide timely and knowledgeable articles that would be well received by the cyber community. Here at NCI we will continue to publish relevant and noteworthy articles three times a year that will serve to enlighten those with a vested interest in the cybersecurity field. In this current issue, you will find articles from notable authors and subject matter experts with a variety of perspectives in the field of cybersecurity.

Miguel Alberto Gomez provides us with a very timely work on understanding the foundations of cyber espionage. This is followed by a fascinating article by Sharon L. Burton and Dustin Bessette on the war against identity cyber assault in social media. Aron Schwartz from Towson University then offers a case study, “The Exclusiveness of Malicious Software Called Spyware and Exploring Mitigating Techniques.” Ken Lerner and Matthew Berry from Argonne National Laboratory present a detailed look at regulation of cybersecurity in the financial sector. Gordon Romney and Dustin Fritz offer their views on cyber training with their article, “Cybersecurity Graduate Training Reveals Security-by-Obcurity Vulnerabilities in Website Authentication.” Teresa Ferrer-Mico and Miquel Angel Prats-Fernandez provide us with an interesting review of the scientific literature on MOOCs, Self Directed Learning (SDL), and educational taxonomies. Finally, we conclude the journal with an update on the latest cyber symposium that was held here at NCI—Security in Cyberspace.

I’m quite sure these articles will provide you, the reader, with knowledgeable insight that you will bring back to the workplace, and will hopefully instill in everyone who reads this a desire for further thought and research on the topics discussed.

It goes without saying that a publication such as this is never the work of one individual, but rather a collaboration of dedicated people here at NCI who work tirelessly to produce the quality product you have before you. My thanks go to all the contributors, administration, and staff for their extraordinary efforts in bringing the National Cybersecurity Institute Journal to our readers once again. I hope that everyone in the cyber community will find this journal informative as you work within your respective cyber areas. As always, I look forward to your comments, suggestions, and future submissions to our journal.



Dr. Jane A. LeClair
Editor in Chief

Intrinsic or Opportunistic: Chinese Cyber Espionage Strategies

Miguel Alberto Gomez

ABSTRACT

The growth of cyber espionage is viewed as a significant threat to both private and public sectors across the globe. While explanations that range from increases in interconnectivity to societal predilections toward cyber espionage have been offered, there continues to exist a dearth of ontological research as to the emergence of this phenomenon. This exploratory study attempts to explain cyber espionage as the manifestation of an established strategic culture. That is to say, cyber espionage is not the result of precipitous technical circumstances within cyberspace nor is it simply the enduring consequence of primordial traits that encourage such activities. Rather, it is the reflection of the manner in which the establishment has consciously decided to further their respective state's interests in an increasingly digitized world. To achieve this, the study analyzes cases of cyber espionage that have been attributed to China through the lens of its strategic culture. Upon its conclusion, this study proposes that while states may have comparable cyber power and cultural traits, variations in the expected behavior of states in cyberspace are the function of their respective strategic cultures as interpreted by political and military elites.

INTRODUCTION

To assert that cyber espionage is a new phenomenon is to suggest the acceptance two critical assumptions. The first being that cyber espionage, defined throughout this study as *the use of dangerous and offensive intelligence measures in the cyber sphere of interactions* (Valeriano & Maness, 2013), may be employed by parties (state actors for this study) that have an investment in cyberspace in terms of capabilities and critical resources, and the second being the scant understanding of the causes of cyber espionage—attributable to its novelty. But to accept these is to deny the fact that cyber espionage has existed for well over a decade with one of the earliest reported instances being the breach of the Pentagon's systems in 1999—now known as Operation Moonlight Maze (Drogin, 1999). Yet despite the passing of 15 years, a universally accepted definition of cyber espionage and, more importantly, a sound explanation as to the causes of cyber espionage is still forthcoming. This study hopes to address the latter by offering an alternative explanation for this phenomenon by identifying an actor's strategic culture as the germ that eventually leads to this activity as opposed to a purely rational occurrence or that is attributable to specific and enduring societal traits.

In doing so, this study is presented as follows. A review of existing hypotheses is necessary to demonstrate to the reader the level of progress that currently exists in our attempts to explain the phenomenon of cyber espionage. This section also serves to highlight the weakness of these hypotheses in explaining certain aspects of the phenomenon. This is then followed by a brief discussion of the notion of strategic culture in which a standard

definition is taken for this study and pre-conditions for its applicability are set. The rationale behind the choice of these two cases will be explained later. Finally, the applicability of strategic culture is demonstrated in explaining the occurrence of Chinese cyber espionage.

As a word of caution to readers who may not be familiar with the concept of cyberspace, there is as of yet no generally accepted definition for this. In order to maintain a single understanding of these concepts for the rest of the study, cyberspace is understood to be *a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information technologies* (Kuehl, 2009). Furthermore, it is important to point out that the United Nation's Group of Government Experts recently concluded that international law is applicable to cyberspace. Consequently, this allows cyberspace to be treated as a domain similar to that of the physical world.

CYBER ESPIONAGE AS A RATIONAL OCCURRENCE

The study of cyber espionage is most often closely associated with that of cyber warfare (another equally contentious topic) in the sense that some authors have implied the former to be a subset of the latter (Hjortdal, 2011). While this study does not attempt to establish the relationship between the two, understanding that such a relationship exists is crucial as the realist view of cyber warfare may be reasonably applied to that of cyber espionage. In this light, the study conducted by Valeriano and Maness serves as our exemplar for this line of thought.

Building on their initial research regarding the probability of cyber conflict vis-à-vis existing rivalry, Valeriano and Maness have provided three hypotheses as a means of establishing a theory for cyber

espionage. (1) Due to power imbalances, less powerful rival states will use cyber espionage as a tactic to perceptively bridge the power gap with the more powerful state. (2) Due to international constraints and norms, rival states will use cyber espionage in order to manage low-level competition between two actors but this competition will be minimal and represent the normal relations range of rival interactions. (3) Rival states will use cyber espionage to provoke economic costs to their rivals, as these perceived threats will get public attention and create demands for more spending on national security (Valeriano & Maness, 2013).

The premise that cyber espionage is used as a tactic that bridges the power gap between rivals is rooted in the understanding that cyberspace favors asymmetric over symmetric engagement due to the low cost of entry and the challenges of attribution afforded to actors. That said, one might reason that between rival states we should expect the weaker states to use their cyber capabilities offensively while stronger states would use theirs defensively—if at all. Within the context of cyber warfare as a whole, this pattern appears to remain firm. But if we are to analyze the occurrence of cyber espionage between states vis-à-vis cyber power, the pre-established relationship appears to lose some of its explanatory capabilities (Gomez, 2013). This is particularly true in the case of Operation Olympic Games that has been attributed to the United States and had a cyber espionage component targeting Iran (Nakashima, Miller, & Tate, 2012). Other cases include Russian cyber espionage campaigns directed toward Georgia and Chinese activities aimed at dissidents (CrowdStrike, 2013; Geers, Kindlund, Moran, & Rachwald, 2013). In all these cases, the initiating actor exists with greater power relative to the recipient(s). In this regard, Valeriano and Maness' first hypothesis cannot account for this deviation in the expected behavior.

The second hypothesis, however, follows the observed behavior much more closely. The idea that rivals maintain a manageable level of hostility in cyberspace—for cyber espionage and other similar

acts—can easily be observed. According to Gomez (Gomez, 2013), it was demonstrated that established rivals engaged one another in cyberspace but within bounds that would not escalate existing tensions or raise doubts as to the actors involved. In this sense, the actors behaved in much the same way as was predicted by Libicki wherein low-impact activity, preferably outside the visibility of the general public, is preferred as this minimizes the possibility of escalation and permits the actors greater freedom of action and response (Libicki, 2009). Quantitatively, Axelrod and Ilev's mathematical model of cyber conflict also account for the observed behavior. In their study, the decision to engage in cyber conflict is a function of three key factors: the stakes, resource characteristics, and the value of the resource. Stakes refer to what the actors have to gain (or lose) if they are to engage in cyber conflict. Resource characteristics pertain to the techniques and technologies available for use and whether or not these resources could be useful at a later date. Finally, the value of the resource determines if it can be used to exploit a weakness at the target at this point in time (Axelrod & Ilev, 2013). Taken collectively, Axelrod and Ilev demonstrate that the capability to engage in conflict in terms of resources is just as significant as the timing to do so—impulsive acts are rarely undertaken.

Finally, Valeriano and Maness argue that continued cyber espionage would harass rivals into action and possibly lead them to incur increased economic costs as means to address the perceived threat. In this regard, confirming the validity of their argument proves to be challenging. On the one hand, an increase in the number of reported cyber espionage activities has the potential of increasing the public's awareness of the threat this poses (Lewis, 2014). On the other hand, gauging the impact of these activities is challenging at best. In their paper, Valeriano and Maness have acknowledged that despite their awareness of Chinese cyber espionage activities, Washington has done little to contain the threat (Valeriano & Maness, 2013)—implying that the American government is either unable to address the threat or that the impact of the perceived threat is highly exaggerated. In support of the latter, a comparative study of recent cases of cyber conflict

has demonstrated that despite advances in technology, events in cyberspace have yet to influence foreign policy (Iasiello, 2013).

As a whole, viewing cyber espionage through the lens of realism is limited. While it can be shown that activities in cyberspace are not random or impulsive acts, this approach fails to provide us with an adequate explanation as to why certain actors choose to engage in cyber espionage—as in the case of the U.S. and China—and the actual impact in terms of gains such activities may have for both parties involved.

Cyber Espionage as a Primordialist Manifestation

Deviating away from the rationalistic interpretation of cyber espionage, an emergent approach to analyzing the phenomenon has presented the occurrence of such as the result of established societal traits. While this view has existed for some time in the form of anecdotal evidence lacking significant empirical proof, exploratory research conducted by Karamanian and Sample have managed to provide some support to these claims. Their study analyzed the societal traits of both initiators and targets of cyber espionage against Hofstede's Cultural Dimension Theory. From their initial findings they have identified specific characteristics unique to these parties. Initiators, as per their results, are characterized as traditional hierarchical societies that value patience and are less individualistic. Targets, on the other hand, are viewed as liberal societies that foster individualism and innovation (Karamanian & Sample, 2014). The authors, however, have cautioned that due to the nature and quality of the available data, the causality established might not be representative of the actual ground truth. Such a warning may indeed be justified.

If the occurrence of cyber espionage is strictly a function of these established traits and given the low cost of entry into cyberspace, one should expect more cases of cyber espionage from states such as Vietnam and India. The history of such events, however, show that states that are expected

to utilize such techniques have not consistently done so—China being an exception. Building on the previous examples, both Vietnam and India have utilized cyberspace but in a different manner¹. More importantly, both have been victims of cyber espionage rather than its initiator, thus finding exemptions to the expected characteristics of targets. To date, no existing study has yet emerged to address these ambiguities. Consequently, this questions the assumption that societal traits, on their own, are proper indicators of actions in cyberspace—cyber espionage in particular.

Strategic Culture Overview

In lieu of the fact that both realist and promordialist framings of cyber espionage have failed to adequately explain the occurrence of these events, this study proposes an alternative view to bridge this gap through an understanding of strategic culture. Jack Snyder first established the concept of strategic culture in 1977 as “*a set of semi-permanent elite beliefs, attitudes, and behavior patterns*” (Snyder, 1977). Snyder also specified other elements of strategic culture such as organizational, historical, and political influence as well as technological constraints (Lantis, 2002). Duffield later expanded this definition by attributing to strategic culture the specific foreign policy goals and objectives that are pursued by elites and the general interpretation of the international environment. In line with this, goals are evaluated on three different levels, “*the cognitive, which includes empirical and causal beliefs; the evaluative, which consists of values, norms and moral judgment, and the expressive or affective, which encompasses emotional attachments, patterns of identity and loyalty, and feelings of affinity, aversion, or indifference*” (Duffield, 1998). From these initial definitions, two key points stand out. First is that strategic culture is constructed rather than intrinsic, this presupposes that possibility of change. Current interpretations of strategic culture posit that change is faster during dramatic events that challenge

previously held beliefs (Eitelhuber, 2009). Building on this, one could reasonably argue that advantages offered by technological revolutions—such as the emergence of cyberspace—may cause state behavior to change and appear irrational. Second, strategic culture is the domain of elites, specifically, the leadership. While current literature does not ascribe strategic culture to a single individual, rather as a “*property of collectivities rather than simply of the individuals that constitute them*” (Legro, 1995), leaders are the ones who “*redefine the limits of the possible*” in foreign and security policy discourse (Cruz, 2000).

Taking these into consideration, this paper adopts the definition of strategic culture proposed by Scobell as “*the set of fundamental and enduring assumptions about the role of collective violence in human affairs and the efficacy of applying force interpreted by a country’s political and military elites*” (Scobell, 2014). This specific definition is suitable for the purposes of this study as it (1) takes into consideration the role of elites in the formation of policy, (2) takes into account political, economic, social, and technological factors as understood to be human affairs, and (3) acknowledges that the subsequent decisions are the result of how the underlying factors were framed by political and military elites.

While the previous arguments have established that strategic culture could explain gaps in understanding the occurrence of cyber espionage and other activities in cyberspace, it is sound to say that no single theory could suffice for all cases. For strategic culture to be applicable, the cases in question should demonstrate the following, (1) strong national cultural identity, (2) elite allegiance to tradition, and (3) strong military organizational culture (Lantis, 2009). Although these constrain the cases for which strategic culture provides suitable explanatory powers, it lends itself well to explaining the case of China that has been at the center of most debates regarding cyber espionage.

¹ In both cases, disruptive events such as DoS and DDoS have been observed.

CHINESE CYBER ESPIONAGE— A CASE FOR STRATEGIC CULTURE

The case for the applicability of strategic culture in the context of analyzing China's cyber espionage campaign rests squarely on meeting the prerequisites established earlier. The value of national cultural identity is rooted in the idea that cultural beliefs and values are the lens through which perceptions of events are shaped and may even influence societal response (Lantis, 2009). In the case of China, cultural identity is rooted firmly in their historical experience. Specifically, this includes their notion of being the "Middle Kingdom" and the injustices experienced during the *100 Years of Humiliation*² (Lantis, 2009; Mahnken, 2011). It has been suggested that these have predisposed China toward greater risk taking in the process of reestablishing its position in the international community, from which a different interpretation of success has emerged. For their elites, success is viewed not at the operational level, but rather to the extent with which the activities have influenced the "overall situation" (Scobell, 2014). Moreover, China has placed a premium on the preservation of internal unity as this has been viewed as a source of instability that in turn may lead to outside powers to intervene with internal affairs. Finally, it has viewed war as costly and should be avoided, and victory taken with the lowest possible cost (Mahnken, 2011).

Taking these into consideration, cyberspace and cyber espionage as an expression of strategic culture becomes apparent. Firstly, how success is defined explains China's continuous use of cyber espionage despite regular disclosures. Since success is judged relative to its contribution to the overall objectives—which in this case one can assume to be China's goal of regaining its prominence in the international community—incremental success is acceptable. The case of Operation Byzantine Hades serves as an example to explain this line of reasoning. While the cyber espionage operation to obtain plans for the F-35 was disrupted, it can be assumed that enough was exfiltrated to have allowed them

to develop their own stealth technology as part of their overall goals to modernize their armed forces (Gertz, 2014). Internally, the use of cyber espionage to obtain information concerning possible dissidents (despite non-alignment with the power imbalance relationship established by realists) is justified as a means of gaining actionable intelligence to preserve internal unity. This is best seen in the case of cyber espionage campaigns aimed toward Tibetan activists. Moreover, the use of cyberspace as a platform for espionage addresses the need to avoid the costs of war for both cases. This is rooted in the challenge of attribution, which is intrinsic to cyberspace.

Since actions in cyberspace cannot be attributed with absolute certainty, this limits the degree of escalation that such actions may invite, making these potentially less costly. This was pointed out by Thomas in reference to the works of Niu Li, Li Jiangzhou, and Xu Dehui, have suggested the use of strategies that "*seize and maintain information supremacy on the basis of using clever methods to prevail at a relatively small cost in information warfare*" (T. Thomas, 2009). As such, this ability to further interests while minimizing consequences gives elites the motivation to continue to instrumentalize historical narratives while enacting policies that utilize cyberspace to further the desired goals. For China, the agent through which such policies are enacted has been the People's Liberation Army (PLA). This position is supported by the current organizational structure of the PLA and existing military doctrine. Both CrowdStrike and Mandiant have recently identified two PLA Units, 61398 and 61486, as being involved in several cyber espionage campaigns³ (CrowdStrike, 2014; Mandiant, 2013). Organizationally, both units report directly to the PLA General Staff Department that in turn is under the auspices of the Communist Party of China Military Commission. It may be reasoned that given this structure, actions by these specific units are the manifestations of elite interests. Besides this, existing military doctrine have embraced the use cyberspace for preemption, most

² Period in Chinese history where it was subjected to significant western pressure and influence that eventually saw it lose socio-political and economic power. ³ In depth analysis of these incidents are beyond the scope of this paper.

notably in form of cyber espionage. Following the ancient dictum, “a victorious army first wins then seeks battle” (T. L. Thomas, 2006).

For China, cyberspace has become a platform upon which strategic culture has wholly manifested itself as a function of the state’s national cultural identity, elite instrumentalism, and its military’s organizational culture.

MOVING FORWARD

As cyberspace becomes the foundation upon which political, economic, and military power is built upon, the need to understand the underlying factors that enable conflict in this domain is crucial. To this end, this study has presented that the phenomenon of cyber espionage may be viewed as a function of strategic culture. In doing so, it does not attempt to discredit realist or primordialist explanations but rather provides a complementary perspective through which cyber espionage may be analyzed and addressed.

While the conceptual analysis presented in this study serves as an initial foray into strategic culture’s applicability in the realm of cyberspace, further rigorous work is crucial. Scholars who intend to carry this research forward should investigate its explanatory capabilities in cases that do not necessarily exhibit the preconditions of (1) strong national cultural identity, (2) elite allegiance to tradition, and (3) strong military organizational culture. A restrictive approach such as this tests the generalizability of strategic culture and, in turn, its theoretical value for this particular domain.

REFERENCES CITED

Axelrod, R., & Iliev, R. (2013). Timing of Cyber Conflict. *Proceedings of the National Academy of Sciences of the United States of America*, 111(4), 1298–303. doi:10.1073/pnas.1322638111

CrowdStrike. (2013). *CrowdStrike Global Threat Report 2013*.

CrowdStrike. (2014). *Putter Panda CrowdStrike Intelligence Report*.

Cruz, C. (2000). Identity and Persuasion: How Nations Remember Their Pasts and Make Their Futures. *World Politics*, 52(3).

Drogin, B. (1999). Russians Seem To Be Hacking Into Pentagon / Sensitive information taken but nothing top secret. *SFGate*. Retrieved November 09, 2014, from <http://www.sfgate.com/news/article/Russians-Seem-To-Be-Hacking-Into-Pentagon-2903309.php>

Duffield, J. (1998). *World Power Forsaken: Political Culture, International Institutions, and German Security Policy after Unification* (p. 23). Stanford: Stanford University Press.

Eitelhuber, N. (2009). The Russian Bear: Russian Strategic Culture and What it Implies for the West. *Connections: The Quarterly Journal*, 6(1), 1–28.

Geers, K., Kindlund, D., Moran, N., & Rachwald, R. (2013). *World War C: Understanding Nation-State Motives Behind Today’s Advanced Cyber Attacks*.

Gertz, B. (2014). Top Gun takeover: Stolen F-35 secrets showing up in China’s stealth fighter. *Washington Times*.

Gomez, M. A. (2013). Investigating the Dynamics of Cyber Conflicts vis-a-vis Cyber Power. In *4th Cyberspace Cooperation Summit*. Palo Alto: East West Institute.

Hjortdal, M. (2011). China’s Use of Cyber Warfare : Espionage Meets Strategic Deterrence. *Journal of Strategic Security*, 4(2), 1–24.

Iasiello, E. (2013). Cyber Attack : A Dull Tool to Shape Foreign Policy. In *5th International Conference on Cyber Conflict* (pp. 451–468). Tallinn: NATO CCD COE.

Karamanian, A., & Sample, C. (2014). Cyber Espionage : A Cultural Expression. In *9th Annual Symposium on Information Assurance* (pp. 57–61). Albany.

Kuehl, D. (2009). From Cyberspace to Cyberpower: Defining the Problem. In F. Kramer, S. Starr, & L. Wentz (Eds.), *Cyberpower and National Security* (1st ed., pp. 24–42). Dulles.

Lantis, J. S. (2002). Strategic Culture and National Security Policy. *International Studies Review*, 4(3), 87–113. doi:10.1111/1521-9488.t01-1-00266

Lantis, J. S. (2009). Strategic Culture and Tailored Deterrence: Bridging the Gap between Theory and Practice. *Contemporary Security Policy*, 30(3), 467–485. doi:10.1080/13523260903326677

Legro, J. (1995). *Cooperation under Fire: Anglo-German Restraint during World War II* (p. 20). Ithaca: Cornell University Press.

Lewis, J. A. (2014). National Perceptions of Cyber Threats. *Strategic Analysis*, 38(4), 566–576. doi:10.1080/09700161.2014.918445

Libicki, M. C. (2009). Sub Rosa Cyber War. In C. Czosseck & K. Geers (Eds.), *The Virtual Battlefield: Warfare* (pp. 55–65). Amsterdam: IOS Press.

Mahnken, T. G. (2011). *Secrecy and Stratagem : Understanding Chinese Strategic Culture*.

Mandiant. (2013). *APT1: Exposing on of China’s Cyber Espionage Units*.

Nakashima, E., Miller, G., & Tate, J. (2012). U . S ., Israel developed Flame computer virus to slow Iranian nuclear efforts , officials say. *The Washington Post*. Retrieved November 09, 2014, from http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPov_story.html

Scobell, A. (2014). China’s Real Strategic Culture: A Great Wall of the Imagination. *Contemporary Security Policy*, 35(2), 211–226. doi:10.1080/13523260.2014.927677

Snyder, J. (1977). *The Soviet Strategic Culture: Implications for Nuclear Options*. Santa Monica.

Thomas, T. (2009). Nation-state Cyber Strategies: Examples from China and Russia. In F. Kramer, S. Starr, & L. Wentz (Eds.), *Cyberpower and National Security* (pp. 465–487). Washington, D.C.: National Defense University Press.

Thomas, T. L. (2006). Nation-State Cyber Strategies: Examples from China and Russia, (November).

Valeriano, B., & Maness, R. (2013). A Theory of Cyber Espionage for the Intelligence Community. In *EMC Conference on Intelligence, National Security, and War*. Newport.

AUTHOR

Miguel Alberto Gomez (mgomez@student.ibeio.org) is a graduate student currently pursuing a master's degree in international security at the Institut Barcelona d'Estudis Internacionals (IBEI) in Barcelona, Spain. Prior to this, he has been involved in the field of information assurance for the past seven years and had spent the last five teaching and conducting research in cybersecurity at the De La Salle University, Manila, Philippines. His main areas of research are cyber conflict in the South East Asian Region and norms in cyberspace.

War Against Identity Cyber Assault in a Social World

Sharon L. Burton | Dustin Bessette

ABSTRACT

Ongoing identity thefts and crimes are continuously debilitating people and causing peril for organizations. According to the U.S. Department of Justice, identity theft and identity fraud is language utilized to refer to all kinds of offenses in which an individual wrongfully attains and uses another individual's personal data in a manner involving fraud or deception, usually for financial gain. Under others' names, identity thieves are securing home loans, automobiles, motorcycles, credit cards, and securing personal loans. Over 18 financial institutions, to include but not limited to Bank of America, Wells Fargo, JP Morgan Chase and Citi, reported cyber-fraud to the Security Exchange Commission. In 1998, in an attempt to combat identity theft, the U.S. Congress passed the Identity Theft and Assumption Deterrence Act. Meanwhile, victims are left with the daunting task of correcting negative information on their credit files, and correcting other financial and/or personal information. Far too often these tasks take more time to correct than it does to commit. Identity theft and crime has created a new need for a cybersecurity educated citizenry, and new expertise in data security from the newly degreed in information security. This text reviewed information and measures that citizenry and businesses can take to protect themselves from such cybersecurity issues. Through the lens of this text, academicians and practitioners will review cyberassault case studies, examine telemarketing scams, and then learn current combative techniques of cybersecurity for protection.

INTRODUCTION

The menace of malicious software and cyber-criminals has reached all avenues of contemporary life; this malicious movement has increased the vulnerability of consumers and businesses. These vulnerabilities reach from personal tablets to laptop in homes, retailers, and medical facilities. Over 18 financial institutions, to include but not limited to Bank of America, Wells Fargo, JP Morgan Chase and Citi, reported cyber-fraud to the Security Exchange Commission. In its 14th year of operation, the Internet Crime Complaint Center disclosed that it received "262,813 consumer complaints with an adjusted dollar loss of \$781,841,611, which is a 48.8 percent increase in reported losses since 2012 (\$581,441,110)" (FBI, 2013, p. 13). Technology provides the citizenry and businesses opportunities to conduct business around the world in an anytime and anyplace manner. Domestic and international business is flourishing. Understanding what is required to protect oneself from cybercriminals is significant to self preservation. This text will uncover the meaning of identity theft, identity fraud, and exposure points.

Identity theft is stealing an individual's identity, pretending to be another person by assuming that individual's identity, generally as a technique to secure entry to resources or acquire credit and other benefits in that individual's name. According to The United States Department of Justice, identity theft is a crime (2014, para 1). Persons victimized by identity theft can experience unfavorable consequences if held accountable for the cybercriminal's behaviors. Identity theft occurs when someone uses another's personally identifying information, like their name, identifying number, social security number, bank

account numbers, credit card numbers, or other personal identification data without that person's permission, to commit fraud or other crimes (The United States Department of Justice, 2014; Federal Deposit Insurance Corporation, 2009). Another name for identity theft is identity crime (The United States Department of Justice, 2014). Protection against cybercriminals and combating digital crime can be understood as one of the five missions of the Department of Homeland Security, DHS. The missions are:

1. Prevent terrorism and enhancing security;
2. Secure and manage our borders;
3. Enforce and administer our immigration laws;
4. Safeguard and secure cyberspace;
5. Ensure resilience to disasters; (DHS, 2014, The Core Missions)

Understanding the link relating information breaches and identity theft is difficult. The difficulty lies in the identity theft victims frequently not knowing how their personal identifying data was attained. Individuals as well as companies must work to avoid becoming victims.

AVOID BECOMING A VICTIM OF IDENTITY THEFT

Hyperconnectivity, multiple means of communications, is a trend that continues to emerge and push and pull cyber security experts to, according to Dawson, Omar, Abramson, and Bessette (2014), develop new security architectures for numerous platforms such as laptops, mobile devices, as well as wearable displays. To protect the citizenry from these multiple forms of exploitation of vulnerabilities, it is critical for organizations to comprehend current and future threats. According to (Dawson, et al., 2014), the threats include the laws that drive organizations and citizens security needs.

Victimization can entail sizeable losses, as well as considerable additional financial costs. As given by Symantec (2014), cybercrime persist as an enlarging global matter. "Both the total global direct cost of cybercrime (U.S. \$113 billion; up from \$110 billion)

and the average cost per victim of cybercrime (\$298; up from \$197) increased this year" (Symantec, 2014, para 3). These costs can be associated with trying to re-establish one's character in the community and correcting incorrect information generated by the criminals. Identity theft and fraud can affect consumers in numerous ways. On the other hand, avenues exist to reduce exposure to identity hijackings and to support victims. Exposure points for review are cloud applications, computers, shopping, smart phones, social media, paying taxes, Phishing E-mails, and trash rummaging.

EXPOSURE FROM COMPUTERS

Technology is knocking down access barriers through a global effect (Oblinger, 2001). According to Marc Goodman, global security advisor and futurist, in a CNN article, "technology has made our world increasingly open, and for the most part that has huge benefits for society. Nevertheless, all of this openness may have unintended consequences (2012, para 4)." Dawson, Omar, and Abramson (2015) posited, since the 1990s, users have mis-used vulnerable access points to obtain access to networks for malicious intent. In recent years the incidents of attacks on U.S. networks continue to increase at an exponential pace; the attacks include but are not limited to malicious embedded code, and exploitation of backdoors (Dawson et al. 2014). Computer cyber terrorism is occurring internationally from computer users employing veiled Internet Protocol (IP) addresses. Malicious software applications are being used to affect computers and gather identifiable information.

Cyber criminals send disguised messages from what they believe to be companies in that people conduct business. The intent is to gather personal data about the individual and the account, and then exploit the account and or the person. Adding to the capability of cybercriminals to exploit data is Internet users' lack of knowledge regarding basic computer security. See Figure 1 under phishing e-mails for an example of a masked message sent by cyber criminals with malicious intent.

EXPOSURE THROUGH ONLINE BANKING

Online banking users may like the convenience of conducting business through desktop computers and handheld technology (i.e., tablets, phablets, smartphones, ipods); however, conducting such business allows for intrusion of personal identifying information. To protect sensitive data (i.e., credit card numbers, social security numbers, date of birth, passwords) users should consider using sites with the prefix, <https://> (Hypertext Transfer Protocol Secure), as opposed to <http://> (Hypertext Transfer Protocol). Passwords should not be saved on sites with sensitive information.

EXPOSURE THROUGH SHOPPING

Numerous stores of the Supervalu supermarket chain (i.e., Acme, Albertson's, Jewel-Osco, Shaw's), and retail chains (i.e., The Home Depot, Target, Neiman Marcus) have reported cyber-fraud. Cybercriminal installed malware into areas of the computer network that processes payment card transactions. Even though malware can be removed, while it is in place, this malware captures sensitive data that can possibly destroy lives and operations. Shoppers should remain aware of this type of cybercrime.

The Supervalu supermarket chain revealed a second breach of customer data on September 30, 2014; up to 21 states could be affected (Roman, 2014). The breach occurred through point-of-sale systems. According to the Sept 30, 2014 article, Supervalu experienced two separate hacks, the first one was August 2014, and the second one September 2014. Customers of the supermarket giant are being offered one year of identity theft protection services (Roman, 2014).

The Home Depot (2014) noted a September 8, 2014 cyber security data breach to its website. This home improvement, a major home improvement chain, provided that malware could possibly impact its customers who utilized payment cards (i.e., debit cards, credit cards) at U.S. and Canadian stores from April

to September (Home Depot, 2014). As given by Cresswell and Perlroth (2014), several Home Depot ex-employees stated the major home improvement chain consistently left its data exposed. The Home Depot is noted to have been warned as far back as 2008 that it needed to better secure its data. Further stated by Cresswell and Perlroth (2014), the Home Depot breach is the largest in the history of retail; the breach compromised 56 million customers' payment cards. According to an article by Sunshine (2014), the malware that placed Target's cash registers at risk, was altered and became a new variation for the Home Depot attack.

In 2013 Target had a massive data breach, which enabled the pilferage of debit and credit card data from Target's cash registers. This data breach compromised millions of Target's customers' credit and debit card data (Sharf, 2014). On the words of Jameison and McClam (2013), the number of customers affected by the Target data breach was as many as 40 million, during three weeks of the holiday season for shopping. Target's breach, considered one of the largest breaches, places Target in the company of Home Depot in regards to securing its customers' data. According to Kash, in an Information Week Government article, hackers gained access to Target's point-of sale system by manipulating the IT system of a vendor (2014, para 1). According to Sharf (2014), Target's shares sank to \$58 per share due to the malware attack, and sales decreased.

Each business posited that the malware was definitely removed from their networks. This cyber exposure in retail, not only hurts consumers in regards to the costs of protecting their identity, the exposure could result in possible higher prices through retailers attempting to recoup losses. Shoppers must think in different terms regarding shopping and remain vigilant of the locations that are repeatedly victims of cybercrimes. Customers have to remain accountable, as well as hold retailers accountable for securing their data.

EXPOSURE THROUGH SMARTPHONES

Consumers should understand that mobile applications rely upon browsers to operate (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2013). With this said, smart phones are susceptible to cyber attacks. On Oct 2, 2014, the Providence Journal reported that SnoopWall cybersecurity experts, a counterintelligence security software company, announced a consumer protection advisory for consumers to remove flashlight applications from their mobile devices. The Providence Journal noted that SnoopWall's cybersecurity experts provided that "all flashlight app users are being spied on and warn that flashlight apps should be considered well designed 'malware.'" According to Campbell (2009), cybercriminals assembled the first phone botnet "...after an SMS worm called "Sexy Space." Users clicking on a message link had software installed on their mobile phones able to connect with a central server, thus making it feasible for the users' mobile phones to be controlled remotely by a third party (Campbell, 2009).

As documented in the Emerging Cyber Threats reports 2013, smartphones, as well as other mobile devices are tremendous avenues to house and proliferate malware (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2013). Security software is available for mobile devices. According to Wright, Dawson Jr., and Omar (2012), 96% of the mobile devices are not protected by security software. This malware message should sound an alarm for mobile phone users. Smart phone users can take steps to secure their devices. These steps include but are not limited to backing up data, using screen locks installing location tracking on the device, and installing a researched security application. Software infections and scams are on the rise. It is important to protect sensitive data on mobile devices.

EXPOSURE THROUGH SOCIAL MEDIA

Social media has transformed the communications industry. This change affects the manner in that people socialize and conduct business transactions. This form of communication allows unparalleled access to

others' lives. On the contrary, a disadvantage exists as social media can permit access to unwanted "friends" who mean to do individuals or their businesses harm.

Users actively search sites such as Facebook and LinkedIn. Such media sites are targets for hackers. According to Kerner (2013a), Facebook armed itself to fight cybercriminals by using a "bug-bounty program that rewards researchers for properly disclosing flaws" (Kerner, 2013a, para. 6). Kerner (2014b) further disclosed that LinkedIn moved to a more secure log-in measure by transitioning the site to <https://>. Social media users are advised to review with suspicion social media requests from unknown persons. Request could include but not be limited to a person using information from their social media profile to contact them and then pretend to be businesses needing information to process orders, refunds, or send prizes.

EXPOSURE THROUGH GOVERNMENT SYSTEMS

Government systems are not out of reach of cyber criminals. According to the U.S. Government Accountability Office (GAO) (2013, para 1), not only government agencies, but country's essential "infrastructures-such as power distribution, water supply, telecommunications, and emergency services have become increasingly dependent on computerized information systems and electronic data to carry out operations and to process, maintain, and report essential information" (para 1). The GAO's has maintained a Federal information security list of high-risk areas since 1997; in 2003, GAO expanded this high-risk area to include cyber CIP. Risks to information and communication systems include insider threats from disaffected or careless employees and business partners, escalating and emerging threats from around the globe, the ease of obtaining and using hacking tools, the steady advance in the sophistication of attack technology, and the emergence of new and more destructive attacks.

Tax payers are being caught up in this cyber scam by cyber criminals. A taxpayer stated that he completed his federal taxes to later be told that his taxes had

been filed previously. A hacker used his personal identifying information to file taxes in his name for two years. The issue has been resolved; however, not without many hours of work and research.

The government is serious about cyber security. Because of development in the accessibility and complexity of malware and the reality that additional technologies escalate new security concerns, the United States of America's infrastructure is confronted with a mounting cyber threat (FBI, 2014). The U. S. government has taken key steps. According to Hewlett-Packard (HP) Development Company site, on February 26, 2014, HP announced the company was awarded a cybersecurity contract worth up to \$32.4 million by the department of Homeland security (DHS). The FBI (2014) provided that it is "concerned about the proliferation of malicious techniques that could degrade, disrupt, or destroy critical infrastructure."

The key take-a-way for consumers is to be cognizant of the usage of their personal identifying information. Consistently review their personal histories to be sure they are not being impersonated. Consumers should have a general understanding of how the government is working to protect their information from cybercrime attacks.

EXPOSURE THROUGH PHISHING E-MAILS

Phishing emails are unsolicited e-mails supposedly from a genuine source attempting to trick individuals into revealing personal data. Such sources include but are not limited to credit unions, banks, telephone companies, Internet Service Providers, utility companies, frequently shopped merchants, and government agencies. Figure 1 is an example of a phishing e-mail.

Dear Customer,

Due to concerns, for the safety and integrity of the Langley Federal Credit Union Online we have issued this warning message.

It has come to our attention that your Langley Federal Credit Union Online Banking information needs to be updated as part of our continuing commitment to protect your account for year 2014 and to reduce the instance of fraud on our website. If you could please take 3-5 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

Once you have updated your account records your Langley Federal Credit Union Online service will not be interrupted and will continue as normal.

Please visit www.langleyfcu.org and start the update process.

Your security is important to us. If you are not aware of this situation, please contact us immediately.

This alert relates to your Online Banking profile, rather than a particular account. The account listed here is for verification purposes only.

Thank you.
We apologize for any inconvenience.

Langley Federal Credit Union | About Us | Accessibility | Careers | Privacy
Policy | Security | Terms of Use



EQUAL HOUSING LENDER
Member FDIC

FIGURE 1: FRAUD NOTICE

EXPOSURE THROUGH DUMPSTER DIVING AND TRASH RUMMAGING

Dumpster diving and trash rummaging is another opportunity to gather key information to steal identities. In the late 90s, Stephen Massey, one of the most tarnished identity ring theft leaders, located unprotected sensitive data in a dumpster and began a career of identity theft (Ledford, 2008). After the major violation of personal security by Massey and his gang, legislation was enacted such as the Identity Theft and Assumption Deterrence Act of 1998, and or the Personal Information Protection and Electronic Documents Act. This legislation pushed companies to be better stewards regarding storage and disposal of personal data.

CONCLUSION

Identity thefts and identity crimes are the fastest growing crimes in the county. Despite the statistics, according to IC3 2013 report, the true number of Internet crime reports remains unknown (FBI, 2013). According to Filshtinskiy (2013), computer crimes are now a business analogous in size to weapons and drug trafficking. February 2014, the Obama administration released recommendations outlining a voluntary national cyber security practices (Jackson, 2014).

Consumers must become and remain cognizant of how to protect themselves from identity thefts and crimes. Protection can occur in the forms of credit monitoring services, covering pin numbers when entering them, reviewing statements consistently, use the https with URLs, protecting personal identifying information, and never click unknown sites.

Credit monitoring services allow individuals to check their credit on a regular basis, and to protect their identities. These services offer diverse benefits such as unlimited access to credit reports and scores, receiving alerts when credit scores increase or decrease, a monetary value of protection against crimes, identity theft protection, access to working with identity thefts protection specialists, blocking fraudulent activities, and monitoring of account activities. The benefit of using a credit monitoring

service is that the service allows individuals to maintain a vigilant watch on their credit and identities. It is important to review the benefits of a service before engaging with the service. Protecting pins numbers is another protection method.

Always cover terminals before entering pin numbers of cards and accounts. Covering the terminals prevents others from seeing the numbers. Also, covering the terminals prevents others from recording your entering the number(s). Do not share pin numbers with others, whether the requests are written, through email, telephone, or in-person. Further, do not use numbers that can be easily guessed such as birthdays, addresses, anniversary dates, and sequential numbers like '4567'. Another protection method is consistently reviewing statements.

Reviewing credit card and bank statements on a regular basis is important. Constant monitoring allows detection of purchases not made by account owners. Reviewers should verify that their payments were properly posted to accounts. Other statement points to monitor are fees, interest rates, and payment due dates. Each of these key points protects consumers against potential long term problems. Next is accessing web sites through a safer method.

Use `Https://` prefix before entering web addresses. This Hypertext Transfer Protocol Secure prefix is an arrangement of the Hypertext Transfer Protocol with the SSL/TLS protocol to deliver encrypted messaging. Also, the prefix secures identification of a network web server. When making payments and inputting sensitive data, ensure the https prefix HTTPS is in use.

Next is protecting personal identifiable data. Cybercriminal can gain access to your pictures through social media, and if they have other personal data, these criminals can wreak havoc on the lives of consumers. Never place social security numbers, driver's license numbers, and other similar data in unprotected places. Never state such numbers in a voice tone, which can be heard by non- intended hearers. Keep such numbers protected. Last is never clicking unknown sites.

Clicking unknown sites can open a computer to viruses. These viruses can be used to steal sensitive data from computers. Such theft can occur without the owners' knowledge. Always maintain current anti-virus, anti-spyware, and anti-adware software. Secure your wireless system. Turn off your wireless network when it is not in use.

Identify thefts and crimes are continuously debilitating people and causing hazards for organizations. Protecting personal identifiable information, and Internet systems are very important measures. Once cybercrimes occur, they can take a very long time to rectify. During these times, the victims could be forced to pay thousands of dollars to regain their identities. Organizations could pay extraordinary sums to regain their reputations and protect affected consumers. The popularization of the Internet has provided an avenue for identity theft and crime. Because of this new wave of crime, a need exists for this type of education on cybersecurity and an educated citizenry.

REFERENCES

- Campbell, M. (2009). Mobile botnets show their disruptive potential. *New Scientist*, 204(2734), 26.
- Consumer Digital Privacy Protection Advisory: Top Mobile Flashlight Applications Spy on Users, Warn SnoopWall Cybersecurity Experts. (2014, October 2). *Providence Journal*. Retrieved from <http://www.providencejournal.com/business/press-releases/20141002-consumer-digital-privacy-protection-advisory-top-mobile-flashlight-applications-spy-on-users-warn-snoopwall-cybersecurity-experts.ece>
- Cresswell, J., & Perlroth, N. (2014, September 19). Ex-employees say home depot left data vulnerable. *Technology*. Retrieved from http://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html?_r=0
- Dawson Jr., M. E., Omar, M., and Abramson, J. (2015). Understanding the methods behind cyber terrorism. *Encyclopedia of Information Science and Technology* (3rd ed). Ed. Mehdi Khosrow-Pour. Hershey: Information Science Reference, 1539–1549. Available at: http://works.bepress.com/maurice_dawson/23
- Dawson, M. E., Omar, M., Abramson, J., and Bessette, D. (2014). The future of national and international security on the Internet. *Information Security in Diverse Computing Environments*. Hershey: Information Science Reference, 2014. 149–178. Available at: http://works.bepress.com/maurice_dawson/24
- Department of Homeland Security (2014). The Core Missions. Retrieved from <http://www.dhs.gov/our-mission>
- Federal Bureau of Investigation. (2014). Cyber threats to U.S. critical infrastructure. Federal Bureau of Investigation. Retrieved from <http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism>
- Federal Bureau of Investigation. (2013). 2013 Internet crime report. Federal Bureau of Investigation. Retrieved from http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf
- Federal Deposit Insurance Corporation (2009). *Identity theft*. Retrieved from <https://www.fdic.gov/consumers/consumer/alerts/theft.html>
- Filshinskiy, S. (2013). Cybercrime, cyberweapons, cyber wars: Is there too much of it in the air?. *Communications of The ACM*, 56(6), 28–30. doi:10.1145/2461256.2461266
- Goodman, M. (2012, July, 29). How technology makes us vulnerable. *CNNOpinion*. Retrieved from <http://www.cnn.com/2012/07/29/opinion/goodman-ted-crime/>
- Hewlett-Packard Company. (2014, February 26). HP Awarded \$32.4 million cybersecurity contract by U.S. Department of Homeland Security. Retrieved from <http://www8.hp.com/us/en/hp-news/press-release.html?id=1590576>
- Jackson, W. (2014, February 12). Feds launch cyber security guidelines for us infrastructure providers. *InformationWeek Government*. Retrieved from <http://www.informationweek.com/government/cybersecurity/feds-launch-cyber-security-guidelines-for-us-infrastructure-providers/d/d-id/1113816>
- Jameison, A., & McClam, C. (2013, December 19). Millions of Target customers' credit, debit card accounts may be hit by data breach. *NBC News*. Retrieved from <http://www.nbcnews.com/business/consumer/millions-target-customers-credit-debit-card-accounts-may-be-hit-f2D11775203>
- Kash, W. (2014, May 15). Retail breaches bolster interest in NIST cyber security advice. *InformationWeek Government*. Retrieved from <http://www.informationweek.com/government/cybersecurity/retail-breaches-bolster-interest-in-nist-cyber-security-advice/d/d-id/1252740>
- Kerner, S. (2014b, June 18). LinkedIn disagrees with researcher that SSL glitch puts it at risk. *Eweek*, 5.
- Kerner, S. (2013a, August 13). Facebook vs. hackers: Win one, lose one. *Eweek*, 3.
- Ledford, J. (2008). Identity theft waiting to happen: Dumpster diving: identity theft 101. *AccuShred LLC* 4(5). Retrieved from http://www.imakenews.com/accushred/e_article001190083.cfm?x=b11,0,w
- Oblinger, D. (2001). The world is getting smaller, but we are seeing farther. *Educause*. Retrieved from <https://net.educause.edu/ir/library/pdf/erm0145.pdf>
- Roman, J. (2014, December 30). Top data breaches of 2014. *Infographic: Lessons Learned from Year's Top Incidents*. <http://www.databreachtoday.com/top-data-breaches-2014-a-7736>
- Sharf, S. (2014, August 5). Target shares tumble as retailer reveals cost of data breach. *Investing*. Retrieved from <http://www.forbes.com/sites/samanthasharf/2014/08/05/target-shares-tumble-as-retailer-reveals-cost-of-data-breach/>
- Sunshine, A. L. (2014, September 14). Home Depot hit by same malware as Target. *KrebsOnSecurity*. Retrieved from <http://krebsonsecurity.com/tag/target-data-breach/>

Symantec (2014). 2013 Norton Report. Retrieved from http://www.symantec.com/aboutnews/resources/press_kits/detail.jsp?pkid=norton-report-2013

The Home Depot. (2014). Customer update on payment breach. *The Home Depot*. Retrieved from https://corporate.homedepot.com/MediaCenter/Pages/Statement1.aspx?cm_mmc=SEM|THD|Test&mid=syNdpcEtb|dc_mtld_8903qmu25195_pcrld_46105304283_pkw_%2Bhome%20%2Bdepot%20security%20data%20breach_pmt_b&gclid=CML21PCuicECFcRrAMgodHmAaww

The United States department of Justice (2014). *What are identity theft and identity fraud?* Retrieved from <http://www.justice.gov/criminal/fraud/websites/idtheft.html>

Traynor, P., Ahamad, M., Alperovitch, D., Conti, G., & Davis, J. (2013). Emerging cyber threats report 2013. Georgia Technical Institute of Technology, Georgia Tech Information Security Center. Retrieved from https://www.gtisc.gatech.edu/pdf/Threats_Report_2013.pdf

U. S. Government Accountability Office. (2013). Protecting the federal government's information systems and nation's cyber critical infrastructures. U. S. Government Accountability Office. Retrieved from http://www.gao.gov/highrisk/protecting_the_federal_government_information_systems/why_did_study

Wright, J., Dawson Jr, M. E., & Omar, M. (2012). Cyber security and mobile threats: The need for antivirus applications for smartphones. *Journal of Information Systems Technology & Technology* 5(14), p. 40-60).

AUTHORS

Sharon L. Burton (sharonlburton2@comcast.net), DBA, MBA-HRM, MBA-Mgmt, HCS, SWP, is a chief learning officer, in municipal government, and leads publishing initiatives for American Meridian University. Also, she serves as an adjunct professor. Her publications are in the areas of cybersecurity, andragogy (adult learning), quality systems management, diversity and inclusion, quality customer service, and learning and development. She has over 32 peer reviewed publications that include book journal articles and a book chapter.

Dustin Ivan Bessette (bessette64@yahoo.com), MBA-MKT/ADV, CIG, is a program manager/coordinator for American Meridian University as well as a park ranger for Oregon Parks & Recreation Department. A majority of his publications are in the areas of online education, pedagogy, andragogy, cybersecurity, quality systems management, leadership, marketing, and parks and recreation. He has over 54 different peer-reviewed and double blind publications that include journal articles, book chapters, and conference proceedings.

Regulation of Cybersecurity in the Financial Sector: Now Modeled on the Emergency Preparedness Cycle

Ken Lerner | Matthew Berry

ABSTRACT

The digitalization of money has led to convenience, efficiency, and speed for financial transactions, and tremendous growth in the financial industry. The increasing reliance of the financial services sector on information technology has led to a host of concerns over risks to individual account holders, businesses, and the financial system itself. To protect markets and consumers, a number of federal agencies have entered the field of regulating cybersecurity in the financial sector. Apart from regulatory requirements, there are also a number of good-practice guides and industry standards addressing cybersecurity in the financial sector. However, the dynamic and fluid nature of the cybersecurity world has required a different approach than in the past: rigid standards and requirements won't work, so the move has been made to a continuous cycle of threat assessment, security development, testing, and evaluation. This model of continuous improvement is familiar in the emergency management world, where a similar process is followed in keeping current on disaster preparedness. It also has roots in the disciplines of problem solving and project management. Similar to preparing for a flood or a new virus or a hazardous materials spill, a continuous process of analysis, updates, testing, and refinement is the best way to keep up.

The submitted manuscript has been created by UChicago Argonne LLC, operator of Argonne National Laboratory ("Argonne"). Argonne, a U.S. Department of Energy Office of Science laboratory, is operated under Contract No. DE-AC02-06CH11357. The U.S. government retains for itself, and others acting on its behalf, a paid-up nonexclusive, irrevocable world-wide license in said article to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government.

INTRODUCTION

An 18th-century English hymn intones, "God moves in a mysterious way" (Cowper, 1773). In the 21st century, it seems the same could be said about money. Freed from the constraints of metal coins or printed paper, money primarily exists as a digital representation of value, a set of numbers in a financial institution's computer. Transactions take place electronically, ranging from a card swipe or phone scan for an ordinary retail purchase to high-speed trading of massive blocks of stocks, bonds, currency, and other commodities.

The transition to a digitalized financial infrastructure has created both new opportunities and new hazards. The rate of change has accelerated. In light of these developments, one may wonder whether the traditionally slow wheels of government have

kept up. How are these new marketplaces regulated and are the regulations suited to addressing the new hazard landscape?

For decades, multiple agencies at the federal and state level have promulgated regulations with the goal of reducing risk to individuals' savings and ensuring transparency in the investment market. Regulations within the financial services industry have been largely in reaction to crises (Whitehead, 2010). Cybersecurity threats to the financial services sector have yet to reach crisis proportions. However, the digitization of finance has offered a glimpse at the potential for consequences should a disruption occur. The technological evolution of the financial services industry has resulted in an alteration of the operational risk landscape.

Currently there is a flurry of quasi-regulatory activity related to cybersecurity threats to the financial services industry. This activity is in response to an evolving threat landscape that includes increased targeting of financial services entities (OCC, 2014). The Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA), a government agency and independent regulator, are leveraging current regulations to address cybersecurity risk. First, officials from the SEC signaled that cybersecurity risk "must be considered as part of board's overall risk oversight" (Aguilar, 2014). This has been interpreted to mean that cyber risk represents "a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant" (SEC, 2011) and therefore should be disclosed (Ferrillo, 2014). Second, the SEC Office of Compliance and FINRA announced that they would be adding cybersecurity preparedness to their examinations (SEC, 2014; FINRA, 2014).

Directions from the White House are setting the stage for the next level actions to promote cybersecurity. In 2013 President Obama signed Executive Order 13636—*Improving Critical Infrastructure Cybersecurity*. The pillars of EO 13636 were a framework for cybersecurity through the National Institute for Standards and Technology (NIST) and a call for greater information sharing between

government and the private sector. Additional policies to promote information sharing are the subject of a February 2015 Executive Order, *Promoting Private Sector Cybersecurity Information Sharing* (Obama, 2015).¹

Digitization of Finance and Attendant Risks

The digitalization of money has led to convenience, efficiency, and speed for financial transactions, and tremendous growth in the financial industry. At its peak in 2006, the financial services sector contributed 8.3 percent to U.S. Gross Domestic Product (GDP), compared to 4.9 percent in 1980 and 2.8 percent in 1950 (Greenwood and Scharfstein, 2013). Algorithmic trading firms—a new breed of financial services firm that specializes in leveraging a combination of high-speed communications, high-speed computing and mathematical advances to implement trading strategies—grew from 30 percent of total trading volume in 2005 to 70 percent in 2009 (Clark, 2010). Sustaining the growth of the modern financial services industry is a complex system of information technology and communications networks (Gorman et. al 2004; McAndrews & Stefanadis, 2000). Commercial and investment banks and financial services firms rely on financial infrastructure networks to support core activities including payments, trading, clearing, and custody activities (Payments Risk Committee, 2007).

The increasing reliance of the financial services sector on information technology has led to a host of concerns over risks to individual account holders, businesses, and the financial system itself. Motives for cyber penetration range from ordinary greed to terrorism to the simple thrill of hacking. Concerns at the individual and business level include financial privacy, protection against fraud and theft, integrity of data, and the threat of cyber attack for economic or political reasons.

Systemic risk refers to the concern that a problem or defect in networks supporting one financial market, "can have a domino effect on another network resulting in a cascading series of defaults and

¹ See fact sheet at <https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari>.

failures, even across markets, regions or globally” (Payments Risk Committee, 2007, Sec. 3.11); or put another way, it refers to the possibility of market-wide instability or collapse. Two criteria characterize systemic risks to the financial services sector: contagion effect and degree of loss. Contagion refers to the transmissibility of a risk to the rest of the system. Degree of loss refers to the potential loss relative to the victim institution’s overall capitalization (Lemieux, 2003).

The potential costs of security failures and market disruptions are substantial, as demonstrated by recent incidents. In late 2013 in the midst of the holiday shopping season, news broke that the Target department store chain had suffered a security breach affecting customer credit card data; profits for that quarter were down over \$400 million, including \$61 million in direct costs from the breach (partly offset by insurance) and a drop in sales (Marketwatch.com, 2014). Four months later, the company was still working to recover reputation and customer loyalty (Cheng, 2014). Estimates of the cost to Sony Corp. due to a hacking incident in late 2014 range around \$100 million. As reported by Reuters, “Major costs for the attack by unidentified hackers include the investigation into what happened, computer repair or replacement, and steps to prevent a future attack. Lost productivity while operations were disrupted will add to the price tag” (Richwine, 2014). Reputational damage and loss of confidential information, while difficult to quantify, may add to the total loss to the corporation.

On the systemic level, an accidental occurrence in 2010 hints at the possibilities for costly disruption. On May 6th of that year, trading on the New York Stock Exchange was disrupted by an unexpected combination of algorithmic computerized trading. During the resulting “flash crash,” major equity indices dropped in minutes to values more than 9% below the previous day’s close, then for the most part rebounded almost as quickly. The entire episode lasted less than 30 minutes, but during that brief time the Dow Jones index dropped almost a thousand points, and about \$1 trillion in equity was temporarily lost (CFTC/SEC Staff Report, 2010; Rooney, 2010).

Federal Efforts to Control Financial Sector Risk

The federal government has long sought to manage financial sector risk of all kinds, through a series of statutory and regulatory requirements and guidelines. Standards, auditing rules, and enforcement agencies and processes were created, often in response to financial crises such as the Great Depression or the savings and loan collapse of the 1980s. A welter of regulatory agencies, standards, guidelines, and handbooks are now applied to oversight of the financial sector (Appendix A contains an overview of the various agencies and their authorities). They employ traditional regulatory techniques such as standards (minimum reserve requirements for banks, for example), licensing, and required disclosures.

The new threat posed by cyber disruptions has forced adoption of a different approach, focusing on processes and practices rather than specific behavioral rules or numeric standards. In this model, the process is a continuous cycle of threat assessment, development of preparedness measures, testing and exercising, and integration of lessons learned (Payments Risk Committee, 2013).

The Emergency Preparedness Cycle

Emergency management agencies at the local, state, and federal level (and the private sector) are responsible for dealing effectively with emergencies and disasters such as earthquakes, hurricanes, wildfires, floods, hazardous chemical spills, and terrorist attacks. Borrowing from project-management paradigms, best practices in the emergency management field have come to include a “preparedness cycle” that incorporates a concept of continual improvement through a succession of hazard assessment; planning and equipment acquisition; exercises and testing; and application of lessons learned. This cycle is presented in Federal Emergency Management Agency (FEMA) guidance and elsewhere in emergency management literature.

Parallels Between the Cybersecurity and Emergency Preparedness Cycle

Cybersecurity and emergency preparedness staff face a common situation: a changing threat environment, and a continuing evolution of best practices for preventing or responding to disruptions. This has led to similar emphasis on a continual update cycle.

This article surveys the authorities, standards, and guidance on cybersecurity in the financial services industry, and the process-oriented cybersecurity model that is emerging. It then describes the parallel process used in emergency management, where best practice requires a continual cycle of threat analysis, planning, exercising, and incorporation of lessons learned. Lastly, the article identifies the common features of these two protective systems and argues that they have converged on a similar management solution.

FINANCIAL SECTOR CYBERSECURITY REGULATION AND STANDARDS

There is a long history of regulation in the financial services sector. Most of it is directed at ensuring the financial soundness of banks and other savings institutions, fair treatment of investors, and transparency of markets, along with the larger value of ensuring adequate money supply to the economy. Cybersecurity and resilience are relatively new issues and are addressed partly in regulation and partly in industry guidelines. This section summarizes key federal regulations and industry guidelines and briefly discusses other legal mechanisms that may force compliance with cybersecurity standards.

Data Security Protection Under the Gramm-Leach-Bliley Act of 1999 (GLBA)

The GLBA requires financial institutions to safeguard the security and confidentiality of customer information. Through GLBA, Congress directed regulatory agencies to implement:

Appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer (GLBA 1999).

GLBA delegated authority to a wide variety of regulators to address various segments of the financial industry, (CRS, 2014)² and the different agencies issued regulations (CFPB, 2011).³ The regulations primarily address subjects such as disclosure of personal information and explanation of privacy rights to customers. However, the regulations also address good practices that may offer general protection against penetration of financial institutions' data systems.

² As noted in CRS Report RS 20185, *Privacy Protection for Customer Financial Information* (January 2014), GLBA delegated authority to the federal banking regulators: the Office of the Comptroller of the Currency (national banks); the Office of Thrift Supervision (federal savings associations and state-chartered savings associations insured by the Federal Deposit Insurance Corporation (FDIC)); the Board of Governors of the Federal Reserve System (state-chartered banks which are members of the Federal Reserve System); FDIC (state-chartered banks which are not members of the Federal Reserve System, but which have FDIC deposit insurance); and the National Credit Union Administration (federal and federally insured credit unions). Also included is the Securities and Exchange Commission (brokers and dealers, investment companies, and investment advisors). 15 U.S.C. §6805(a) (1)-(5). For insurance companies, state insurance regulators are authorized to issue regulations implementing the GLBA privacy provisions. 15 U.S.C. §6805(a)(6). For all other "financial institutions," the Federal Trade Commission was provided authority to issue rules implementing the privacy provisions of GLBA. 15 U.S.C. §6805(a)(7).

³ Under Dodd-Frank, the CFPB has inherited some of these responsibilities, and has issued consolidated regulations for interim use regarding privacy notices. 12 C.F.R. Part 1016 (CFPB's Regulation P). 76 Federal Register 79025 (December 21, 2011).

FFIEC IT Examination Handbook – Data Security

The Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook, actually a series of booklets, guides bank examiners from several agencies: the Federal Reserve Board (FRB or Fed), Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), Office of Comptroller of the Currency (OCC), and Office of Thrift Supervision (OTS). (See Appendix A for brief descriptions of these agencies.) As such it applies to a wide variety of banks, thrift institutions, credit unions, and their IT and telecommunications providers.

The Information Security booklet (FFIEC 2006) addresses implementation of the GLBA data protection requirements and provides a detailed checklist of measures to take. It is organized around a five-step process:

- *Risk Assessment.* A process to identify and assess threats, vulnerabilities, attacks, probabilities of occurrence, and outcomes.
- *Security Strategy.* A plan to mitigate risk that integrates technology, policies, procedures, and training. The plan should be reviewed and approved by the board of directors.
- *Security Controls Implementation.* Acquisition and operation of technology, specific assignment of duties and responsibilities to managers and staff, deployment of risk-appropriate controls, and assurance that management and staff understand their responsibilities and have the knowledge, skills, and motivation necessary to fulfill their duties.
- *Security Monitoring.* The use of various methodologies to gain assurance that risks are appropriately assessed and mitigated. These methodologies should verify that significant controls are effective and performing as intended.
- *Security Process Monitoring and Updating.* The process of continuously gathering and analyzing information regarding new threats and

vulnerabilities, actual attacks on the institution or others combined with the effectiveness of the existing security controls. This information is used to update the risk assessment, strategy, and controls. Security risk variables include threats, vulnerabilities, attack techniques, expected frequency of attacks, financial institution operations and technology, and the financial institution's defensive posture.

Rules for Swap Data Repositories

A Swap Data Repository (SDR) collects and maintains records for over-the-counter derivatives sales sent to it by a reporting entity, typically a derivatives clearinghouse, and may itself purchase derivatives. It is not considered a bank. The Commodity Futures Trading Commission (CFTC) recently estimated the notional value of the swaps market at about \$390 trillion (Ackerman, 2013).

The CFTC has issued regulations governing data protection and business continuity planning at SDRs. These regulations implement portions of the Dodd-Frank Act. They address financial-industry systemic risk, in part, by requiring backup and continuity of operations capabilities for SDRs (Gensler, 2011). Telecommunications is specifically included as one of the critical supporting infrastructures that should be accounted for in business continuity plans.

The CFTC rules (17 CFR § 49.24) include requirements to:

- Perform risk analysis and develop a plan to manage risk to data.
- Maintain backup facilities and emergency/business continuity plans for timely recovery of operations. The goal for SDRs designated as “critical” by the CFTC is same-day recovery of operations; noncritical SDRs should plan to be operational by the next day.
- Apply best practices to data security.
- Notify the CFTC of malfunctions, incidents, or threats.

- Provide copies of plans and procedures to the CFTC upon request.
- Conduct periodic testing of systems and recovery capabilities, and keep records of test results.
- Coordinate planning and testing with customers and service providers.

Rules for Alternative Trading Systems

Alternative trading systems (ATSs) provide a market place for purchasers and sellers of securities that are an alternative to using a traditional stock exchange. They can be used to trade large blocks of securities at low cost and without affecting prices on the exchanges. Operation of an ATS must be approved by the SEC. The SEC has promulgated rules for ATSs that, among other things, require them to: (17 CFR § 242.301)

- Ensure their automated systems have adequate capacity to handle expected trading volumes.
- Review system vulnerability to internal and external threats.
- Establish contingency and disaster-recovery plans.
- Obtain independent review of the above systems annually.
- Report significant outages to the SEC.
- Establish safeguards and procedures to protect subscribers' confidential trading information.

Federal Government Data Protection Rules Applicable to the Federal Reserve System

The Federal Information Security Management Act of 2002 (FISMA) created a security framework for federal information systems, with an emphasis on risk management, and gave specific responsibilities to the Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), and each federal agency (CRS, 2013). The Federal Reserve Board and many of the Federal Reserve Bank activities are subject to FISMA requirements (FRB, 2005).⁴ FISMA requires that each agency develop and implement an agency-wide information security program that includes:

- Conducting periodic risk assessments;
- Developing security plans;
- Establishing minimum security configuration requirements;
- Providing security awareness training;
- Conducting periodic control testing;
- Establishing procedures for detecting, reporting, and responding to security incidents; and
- Developing a process for planning, implementing, evaluating, and documenting remedial actions to address deficiencies.

⁴ As noted in a September 2005 Federal Reserve Board Office of Inspector General report, "Because the Federal Reserve Banks (Reserve Banks) are not Federal agencies as defined in FISMA, they are not directly subject to the legislation. However, the Reserve Banks perform functions on behalf of, or under delegated authority from, the Board, the U.S. Department of the Treasury (Treasury), and other federal agencies. For example, the Reserve Banks act under delegated authority from the Board to examine and supervise bank holding companies, state member banks, and all international banks and facilities located in the United States. The Reserve Banks also act as fiscal agents for the Treasury in the issuance and redemption of U.S. government securities and as repositories for federal tax payments. In performing these functions, the Reserve Banks collect or maintain information and use or operate information systems on behalf of these agencies. This information and these information systems are therefore subject to FISMA's requirements."

Other Obligations and Standards Affecting Financial Sector Cybersecurity

Apart from federal statutory and regulatory standards, firms in the financial sector may face cybersecurity requirements that derive from common-law duties and from industry standards combined with contractual obligations.

Common-Law Duties. Failure to adequately protect data may constitute a breach of duty, subjecting a firm to civil lawsuit by those who are harmed. Legal commentators and a few cases have supported this view (Smedinghoff, 2008). Compliance with applicable standards could constitute a defense in such lawsuits.

Industry Standards/Contractual Obligations. Standards adopted within the industry may have considerable power to influence security practices. Firms wishing to participate in networks essential for conducting business must promise (through contractual obligation) to adopt the practices specified in the standard. For example, merchants must accept the Payment Card Industry Data Security Standard in order to take credit card payments. As noted above, brokers doing business through the major stock exchanges (NYSE and NASDAQ) must agree to standards and oversight administered by FINRA. Lastly, ISO/IEC 27000-series standards address information security management controls and practices. A revised standard 27001 (Information Security Management System) was published in September 2013 (ISO, 2013). Certification to this standard may be referenced in business contracts.

EMERGENCY PREPAREDNESS CYCLE

Modern emergency management practice establishes a cycle of continuous analysis, planning, testing, evaluation, and improvement. The cyclic approach is reflected in FEMA CPG 101, FEMA's main guide for state and local governments, and is also found in emergency management textbooks and as applied practice in diverse jurisdictions. This section provides a brief description of the emergency

preparedness process and notes the origins of the cyclical approach in doctrines of project management and problem-solving.

Examples of Cyclical Method in Emergency Preparation

Comprehensive Preparedness Guide (CPG) 101 is FEMA's basic guide to emergency planning. As stated in the cover letter from the FEMA Administrator, "CPG 101 is the foundation for state, territorial, tribal, and local emergency planning in the United States. Planners in other disciplines, organizations, and the private sector, as well as other levels of government, may find this Guide useful in the development of their emergency operations plans" (Fugate, 2010). Chapter 1 of the document notes the cyclical nature of emergency preparedness, illustrated with a wheel-like diagram:



FIGURE 1: FEMA CPG 101, VERSION 2.0

The "plan" component of this cycle is further broken down into steps including assembling a planning team, assessing risk, determining goals and priorities, developing plans to meet the goals (i.e., address the hazards), and plan review and testing. Planning itself is described as a cyclical process, "a continuous process that does not stop when the plan is published. Plans should evolve as lessons are learned, new information and insights are obtained, and priorities are updated" (FEMA, 2010, p.4–26).

The FEMA webpage on preparedness states, “Preparedness is achieved and maintained through a continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action” (FEMA, 2014).

The preparedness cycle is well explained by Haddow and Bullock (Haddow & Bullock, 2003) in a section titled, “A systems approach: the preparedness cycle.” The section describes the preparedness cycle, illustrated by a two-ring diagram with an outer circle of assessment, planning, preparation, and evaluation, and an inner circle of steps comprising assess threat, assess vulnerability, identify shortfalls/requirements, implement enhancements, train/exercise, and reassess. As noted in the discussion, “The important realization that preparedness is a dynamic state . . . must be understood by the emergency management professional.”

Other references to the preparedness cycle are found in diverse applications and locations; a brief sampling includes:

- The International Federation of Red Cross and Red Crescent Societies disaster preparedness training guide, *Introduction to Disaster Preparedness* (June 2000), includes a learning module on project planning which highlights a similar type of iterative cycle. It has a five-step process: conceptualize; plan; prepare; implement and monitor; evaluate.
- “Emergency management, like continuous quality improvement, is a cyclic process involving risk reduction/mitigation, readiness, response and recovery” (New Zealand West Coast District Health Board, 2014).
- Preparation for animal disease outbreak—a five-element cycle of planning, preparedness, mitigation, response, and recovery (Texas A&M University Institute for Infectious Animal Diseases, 2014)
- The flood risk management cycle (U.S. Army Corp of Engineers Institute for Water Resources, 2014)

- Public health preparedness (5-part cycle of prevention, mitigation, preparedness, response, recovery) (Public Health Ontario, 2014)

Origins in Project Management and Problem Solving Doctrine

The formalized cyclical approach to emergency preparedness in turn has roots in other disciplines associated with practical solutions to complex situations; in particular, project management and problem solving.

The beginnings of project management as a formal discipline stretch back to the mid-20th century and the relationship between the Department of Defense and its contractors (Kerzner, 2006; Söderlund, 2002; Fondahl, 1987; Snyder, 1987). Project management principles being relevant across multiple industries or pursuits, they have been adapted to fit the needs of organizations engaged in functions from research and development to manufacturing to infrastructure construction (Filippov & Mooi, 2010; Shenhar & Dvir, 1995; Fangel, 1993). Since that time an industry and/or profession has grown up around the concepts of project management, including an accrediting body, certifications, journals, and books. (Soderlund, 2004; Cooke-Davies, 2002; Packendorff, 1995). In short, project management has become an analytic lens through which to study complex problems.

To impose structure on the management process, one tool project managers use is the concept of a project life cycle. A simple statement of a project life cycle is a division into five phases: Conceptual, Planning, Testing, Implementation, Closure (Kerzner, 2006, p. 66). A project, however, is generally defined as a task with an endpoint (Kerzner, 2006; Munns & Bjeirmi, 1996; Packendorff, 1995). Therefore the project life cycle is more of a once-through process; it is not circular and repeating.

Problem-solving as a generic process is studied in various fields, including psychology, cognitive science, computer science, and mathematics (see, e.g., Schacter et al., 2009, Schoenberg, 2013). It is described as a cyclical process in some applications.

For example, Davidson and Sternberg (2003) describe a cyclical process involving seven steps that a problem-solver follows:

- Recognize or identify the problem.
- Define or represent the problem mentally.
- Develop a solution strategy.
- Organize his or her knowledge about the problem.
- Allocate mental and physical resources for solving the problem.
- Monitor his or her progress toward the goal.
- Evaluate the solution for accuracy.

(Davidson & Sternberg (2003), pp. 3–4.)

More generically, Sternberg (2008) describes a problem-solving cycle consisting of the following steps: identify problem, define problem, select strategy, organize information, allocate resources, monitor solving, evaluate success. Problem-solving can be a once-through process too, but in many contexts it can be a continual cycle—for example, product development where a product must be continually refined and improved (or replaced with a new product) to maintain sales (Kerzner, 2006, p. 67).

PARALLELS TO THE CYBERSECURITY CYCLE

The following components of the cybersecurity process for financial services, as reflected in regulations, handbooks, and guides, parallel the emergency preparedness cycle.

Risk Analysis. Business continuity and contingency plans include some form of risk analysis at the outset. References to risk analysis or risk assessment are found in NIST’s *Framework for Improving Critical Infrastructure Cybersecurity*, the FFIEC *IT Examination Handbook*, the CFTC regulations for swap data repositories, and the

FISMA rules for federal information systems that govern, among many other systems, data protection at the Federal Reserve.

This focus on risk aligns closely with the description of planning found in CPG101 which states “[p]lanning is fundamentally a process to manage risk” (FEMA, 2010).

Planning. Whether written as rules by federal regulators or best practices by industry organizations, standards for cybersecurity and business continuity begin with planning. Rules for swap data repositories, alternative trading systems, and the Federal Reserve all require contingency planning. Reflecting a broader recognition of the need for planning, the Securities Industry and Financial Markets Association (SIFMA) notes that robust planning is a key foundational element to ensuring firms are prepared in the event of a cyber incident (SIFMA, 2014). Firms are encouraged to document processes for responding to incidents in business continuity plans.

Organize and Equip. Organizing and equipping is quite simply ensuring the resources are available to implement the plan when necessary. Maintaining critical functions supported by communications and information technology infrastructure requires engineering redundancy and resiliency into firm operations. Regulations and best practices encourage or require firms to maintain backup facilities for their own critical operations, as well as work with service providers to ensure supporting infrastructure will be ensure availability of functions. The importance of including service providers cannot be overstated. Resilience cannot be (affordably) maintained within a single firm, but requires coordination with suppliers. For example, critical functions dependent on communications connectivity rules address ensuring circuit diversity between the primary and backup locations. Circuit diversity ensures that functionality will be maintained given the loss of a primary telecommunications provider. The CFTC rules for swap data repositories emphasize redundancy and avoiding single points of failure. Redundancy and backup capabilities are also addressed in the business-continuity standards from FINRA/SEC/CFTC and BITS.

Train and Exercise. Federal rules for maintaining critical financial systems require that firms in some way validate their contingency plans periodically. This validation process may take different forms, from independent reviews to internal control testing. Industry and trade organizations have taken the lead in coordinating training and exercising. SIFMA has conducted two full-scale exercises since 2011 as well as periodic tabletop exercises. The Quantum Dawn exercises tested the business continuity plans in the event of a cybersecurity incident (SIFMA, 2013). The original Quantum Dawn exercise in 2011 included 30 companies. Quantum Dawn 2 in 2013 grew to 50 financial services organizations (Sposito, 2013).

Evaluate and Improve. Maintaining actionable continuity and contingency planning is reliant on cyclical evaluation of plans against the current environment. Regulations and recommended best practices effectively view contingency plans as being in a constant draft status. As the operational environment evolves, organizations must review and update plans to reflect new realities. Evaluation and improvement are dependent on subjecting business operations and their supporting systems to periodic risk analysis. Regulations and recommended best practices endorse surveys of the threat environment and evaluation of systems for potential vulnerabilities.

CONCLUSION

Standards evolve to meet perceived threats and changes in the industry. Regulation of the financial services industry has evolved in order to meet changing perceptions of threat (sometimes to address a recent crisis) and in response to changes in the industry itself. To craft appropriate safeguards it is necessary to understand industry trends, pressures, and incentives. Certainly, any financial institution has business incentives to protect data and systems from malicious hacking or theft, apart from any requirement to meet a standard. However, new

standards nonetheless meet resistance. The CFTC's proposed regulation of SDRs drew extensive negative commentary from the industry, concerned about costs and loss of flexibility.⁵ As the industry and the threat landscape change, it will be important to seek ways to minimize systemic risk in ways that allow for flexibility and efficiency in financial services.

It is easy to see how specific, rigid standards would rapidly be overtaken by events as IT systems evolve. For example, data encryption relies on mathematical problems that are hard to solve without a key piece of information, which is supplied separately. However, as computing power increases and becomes cheaper, solving the problem without the key (through brute-force computing) can become feasible, making the encryption technique obsolete. DES, the data encryption standard approved by the U.S. National Bureau of Standards (NBS) in 1977, is now considered insecure for that reason. National Institute of Standards and Technology (NIST, the successor to NBS) officially withdrew it as an approved option for federal government encryption in 2005. Whereas decrypting DES-encrypted data in 1977 was cost-prohibitive, hardware and software to crack DES encryption efficiently is now available for under \$10,000 (Newton, 2013).

To meet the cybersecurity challenge, the newer regulatory model is process-oriented, implementing a continual cycle of preparedness including assignment of responsibility, risk analysis, planning, training, periodic review and testing, incident reporting, and rapid updating of systems based on new threat information. The focus is on a robust, iterative process rather than on application of specific protective measures.

With an emphasis on information sharing and risk communication (EO 13636), examinations (SEC, FINRA), and exercises (SIFMA), much of the framework for cybersecurity within the financial services sector appears to mirror in part the emergency preparedness cycle. Examinations that focus

⁵ See comments and responses in the Federal Register, 76 Fed. Reg. 54538 (September 1, 2011).

attention on cybersecurity, information sharing practices that help organize and equip firms to defend against cybersecurity incidents, and exercises coordinated with government and industry align well with the emergency preparedness cycle.⁶

Disaster threats, and the techniques, equipment, and systems used to respond to them, are constantly in flux. Whether protecting against a cyber attack on banks, a new animal virus, or a trainload of fracked oil, a continuous process of analysis, updates, testing, and refinement is the best way to keep up.

REFERENCES CITED

Ackerman, A. (2013). *CFTC Misreporting Size of Swaps Market, Agency Says* Wall Street Journal, Dec. 18, 2013. Retrieved from <http://online.wsj.com/news/articles/SB10001424052702304866904579266851056302512>.

Aguilar, L.A. (2014). Speech: *Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus*. Retrieved from <http://www.sec.gov/News/Speech/Detail/Speech/1370542057946#.VQNW6fnF-Zo>.

Argonne National Laboratory, *The Regulatory Landscape: Overview of the Impacts of Regulatory Agency Practices on Critical Infrastructure Protection, Report to the President's Commission on Critical Infrastructure Protection*, p. 78 (1997).

The Business Roundtable (2013) *More Intelligent, More Effective Cybersecurity Protection*. Retrieved from http://businessroundtable.org/sites/default/files/legacy/uploads/studies-reports/downloads/More_Intelligent_More_Effective_Pre-Publication.pdf.

CFPB (2011, December 21). Consumer Financial Protection Bureau, 12 C.F.R. Part 1016 (CFPB's Regulation P). 76 Federal Register 79025

Cheng, A. (2014, April 2). *Target data breach has lingering effect on customer service, reputation scores*. Wall Street Journal Marketwatch, Retrieved from <http://blogs.marketwatch.com/behindthestorefront/2014/04/02/target-data-breach-has-lingering-effect-on-customer-service-reputation-scores/>

Clark, C. L. (2010). *Controlling Risk in a Lightning-speed Trading Environment*, Policy Discussion Paper Series (2010), Federal Reserve Bank of Chicago. Retrieved from http://chicagofed.org/digital_assets/publications/policy_discussion_papers/2010/PDP2010-1.pdf.

Cooke-Davies, T. (2002). The "real" success factors on projects, *International Journal of Project Management*, Volume 20, Issue 3, pp. 185-190.

Cowper, W. (1773). "God moves in a mysterious way, His wonders to perform; He plants His footsteps in the sea, And rides upon the storm." William Cowper, 1773. Retrieved from http://en.wikipedia.org/wiki/God_Moves_in_a_Mysterious_Way.

CRS (2013, June). *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*. Congressional Research Service Report R42114, p. 44.

CRS (2014, January). *Privacy Protection for Customer Financial Information* (Congressional Research Service Report RS 20185).

Davidson, J. E., and Sternberg, R. J. (Eds). (2003). *The Psychology of Problem Solving*, Cambridge University Press, Cambridge, U.K.

Fangel, M. (1993). Comment: The broadening of project management. *International Journal of Project Management*, Volume 11, Number 2, p. 72.

FEMA (2010). *Developing and Maintaining Emergency Operations Plans, Comprehensive Planning Guide (CPG) 101, Version 2*. Federal Emergency Management Agency. Retrieved from www.fema.gov/pdf/about/divisions/npd/CPG_101_V2.pdf.

FEMA (2014). *Preparedness*. Webpage Retrieved from <http://www.fema.gov/preparedness-0>.

Ferrillo, P. (2014). *Cybersecurity and Cyber Governance: Federal Regulation and Oversight – Today and Tomorrow*. Retrieved from <http://blogs.law.harvard.edu/corpgov/2014/09/10/cyber-security-and-cyber-governance-federal-regulation-and-oversight-today-and-tomorrow/#9>.

FFIEC (2006). *IT Examination Handbook, Information Security booklet* (Federal Financial Institutions Examination Council, July 2006). Retrieved from <http://ithandbook.ffiec.gov/it-booklets/information-security.aspx>.

FFIEC (2008). *IT Examination Handbook, Business Continuity Planning booklet* (Federal Financial Institutions Examination Council, March 2008), Appendix C: Internal and External Threats.

Filippov, S. and Mooi, H. (2010). Innovation Project Management: A Research Agenda, *Journal on Innovation and Sustainability* Volume 1, Number 1.

FINRA (2013, August). Regulatory Notice 13-25, *Business Continuity Planning*. Joint advisory from FINRA, the SEC and CFTC. Retrieved from <http://www.finra.org/Industry/Regulation/Notices/2013/P308420>.

FINRA (2014). Targeted Examination Letters, *Re: Cybersecurity*. Retrieved from <http://www.finra.org/industry/regulation/guidance/targetedexaminationletters/p443219>.

Fondahl, J.W. (1987). The history of modern project management, *Project Management Journal*, Volume 18, Number 2, pp. 33-36.

FRB (2005). *Final Report on the Audit of SR FISMA Implementation* (Federal Reserve Board Inspector General, September 2005). Retrieved from http://www.federalreserve.gov/oig/Final_report_on_the_Audit_of_SR_FISMA_Implementation.htm#4969.

Fugate, W.C. (2010). Fugate, W. Craig, FEMA Administrator, cover letter accompanying CPG 101 Version 2.0, November 2010.

Gensler, G. (2011). Statement of Gary Gensler, CFTC Chairman, promulgating 17 CFR Part 49, 76 Fed. Reg. 54538, at 54597 (September 1, 2011). "This rule will enhance transparency in the swaps market and help reduce systemic risk."

⁶ Sales (2013) presents another categorization of cybersecurity regulation with some parallels – in his analysis, regulatory requirements are parsed into four steps: surveillance, target-hardening, survival/recovery (sometimes referred to as resilience) and response to attacks.

- GAO (2003). GAO-03-173, *Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats*. Report to the Subcommittee on Domestic Monetary Policy, Technology, and Economic Growth, Committee on Financial Services, House of Representatives. Retrieved from <http://www.gao.gov/assets/240/237103.pdf>.
- GLBA (1999). Gramm-Leach-Bliley Act of 1999. 15 U.S.C. § 6801.
- Greenwood, R. and Scharfstein, D. (2013). The Growth of Finance, *Journal of Economic Perspectives*. Volume 27, Number 2, pp. 3–28.
- Gorman, S. P. et al. (2004). The Revenge of Distance: Vulnerability Analysis of Critical Information Infrastructure, *Journal of Contingencies and Crisis Management* Volume 12, Number 2.
- Haddow, G.D., and Bullock, J.A. (2003). *Introduction to Emergency Management*, pp. 117–120. Published by Butterworth Heinemann.
- International Federation of Red Cross and Red Crescent Societies (2000). *Introduction to Disaster Preparedness*. Retrieved from <http://www.ifrc.org/Global/Introdp.pdf>.
- ISO 27001 International Organization for Standards, *Information technology – Security techniques – Information security management systems – Requirements*. Retrieved from <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>.
- Kerzner, H. (2006). *Project Management: A Systems Approach to Planning, Scheduling, and Controlling*, ninth edition. John Wiley & Sons Inc., Hoboken, New Jersey.
- Lemieux, C. (2003). *Network Vulnerabilities and Risks in the Retail Payment System*, *Emerging Payments Occasional Papers Series*. Federal Reserve Bank of Chicago. Retrieved from http://chicagofed.org/digital_assets/publications/occasional_papers/2003/eps-2003-1F.pdf.
- Marketwatch.com (2014, February 26) *Target's profits down \$440M after data breach*, New York Post. Retrieved from <http://nypost.com/2014/02/26/targets-profits-down-46-after-data-breach/>.
- McAndrews, J., and Stefanadis, C. (2000). *The Emergence of Electronic Communications Networks in the U.S. Equity Markets*, *Current Issues in Economics and Finance* Volume 6, Number 12.
- Munns, A.K. and Bjeirmi, B.F. (1996). The role of project management in achieving project success. *International Journal of Project Management*, Volume 14, Number 2, pp. 81–87.
- Newton, G.E. (2013). *The Evolution of Encryption*, May 7, 2013. Wired Magazine. Retrieved from <http://www.wired.com/2013/05/the-evolution-of-encryption/>.
- New Zealand West Coast District Health Board (2014) New Zealand West Coast District Health Board, webpage accessed Retrieved from http://www.westcoastdhsb.org.nz/publications/emergency_management_planning.aspx.
- Obama, B. (2013, February 12). Executive Order 13636: *Improving Critical Infrastructure Cybersecurity*. Retrieved from <https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.
- Obama, B. (2015, February 13). Executive Order (unnumbered): *Promoting Private Sector Cybersecurity Information Sharing*. Retrieved from <https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari>.
- Office of the Comptroller of the Currency (2014). *Semiannual Risk Perspective*. Retrieved from <http://www OCC.gov/publications/publications-by-type/other-publications-reports/semiannual-risk-perspective/semiannual-risk-perspective-fall-2014.pdf>.
- Packendorff, J. (1995). Inquiring into the temporary organization: New directions for project management research, *Scandinavian Journal of Management*, Volume 11, Number 4, 319–333.
- Payments Risk Committee (2007). *Financial Market Infrastructure Risk: Current Report of the Financial Market Infrastructure Risk Taskforce*, Federal Reserve Bank of New York. Retrieved from <http://www.newyorkfed.org/prc/files/FMIMay07.pdf>.
- Payments Risk Committee (2013). *Business Continuity Planning: Lessons from a Communications Exercise*, Federal Reserve Bank of New York. Retrieved from <http://www.newyorkfed.org/prc/files/report130709.pdf>.
- Public Health Ontario (2014). Public Health Ontario, Canada, webpage Retrieved from <http://www.publichealthontario.ca/en/About/Departments/Pages/Emergency-Management.aspx#.VC62UhZGUg8>.
- Public Law 111-203, 12 U.S.C. §§ 5301–5641 (2010).
- Report of the Staffs of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues (2010, September 30). *FINDINGS REGARDING THE MARKET EVENTS OF MAY 6, 2010*. Retrieved from <http://www.sec.gov/news/studies/2010/marketevents-report.pdf>.
- Richwine, L. (2014). Reuters.com, *Cyber attack could cost Sony studio as much as \$100 million*. Retrieved from <http://www.reuters.com/article/2014/12/09/us-sony-cybersecurity-costs-idUSKBN0JN2L020141209>.
- Rooney, B. (2010). CNNMoney.com, *Trading program sparked May 'flash crash'*. Retrieved from http://money.cnn.com/2010/10/01/markets/SEC_CFTC_flash_crash/.
- Sales, N. A. (2013). *Regulating Cyber-security*, 107 Nw. U. L. Rev. 1503 (2013). Retrieved from <http://scholarlycommons.law.northwestern.edu/nulr/vol107/iss4/1>.
- Schacter, D.L. et al. (2009). *Psychology*, Second Edition. New York: Worth Publishers. p. 376.
- Schoenberg, A. H. (2013, January). Reflections on Problem Solving Theory and Practice, *The Mathematical Enthusiast*, Vol. 10 No. 1. Retrieved from <http://www.math.umd.edu/tmme/vol10no1and2/>.
- Securities and Exchange Commission. (2011). CF Disclosure Guidance: Topic No. 2 – Cybersecurity. Retrieved from <http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>.
- Securities and Exchange Commission. (2014). OCIE Cybersecurity Initiative. Retrieved from <http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf>.
- Shenhar, A. J. and Dvir, D. (1996). *Toward a typological theory of project management*, *Research Policy*, Volume 25, pp. 607–632.

SIFMA (2013). Cybersecurity Exercise: Quantum Dawn 2. Retrieved from <http://www.sifma.org/services/bcp/cybersecurity-exercise--quantum-dawn-2/>.

Smedinghoff, T. J. (2008). *The State of Information Security Law*, Social Science Research Network website, Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1114246.

Snyder, J.R. (1987). Modern project management: How did we get here – where do we go? *Project Management Journal*, Volume 28, Number 1, pp. 28–29.

Söderlund, J. (2004). Building theories of project management: past research, questions for the future, *International Journal of Project Management*, Volume 22, Number 3, pp. 183–191.

Sposito, S. (2013). “Quantum Dawn 2 a Useful Test, But Banks Have More Cyberwar Prep to Do” *American Banker* | *Bank Technology News*. Retrieved from http://www.americanbanker.com/issues/178_139/quantum-dawn-2-a-useful-test-but-banks-have-more-cyberwar-prep-to-do-1060741-1.html.

Sternberg, R. J. (2008). *Cognitive Psychology*, 5th Edition, Chapter 11: Problem Solving and Creativity, Wadsworth Press. See also Spring HIP Lecture 12, Retrieved from <http://www.itu.dk/people/rkva/2011-Spring-T14/slides/Week11/2011-Spring-HIP-Lecture12-ProblemSolvingCreativity.pdf>.

Texas A&M University Institute for Infectious Animal Diseases (2014). Texas A&M University Institute for Infectious Animal Diseases. Retrieved from <http://iiad.tamu.edu/about/thrusts/emergency-management/>.

U.S. Army Corps of Engineers Institute for Water Resources (2014). U.S. Army Corps of Engineers Institute for Water Resources. Retrieved from <http://www.iwr.usace.army.mil/Missions/FloodRiskManagement/FloodRiskManagementProgram/PartnersinSharedResponsibility/Federal.aspx>.

Whitehead, C. K. (2010). “Reframing Financial Regulation” *Boston University Law Review* 90. Retrieved from <http://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1041&context=facpub>.

APPENDIX A: OVERVIEW OF FINANCIAL SERVICES REGULATORY AGENCIES AND STANDARD-SETTING ORGANIZATIONS

Regulatory Agencies

Regulation and oversight of financial services is carried out by a combination of federal and state agencies. The patchwork structure of financial services regulation reflects its development over time, as additional structures and rules were set up in response to periodic crises and to the growth of new types of financial institutions. Key players are:

Federal Reserve Board (FRB or Fed). The Fed is an independent agency with the responsibility for regulating the nation’s supply of money, and supervisory

jurisdiction over all state-chartered banks that belong to the Federal Reserve System. The Fed can mobilize cash reserves, issue credit to national banks, and oversee the required balances.

Office of the Comptroller of the Currency (OCC). The OCC is a bureau in the Department of the Treasury, with supervisory jurisdiction over all federally chartered banks.

Federal Deposit Insurance Corporation (FDIC). The FDIC is a federally chartered corporation that manages the Bank Insurance Fund. In that role, the FDIC insures deposits in all federally chartered banks, state-chartered banks that join the Federal Reserve System, and all thrift institutions eligible for the insurance fund. (Thrift institutions include credit unions, savings & loan associations, and mutual savings banks.) The FDIC also has supervisory responsibility over state-chartered banks that choose to be insured by the Bank Insurance Fund but not to join the Federal Reserve System. The FDIC also resolves and liquidates failed banks covered by the Bank Insurance Fund.

Office of Thrift Supervision (OTS). The OTS is a Treasury Department agency that oversees all thrift institutions insured by the FDIC. The OTS resolves and liquidates all failed thrifts under its supervision.

National Credit Union Administration (NCUA). The NCUA is an independent federal agency created by Congress to regulate, charter, and supervise federal credit unions. The NCUA operates and manages the National Credit Union Share Insurance Fund, insuring the deposits of all federal credit unions and the majority of state-chartered credit unions. As of September 2013, there were 6,620 federally insured credit unions with total assets of more than \$1 trillion.

Commodity Futures Trading Commission (CFTC). The CFTC is an independent federal agency that regulates futures and option markets. Originally tasked with regulating agricultural commodity futures, the jurisdiction of the CFTC has grown with the evolution of futures and derivative markets. The 2010 Dodd-Frank Act Wall Street Reform and

Consumer Protection Act (Dodd-Frank) (Public Law 111-203) tasked the CFTC with regulating the swaps market, a process that is still unfolding.

Securities and Exchange Commission (SEC). The SEC oversees key participants in the securities world, including securities exchanges, alternative trading systems (ATSs), securities brokers and dealers, investment advisors, and mutual funds. The Division of Trading and Markets provides day-to-day oversight of the major securities market participants: the securities exchanges; securities firms; self-regulatory organizations (SROs), including the Financial Industry Regulatory Authority (FINRA), the Municipal Securities Rulemaking Board (MSRB), clearing agencies that help facilitate trade settlement; transfer agents (parties that maintain records of securities owners); securities information processors; and credit rating agencies. The Division also oversees the Securities Investor Protection Corporation (SIPC), which is a private, non-profit corporation that insures the securities and cash in the customer accounts of member brokerage firms against the failure of those firms.

Consumer Financial Protection Bureau (CFPB). Established by the Dodd-Frank Act, the CFPB supervises banks, credit unions, and other financial companies to enforce federal consumer financial protection laws.

Federal Financial Institutions Examination Council (FFIEC). The FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for examination of financial institutions by the Fed, FDIC, OCC, NCUA, and CFPB, and to make recommendations to promote uniformity in the supervision of financial institutions. The FFIEC also coordinates extensively with state regulators. The FFIEC's *IT Examination Handbook* (2006) serves as a summary of IT standards for banks, credit unions, and similar institutions.

State Regulatory Agencies. Most state regulatory agencies have authority to examine all depository and non-depository institutions for compliance with both state and federal laws. Such authority typically includes state-chartered banks, national banks,

state savings banks, federal savings banks, branches of out-of-state banks of all kinds, trust companies (special entities established to hold property subject to a trust, to buy and sell securities for others, and to offer advice on these matters), securities and commodities dealers, and building and loan associations. Many states also regulate personal loan vendors and makers, personal property finance companies, mortgage brokers, check sales and cashing services, and other financial services (Argonne, 1997). Many states have enacted legislation specifically regulating security of personal information, including specific provisions regarding social security numbers, data disposal, and notification of security breaches (Smedinghoff, 2008).

Sources of Non-Regulatory or Quasi-Regulatory Standards and Guidelines

A number of advisory committees and industry organizations have developed standards and guidance in the financial services sector. In some cases, these organizations have a formal or quasi-formal status in the sense that the federal government recognizes their standards and authorizes enforcement of them. The term Self-Regulatory Organization (SRO) is sometimes used to refer to such organizations. In addition to financial services organizations, there are various national and international standard-setting organizations that address business-continuity or cybersecurity practices.

Financial Industry Regulatory Authority (FINRA). FINRA is an SRO that develops and enforces standards for securities brokerage firms, brokers, and exchanges. It oversees over 4,000 brokerage firms that do business with the NYSE, NASDAQ, and other exchanges. FINRA is non-governmental, but the SEC has authorized FINRA to enforce federal securities laws and FINRA rules through fines and other disciplinary measures.

Financial Services Sector Coordinating Council (FSSCC). The Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security, established in 2002, is the sector coordinator for Financial Services

for the protection of critical infrastructure, focused on operational risks. The FSSCC has issued guidance for financial service firms that rely on undersea cables for international telecommunications.

National Institute of Standards and Technology (NIST). NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, issued February 12, 2014, provides a set of industry standards and best practices to help organizations manage cybersecurity risks. It implements Executive Order 13636, "Improving Critical Infrastructure Cybersecurity."

Financial Services Roundtable. The Financial Services Roundtable represents 100 of the largest American financial services companies that provide banking, insurance, and investment products and services. The Roundtable's technology policy division, BITS, addresses issues at the intersection of financial services, technology, and public policy, such as critical infrastructure protection, fraud prevention, and the safety of financial services. The BITS Guide to Business-Critical Telecommunications Services, November 2004, summarizes good practices to ensure continued connectivity.

Financial Services Information Sharing and Analysis Center. The FSISAC is an industry organization created in response to PPD 63 (later HSPD 7) as a means to promote information sharing among sector firms and between the private sector and government. FSISAC membership is open to firms and companies engaged in all facets of the financial services industry, including banking and credit, securities, insurance, commercial lending, and security service providers. Additionally, FSISAC partners with government agencies, other professional and industry organizations, and similarly interested firms. The FSISAC provides a mechanism for firms to share confidentially information related

to physical and cybersecurity threats for the purposes of developing recommended solutions that can be promulgated to FSISAC members.

Other Technical Standard-Setting Organizations. Many other organizations issue technical standards that may be relevant to cybersecurity and telecommunications continuity in the financial services sector. The three largest are the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), and International Telecommunication Union (ITU), all based in Geneva, Switzerland. The American National Standards Institute (ANSI) oversees the development of voluntary consensus standards in the United States and coordinates U.S. standards with ISO. Other organizations include the Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF), and the World Wide Web Consortium (W3C).

AUTHORS

Ken Lerner (klerner@anl.gov) is a technical programs attorney in the Global Security Sciences Division at Argonne National Laboratory. He has a Bachelor of Art in Economics and in Philosophy from the University of Illinois, Urbana, and a J.D. from the University of Michigan School of Law. At Argonne he analyzes law and policy issues for a variety of federal programs in the homeland security and emergency preparedness field.

Matthew Berry (mberry@anl.gov) is an infrastructure systems and modeling analyst in the Risk and Infrastructure Sciences Center at Argonne National Laboratory. He is a BA political science graduate of Northeastern Illinois University and received his MPA from University of Illinois at Chicago.

Cybersecurity Graduate Training Reveals Security-by-Obcurity Vulnerabilities in Website Authentication

Gordon W. Romney | Dustin L. Fritz

ABSTRACT

NIST guidelines for general server security encourage open design and specifically discourage system security dependent on the secrecy of the implementation or its components. In cybersecurity such intended secrecy is known as “Security by Obscurity.” Users frequently assume that website authentication processes using SSL/TLS involving ID/username and password are secure. Suspecting a website of vulnerabilities, graduate student teams were tasked with passively obtaining forensic evidence to identify potential vulnerabilities using sniffing and packet analysis tools in a non-invasive manner. Passive, manual testing was performed on a target website that used TLS and ID-password authentication. All the teams substantiated that normal credential authentication was encrypted for both valid and invalid credentials. However, the password change process, re-routed through a proxy, non-SSL URL website, revealed unencrypted usernames and passwords in sniffed packets. Forensic analysis by all teams, using Kali virtual machines, revealed a serious information disclosure vulnerability because all data was transmitted in the clear and could lead to theft of the website data. Since everything was transmitted in the clear it was possible to hijack the Secure Session Cookie. The website also used Client Side Validation, which was documented nicely and made it easy to bypass. After the vulnerabilities were verified and evidence was collected, research was conducted on methods to resolve or mitigate the vulnerabilities, and recommendations were provided to avoid unnecessary “Security by Obscurity.”

INTRODUCTION

NIST guidelines for general server security encourage open design and specifically discourage system security dependent on the secrecy of the implementation or its components (NIST Server, 2008). Security implementations should be readily apparent, such as with the designation of using Secure Sockets Layer (SSL/TLS), HTTPS, as most Web users would recognize. If diversions, IP redirections, and tricks of secrecy are employed, then such practices are not in accordance with NIST guidelines and industry good security practices. Furthermore, customers of Web services should not be confused or uncertain regarding the security of a website they might frequent. In cybersecurity such intended secrecy is known as “Security by Obscurity.” Such practices are not accepted by security professionals because they inevitably lead to vulnerabilities that are easily exploited. Users frequently assume that website authentication processes using SSL/TLS involving ID/username and password are secure. Suspecting a website of vulnerabilities, graduate student teams from the MS Cyber Security and Information Assurance program of National University were tasked with passively obtaining forensic evidence to identify potential vulnerabilities using sniffing and packet analysis tools in a non-invasive manner (NUCSIA.nu.edu., n.d.). Passive, manual testing was performed on a target website, identified as SafeWebsite for anonymity, that used TLS and ID-password authentication.

SECURITY BY OBSCURITY IS NOT AN ANSWER

“Many people in the information security industry believe that if malicious attackers don’t know how software is secured, security is better. Although this might seem logical, it’s actually untrue. Security through obscurity means that hiding the details of the security mechanisms is sufficient to secure the system alone” (Breithaupt, 2014; Merkow, 2014). Hence, when the secret is first discovered, the question frequently asked is, “How many people know about this?” Breithaupt and Merkow continue by saying, “The better bet is to make sure no one mechanism is responsible for the security of the entire system. Again, this is defense in depth in everything related to protecting data and resources.

Obscuring components in security, on the other hand, in an already secure environment does add security by defense in depth but must not be confused with “security by obscurity,” which is the sole defense (Miessler, 2015). Miessler used, as an example, changing the normal port for SSH from 22 to something different. Then using the new port number as an alarm for potential intrusion.

Politically, “Security by Obscurity” was used as the reason why the White House refused a request for Healthcare.gov security details because sharing the information might lead to hacker discovery of vulnerabilities that might lead to “risk to consumers’ private information” (Masnick, 2015). A comment in this report stated, “These days, in the computer security world, it’s pretty well known that if you’re relying on security by obscurity, you’re not being secure.”

SECURITY PROFESSIONALS NEED TO KNOW

Heim, vp of Enterprise Security for McKesson Corporation posits, “...I would argue that it is essential for individuals placed in charge of designing, building, and maintaining information infrastructure to be fully aware of the true threats that their systems will need to repel.” (Bradley, 2015). Bradley, additionally states, “Ignorance is not

bliss. Security through obscurity doesn’t work. It only means that the bad guys know things that you don’t and will exploit your ignorance to the fullest every opportunity they get.” Cybersecurity professionals and students need to be trained with the tools that attackers use.

MS IN CYBERSECURITY AND INFORMATION ASSURANCE (MS CSIA)

Research for this paper was performed by graduate students of the MS CSIA program at National University (NU). Romney, one of the authors, was the architect of the MS CSIA program, and Fritz, an author, was an MS CSIA Advisory Board Member that supported and guided the Ethical Hacking specialization. The MS CSIA program was designated an NSA/DHS Center of Academic Excellence in IA Education in 2013 (NUCSIA.nu.edu., n.d.; NSA.gov. (n.d.)). It has graduated over 200 master’s students and has another 100 currently enrolled in both onsite and online courses. Significant characteristics of the program are the following:

- The curriculum was designed to meet both online and onsite instruction in a one-semester-course-per-month modality.
- A CSIA Advisory Council of industry and academic partners was created in order to incorporate needed skills required to meet the Cyber Warrior demand.
- Agile pedagogy and software development methods would be a standard (Agile, 2013; Agile Manifesto, 2001).
- The virtual lab using VMware ESXi was created and implemented to provide virtual machines (VMs) for cybersecurity laboratory exercises. The current implementation has approximately 1,000 servers and appliances.
- The courses were designed in order to meet the specific security certification requirements of the CNSS standards, 4011 and 4012 (CNSS (n.d.)).

- Both online and onsite instruction and assessment was designed to meet WASC accreditation requirements.
- Kali Linux is one of the preferred pen testing systems (Kali Linux (n.d.).

TOOLS EMPLOYED

Virtualization

Operating system virtualization has been a foundational tool in the creation of the virtual lab and MS CSIA lab instruction and a great facilitator in the teaching of engineering and security at NU in an Agile manner (Romney et al., 2013, October; Romney et al., 2014, April). Romney and colleagues stressed the role of “Agility” in engineering education and signaled the fact that NU is an “Agility incubator.” (Romney, 2009; Dey et al., 2012). As Gartner’s Bittman said, “Agility is probably the top attribute [one] ... get[s] out of virtualization. For example, [one] ... can deploy servers 30 times faster; if it took two months before, it now takes two days.” (Bittman, n.d.). Efficiency was gained by the ability to provide students with a stable, hardware-independent, virtual machine configuration that ran on a Windows computer on the first day of lab. This saved two weeks of time traditionally lost coordinating all students with different laptops and hardware drivers simply to begin the assignment. By using virtualization, flexibility was gained as new concepts could be introduced more readily.

Kali Linux

Kali Linux, released in February 2014, is the primary pen testing system used by the MS CSIA program (Kali Linux, n.d.). Kali, an open-source product, is the successor to the very successful Backtrack 5. Kali efficiently served as the penetration testing system for this research. Two important software tools within its distribution are Tcpdump and Wireshark. (TCPDUMP, 2014; Wireshark, 2014). Both Tcpdump and Wireshark are sniffing

and packet capture tools that allow one to view the transmission order and digital content of internet packets. Tcpdump is a command line tool whereas Wireshark has a GUI interface and is also a packet analyzer (Bae, 2012; Lamping et al., 2014). Their use is explained in the sections that follow.

DESIRED RESEARCH OUTCOME: PROCESS AND ANALYSIS

The outcome of the research of this paper was to determine if the SSL-identified login of SafeWebsite was securely authenticating users and protecting personal credentials. Three research objectives, each represented by a unique lab, were designed to contribute to the research outcome.

The challenge to the 23 cybersecurity graduate students who participated was to determine if their own personal login credentials were secure on a website that all had access to and used on a regular basis. In that process, if vulnerabilities were identified, policy recommendations were solicited. All had been using SafeWebsite, an SSL-supported login website, and had assumed, as most users do of websites broadcasting SSL support, that all traffic was encrypted. After all, that is what Google.com and Amazon.com do when personal, confidential data is involved. To evaluate the security of authenticating into SafeWebsite the students were given three consecutive laboratory exercises using the tools previously reviewed.

THREE LABS, FOUR TEAMS, AND 23 STUDENTS

The three labs investigate the interactions with SafeWebsite involving user authentication: 1) a login attempt using fake credentials, 2) a login attempt using genuine credentials, and 3) changing credentials. The labs involve using a Kali Linux virtual machine, sniffing internet packet traffic using Wireshark and tcpdump, capturing the packets and analyzing them with Wireshark. Credentials for SafeWebsite consist of an email address paired with a password. The Internet traffic that is sniffed must

be captured into a standard pcap file used by both Wireshark and tcpdump. The pcap file facilitates subsequent off-line analysis of recorded Internet packet traffic by Wireshark.

Students were required to develop their own penetration testing standard operating procedure by creating a step-by-step outline for each lab in order to ensure accurate and repeatable results. Additionally, recording the baseline technical configuration of all hardware and software was a requirement in accordance with correct scientific research procedures.

Four teams consisting of the 23 students in the cohort recorded the research outcome. Teams were used for collaborating and developing consistent technical processes. Each student performed her own research and produced her own research report.

FIGURE COLOR KEY

All the figures in this paper use the following color key in the Wireshark scans that are shown.



COLOR	REPRESENTS
	Safe Website URL
	RedirectWebsite URL
	Redacted Information
	Vulnerability or Emphasis

FIGURE 1: COLOR KEY FOR FIGURES IN THIS PAPER

The original, recognizable URL or IP address for SafeWebsite was redacted with a green bar. Its access is as HTTP, on port 80. It immediately redirects to a different IP address for login using HTTPS TLS that this paper refers to as RedirectWebsite and is redacted in all Wireshark scans as a yellow bar. Its access is as HTTPS TLS, on port 443, for https://RedirectWebsite.com. All information that might be confidential or identify websites is redacted by green, yellow, or black bars. Vulnerabilities and points of emphasis are denoted by underline bars or red arrows.

LAB 1: FAKE CREDENTIALS

Lab 1 focused on a login attempt using fake credentials. The objective was to demonstrate proficiency of using Wireshark to sniff and analyze Internet traffic between a user host Kali VM and

SafeWebsite. The objective of the lab was to prove that SafeWebsite’s process for handling fake credentials was secure.

Packet Capture

Wireshark on Kali Linux was used to capture the packet traffic between the student Kali host and SafeWebsite. This capture was turned on prior to typing in the destination URL into the browser and was turned off when the student logged off.

Packet Analysis

Immediately upon first typing of http://”SafeWebsite”.com into a browser a redirect to https://”RedirectWebsite”.com (represented by the yellow bar in Figure 1) occurred.

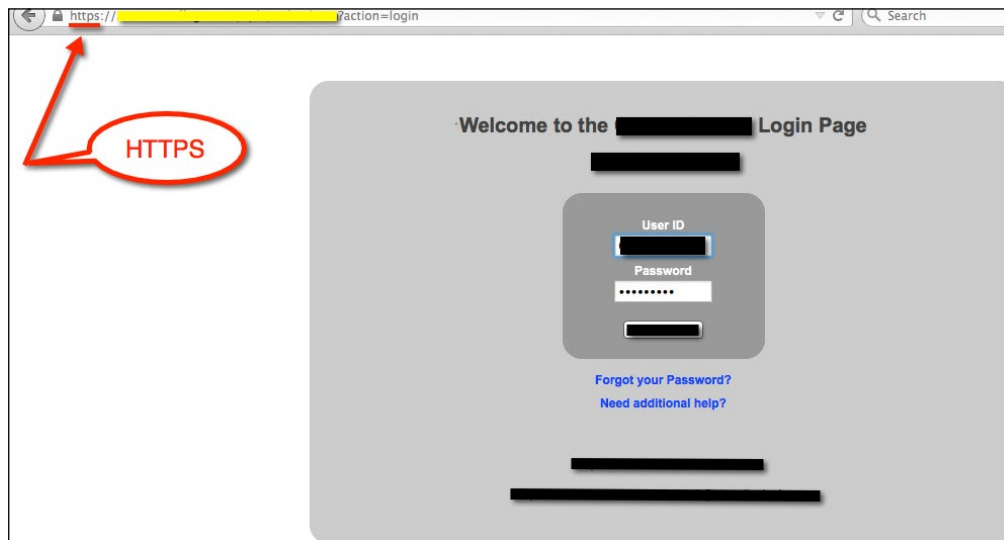


FIGURE 2: LOGIN WEB PAGE FOR SAFEWEBSITE

The captured Lab1.pcap file was analyzed by Wireshark. One team found the following display filter setting useful for Wireshark analysis:

- 172.24.87.4 (or the appropriate IP address) was excluded. This is the IP address of the workstation connected to the Kali Linux VM using VNC over SSH as the traffic this connection created was noisy.
- ARP was excluded as it is a chatty protocol that requires an acknowledgment before proceeding.
- NBNS was excluded as it likewise is a chatty protocol (NetBIOS Name Service). It translates NBNS messages of names to associated IP addresses.

Figure 3 shows the Wireshark packet list analysis of the captured Lab1.pcap that were selected by applying the specified display filters. The filters exclude much unnecessary, detailed traffic that complicates the desired analysis. The green bars indicate the initial unencrypted HTTP frames that

result from typing `http://SafeWebsite.com` and then selecting the login option. Frame 798 in the left column shows the initial SYN from the student host (Source) to SafeWebsite (Destination – yellow bar), and in frame 803 the SafeWebsite (Source – yellow bar) response of SYN-ACK to the student host on IP 172.24.60.65. Frame 804 shows the student host response of an ACK that completes the three-way handshake of a TCP connection (SYN, SYN-ACK, ACK). Note that the frame numbers are not sequential as those missing were dropped by the specified Wireshark display filters as they are not germane to this analysis. Only those frames that pass the filter are shown in the Wireshark analysis window.

Two IP Addresses

A redirect from one URL/IP address to another is evident by referencing frames 834 through 838 in Figure 3, the reference “object moved” and `https`. The new URL for RedirectWebsite is shown in frames 836-7 and replaced with a yellow bar.

Filter: (ip.addr == 172.24.87.4 or arp or nbns or db-lsp-disc)		Expression...	Clear	Apply	Save
Time	Source	Destination	Protocol	Length	Info
798	12.049710000	172.24.60.65	TCP	74	53032 > http [SYN] Seq=0 Win=14600 Len=0 MSS=
799	12.050318000	172.24.60.65	DNS	77	Standard query 0xb465 A [REDACTED]
800	12.050359000	172.24.60.65	DNS	77	Standard query 0x99d1 AAAA [REDACTED]
801	12.052395000	172.24.236.2	DNS	93	Standard query response 0xb465 A [REDACTED]
802	12.052408000	172.24.236.2	DNS	141	Standard query response 0x99d1
803	12.092791000	172.24.60.65	TCP	78	http > 53032 [SYN, ACK] Seq=0 Ack=1 Win=4308
804	12.092815000	172.24.60.65	TCP	66	53032 > http [ACK] Seq=1 Ack=1 Win=14720 Len=
805	12.092936000	172.24.60.65	HTTP	469	GET / HTTP/1.1
816	12.235963000	172.24.60.65	TCP	66	http > 53032 [ACK] Seq=1 Ack=404 Win=4711 Len
834	12.389913000	172.24.60.65	HTTP	555	HTTP/1.1 302 Object moved (text/html)
835	12.389938000	172.24.60.65	TCP	66	53032 > http [ACK] Seq=404 Ack=490 Win=15744
836	12.393333000	172.24.60.65	DNS	79	Standard query 0x77dd A [REDACTED]
837	12.393355000	172.24.60.65	DNS	79	Standard query 0xb2fe AAAA [REDACTED]
838	12.393538000	172.24.60.65	TCP	74	36192 > https [SYN] Seq=0 Win=14600 Len=0 MSS=
839	12.400735000	172.24.60.65	DNS	95	Standard query response 0x77dd A [REDACTED]

FIGURE 3: TWO IP ADDRESSES: HTTP FOR SAFEWEBSITE AND HTTPS FOR REDIRECTWEBSITE

The HTTPS SSL/TLS handshake, exchange of TLS digital certificate and encryption key packets between RedirectWebsite (yellow bars) and the student host are shown in frames 848 through 875 of Figure 4. All attempted Client Side Validation

traffic for the student credentials was done by RedirectWebsite and all traffic between the student host and RedirectWebsite was encrypted.

Filter: (ip.addr == 172.24.87.4 or arp or nbns or db-lsp-disc)		Expression...	Clear	Apply	Save
Time	Source	Destination	Protocol	Length	Info
848	12.435422000	172.24.60.65	TLSv1	274	Client Hello
849	12.479240000	172.24.60.65	TCP	1490	[TCP segment of a reassembled PDU]
850	12.479268000	172.24.60.65	TCP	66	36192 > https [ACK] Seq=209 Ack=1425 Win=1753
851	12.479281000	172.24.60.65	TCP	90	[TCP segment of a reassembled PDU]
852	12.479289000	172.24.60.65	TCP	66	36192 > https [ACK] Seq=209 Ack=1449 Win=1753
853	12.479291000	172.24.60.65	TCP	1490	[TCP segment of a reassembled PDU]
854	12.479297000	172.24.60.65	TCP	66	36192 > https [ACK] Seq=209 Ack=2873 Win=2048
855	12.479299000	172.24.60.65	TCP	1490	[TCP segment of a reassembled PDU]
856	12.479303000	172.24.60.65	TCP	66	36192 > https [ACK] Seq=209 Ack=4297 Win=2329
866	12.520446000	172.24.60.65	TLSv1	115	Server Hello, Certificate, Server Hello Done
867	12.520466000	172.24.60.65	TCP	66	36192 > https [ACK] Seq=209 Ack=4346 Win=2329
868	12.521266000	172.24.60.65	TLSv1	376	Client Key Exchange, Change Cipher Spec, Encr
874	12.580246000	172.24.60.65	TLSv1	109	Change Cipher Spec, Encrypted Handshake Messa
875	12.580527000	172.24.60.65	TLSv1	477	Application Data

FIGURE 4: TLS HANDSHAKE AND KEY EXCHANGE

Return to SafeWebsite After Non-authentication

As appropriate, following an unsuccessful authentication, RedirectWebsite returned to HTTP SafeWebsite for another login attempt as shown in Figure 5.

Open the "Display Filter" dialog, to edit/apply filters

Time	Source	Destination	Protocol	Length	Info
821	22.815845000	172.24.60.65	HTTP	571	GET /verifpwd.learn?URL=A%5FSPSH%2Ereal&SSL=5t
830	22.960009000	172.24.60.65	TCP	66	http > 53032 [ACK] Seq=490 Ack=909 Win=5216 L
868	23.259936000	172.24.60.65	HTTP	511	HTTP/1.1 302 Object moved (text/html)
869	23.259953000	172.24.60.65	TCP	66	53032 > http [ACK] Seq=909 Ack=935 Win=16768
870	23.263049000	172.24.60.65	HTTP	483	GET /formslogin.asp HTTP/1.1
882	23.406530000	172.24.60.65	TCP	66	http > 53032 [ACK] Seq=935 Ack=1326 Win=5633
885	23.469348000	172.24.60.65	HTTP	557	HTTP/1.1 302 Object moved (text/html)

FIGURE 5: RETURN TO HTTP AND CLEAR TEXT

Findings for Lab 1

The SafeWebsite process for handling a fake credential was secure and all exchange of student credentials was done encrypted under HTTPS and TLS.

LAB 2: GENUINE CREDENTIALS

Lab 2 focused on a login attempt using genuine credentials. The objective was to demonstrate proficiency of using tcpdump to sniff internet traffic between a user host Kali VM and SafeWebsite and use Wireshark for packet analysis. The objective of the lab was to prove that SafeWebsite's process for handling genuine credentials was secure and that SafeWebsite remained secure for subsequent application processes.

Packet Capture

Tcpdump on Kali Linux was used to capture the packet traffic between the student Kali host and SafeWebsite. This capture was turned on prior to

typing the destination URL into the browser and was terminated after 1000 packets and saved as Lab2.pcap. One team then emailed the Lab2.pcap to team members for offline analysis.

Packet Analysis

The captured Lab2.pcap file was analyzed by Wireshark. The same display filter settings specified for Lab 1 continued to be useful for Wireshark analysis in Lab 2. Figures 2, 3, and 4 and their analysis remained the same for the RedirectWebsite authentication process. Now, where in Lab 1 RedirectWebsite returned to HTTP, SafeWebsite and Clear Text as shown in Figure 5 a surprise occurred that was picked up by only one team during Lab 1 and all during Lab 2. RedirectWebsite, as part of its Client Side Validation process continued to communicate beyond what is shown in Figure 5 in clear text with SafeWebsite as shown in Figure 6. The yellow area represents HTTPS encrypted packets while RedirectWebsite was authenticating the student user. One can see that the content is not interpretable as it is encrypted.

```

File Edit View Search Terminal Help
...*...%Y_...'.a.|WB...
[&...jk.*...vy_*s.Y...M'...:.....$wCy...^MP...l/.....s.W....%`...yKX01
06:50:08.585169 IP [redacted].https > 172.24.60.49.39218: Flags [P.], seq 13498:14
458, ack 1892, win 6199, options [nop,nop,TS val 2421791992 ecr 1261892677], length 960
E....@.....o...<1...2...F..K...7/J.....
.Y..K6.E.....I...T0.....m..s..h...=l7.9.....#.B.P.....|..9..Hu.R.).[R>?...
w.^MWX...!.....G4G..qa.E..=Fp.iR...H!.Am.....\S.y9-..a]..R...-M(.0V.....=C.o...&T.smx
....w.| @!...M..\.v...>.....?BaH?.H.:b...4.3..X.U.m.E.Z.I...f..+Y'.....X,...
...M.....'C0..7.U-.zAz.*=Z..{...x..9.....A.....~F..2.....>Xmv...#.Z.
..Z..%..H...`..|MG..J.)Z.K..|.W8Z*H.....U..n=.]2e.^.....k..4].^...WC.C#.RBrD.....
9>&...<.,4.,6w.Z&..g.&e..].)R./~.U..2).b.....t...2...u.4.T`I.....T.R6fB.4...-
..j.D..q...5...GZ....2.....9.NZ.....<.....F.<....zp...[....Avg
^M.$.=v-.U...W.F.kM...sm.5.$'.[Sf9...^M.'... .."....%...C...^..G...$l..c....o
.....n;Cb.....}.....o
\E.)b..pb....._...x.....&.....jw.....l8`..L..2:5.....);6.;;!.....a.....[.7?..
.a
?.....@!.....@.....t..mo.....T.GL.w.o.A.\...<8...3..0...e..xyS...9...~S0
...8df..0...F.I.s.Y...Q...fLJ...&4\...sq.....i.b...i.e...3..vU...CF.....s...
....2....\N|('...>6..
06:50:08.585193 IP 172.24.60.49.39218 > [redacted].https: Flags [.], ack 14458, wi
n 331, options [nop,nop,TS val 1261892689 ecr 2421791992], length 0
E..4]L@.....<1...o.2..F..K.....K-.....
K6.Q.Y..
06:50:08.616340 IP [redacted].172.24.60.49.35588 > [redacted].http: Flags [P.], seq 305:820,
ack 622, win 124, options [nop,nop,TS val 1261892689 ecr 2421791992], length 515
E..7..@..M...<1...P..[.....l/.....
K6.Y.Y..GET /verifpwd.learn?URL=A%5FSPSH%2Ereal&SSL=81Azr7QsbaBb$22zsRI1Bb$22z$217$10vsk
b7r0dh$24BRjxgJvIP$19lsMb57$16$03Yhww HTTP/1.1^M
Host: [redacted]^M

```

FIGURE 5: HTTPS REDIRECT WEBSITE VALIDATES

As part of that authentication, RedirectWebsite then sent three important Client Side Validations all in clear text (represented by green) in Figure 5 that are readable and the GET for Client Side Validation

of the password (verifpwd) as shown in Figure 6. Other in the clear requests followed for Client Side Validation of the browser and first visit.

172.24.60.65	[redacted]	TLSv1	733 Application Data
159.182.165.111	172.24.60.65	TLSv1	1107 Application Data
172.24.60.65	[redacted]	TCP	66 44088 > https [ACK] Seq=1510 Ack=12723 Win=42368
172.24.60.65	[redacted]	HTTP	608 GET /verifpwd.learn?URL=A%5FSPSH%2Ereal&SSL=83n28x
159.182.165.131	172.24.60.65	TCP	66 http > 60928 [ACK] Seq=622 Ack=847 Win=5154 Len=0
159.182.165.131	172.24.60.65	HTTP	1427 HTTP/1.1 302 Object moved (text/html)

FIGURE 6: PASSWORD VERIFY IN THE CLEAR

Additionally, this transition to HTTP revealed a cookie as Figure 7 shows. Boyle and Panko identify the vulnerability and describe the risk of such a capture: “An attacker can intercept the cookie used to authenticate you and then post content as if it came from you. This is a form of session hijacking” (Boyle & Panko, 2015).

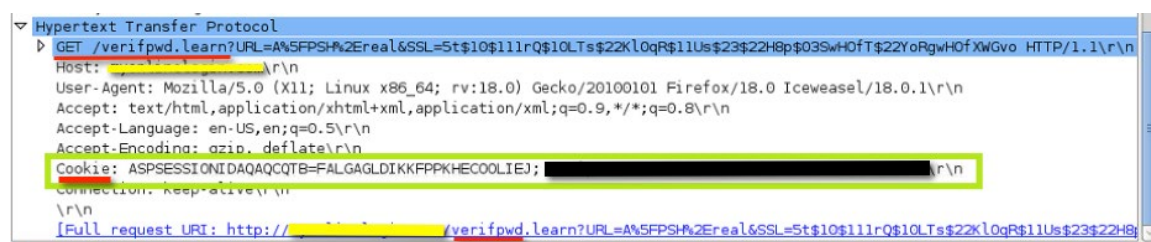
A screenshot of a Wireshark packet capture window. The top pane shows the 'Hypertext Transfer Protocol' details. The request line is 'GET /verifpwd.learn?URL=A%5FSPSH%2Ereal&SSL=5t\$10\$111rQ\$10LTs\$22K10qR\$11Us\$23\$22H8p\$03SwHofT\$22YoRgwHofXwGvo HTTP/1.1\r\n'. The 'Host' field is redacted. The 'User-Agent' is 'Mozilla/5.0 (X11; Linux x86_64; rv:18.0) Gecko/20100101 Firefox/18.0 Iceweasel/18.0.1\r\n'. The 'Accept' field is 'text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n'. The 'Accept-Language' is 'en-US,en;q=0.5\r\n'. The 'Accept-Encoding' is 'gzip, deflate\r\n'. The 'Cookie' field is 'ASPSESSIONID4QAQCQB=FALGAGLDIKKFPKHECOOLIEJ; [REDACTED]\r\n'. The bottom pane shows the 'Full request URI' as 'http://[REDACTED]/verifpwd.learn?URL=A%5FSPSH%2Ereal&SSL=5t\$10\$111rQ\$10LTs\$22K10qR\$11Us\$23\$22H8p\$03SwHofT\$22YoRgwHofXwGvo'.

FIGURE 7: COOKIE IN THE CLEAR

Findings for Lab 2

SafeWebsite redirected to RedirectWebsite using HTTPS TLS only to authenticate the user and keep the user's credentials encrypted. The underlined red areas of Figures 6 and 7 indicate vulnerabilities that were discovered that expose the entire SafeWebsite application that remains unencrypted with TLS and in the clear once a user is authenticated and granted access.tq.

Momentary Use of TLS

After authenticating the user securely under HTTPS TLS, RedirectWebsite returned control via HTTP to SafeWebsite for part of the Client Side Validation process in the GET regarding verifpwd shown in both Figures 6 and 7. A vulnerability was disclosed as all the major functions of SafeWebsite such as recording of grades, posting of work, and so forth would subsequently be done in the clear. The exercise was to employ passive sniffing and not explore breaches of confidentiality so no further forensic work was done in this area.

Client Side Validation Bypass Potential

Following user authentication by RedirectWebsite there was a return to HTTP as shown in Figures 6 and 7. There were additional password, browser, and first visit verifications that were done by SafeWebsite all in clear text. SafeWebsite documented the validation process well, which in turn, would facilitate future exploitation. The vulnerability of Client Side Validation bypass was identified.

Session Cookie Was Captured

Figure 7 revealed a sniffed session cookie and the vulnerability of session hijacking was identified.

LAB 3: USER PASSWORD CHANGE PROCESS

Lab 3 focused on the remaining password-related function of the password change process. Having shown in Lab 2 that SafeWebsite made only a momentary use of SSL/TLS to authenticate, and then reverted to unencrypted traffic, the teams were interested to see how the remaining password-related process of changing a password would be handled. The objective was to discover any other vulnerabilities that might be disclosed. A user host Kali VM, SafeWebsite and Wireshark or tcpdump would be used for packet capture and Wireshark for packet analysis. The objective of the lab was to determine if SafeWebsite's process for handling a change in password was secure and that SafeWebsite remained secure for subsequent application processes.

Packet Capture

Wireshark or tcpdump on Kali Linux was used to capture the packet traffic between the student Kali host and SafeWebsite. This capture was turned on prior to typing in the destination URL into the browser and was terminated after 1000 packets and saved as Lab3.pcap.

Packet Analysis

The Lab3.pcap file was analyzed as previously performed in Labs 1 and 2 using Wireshark. The Lab 3 exercise outline followed Lab 2 to a successful login. At that point the capture revealed that the user had been redirected from HTTPS RedirectWebsite (yellow in figure 5) to HTTP SafeWebsite (green in figure 5) and the user traffic was unencrypted. The user “Profile” tab within the website was selected and the password change

function initiated. The Old Password and New Password were entered. Figure 8 shows in clear text the associated HTTP green packets, redacted target website URL information in black, and, finally, at the bottom three redacted boxes that contained respectively the User Email Address, Old Password, and New Password. All three credentials, in addition to the associated cookie are underlined in red as they are all discovered vulnerabilities. Furthermore, all were in clear text.



```
Frame 4821: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
Ethernet II, Src: Vmware_00:03:22 (00:50:56:00:03:22), Dst: PaloAlto_39:1c:30 (00:1b:17:39:1c:30)
Internet Protocol Version 4, Src: 172.24.60.65 (172.24.60.65), Dst: 159.182.165.131 (159.182.165.131)
Transmission Control Protocol, Src Port: 45902 (45902), Dst Port: http (80), Seq: 5401, Ack: 14961, Len: 48
[2 Reassembled TCP Segments (1496 bytes): #4820(1448), #4821(48)]
Hypertext Transfer Protocol
POST /Shared/Portal/CustomProfiles/PostProfile.real?47=25378158 HTTP/1.1\r\n
Host: [REDACTED]\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:18.0) Gecko/20100101 Firefox/18.0 Iceweasel/18.0.1\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Referer: http://[REDACTED]Shared/Portal/CustomProfiles/A_Profile.real\r\n
[truncated] Cookie: ASPSESSIONIDQABRBTBC=HEJCAHEDJPKOBCEPJEBEDKKH; [REDACTED] ECUSERPROPS=
Connection: keep-alive\r\n
Content-Type: application/x-www-form-urlencoded\r\n
Content-Length: 121\r\n
\r\n
[Full request URI: http://[REDACTED]Shared/Portal/CustomProfiles/PostProfile.real?47=25378158]
Line-based text data: application/x-www-form-urlencoded
EMAIL=[REDACTED]&PASS1=[REDACTED]&shdnOldPwd=Y&PASS2=[REDACTED]&PASS3=[REDACTED]
```

FIGURE 8: ID/EMAIL ADDRESS, OLD PASSWORD, NEW PASSWORD & COOKIE IN CLEAR

Findings for Lab 3

Only the user authentication that occurs under HTTPS TLS in RedirectWebsite is encrypted. Once the authentication is completed, the user is returned to HTTP (noted as green bars in Figure 8) in SafeWebsite for further processing, including entering Profile and the change of password process. All credentials, User Email Address, Old Password and New Password, and session cookie are in clear text and are vulnerable to exploitation as noted by red areas in Figure 8. All subsequent interaction between the website and user is unencrypted. Additionally, all the vulnerabilities identified in Lab 2 remained and were exploitable.

Password Change Process Reveals User Credentials in Clear Text

All credentials, User Email Address, Old Password, and New Password, were discovered to be exploitable and in clear text.

Session Cookie Was Captured

Figure 8 revealed a sniffed secure session cookie and the vulnerability of session hijacking was identified the same as in Lab 2.

SQL Injection Potential

Using the captured secure session cookie, SQL injection would become possible that would leave the entire SafeWebsite database vulnerable to discovery.

CONCLUSION

Useful Tools Led to A Successful Outcome

The outcome of the research of this paper was to determine if the SSL-identified login of SafeWebsite was securely authenticating users and protecting personal credentials. The research process introduced students to a real-world scenario. Three research objectives, each represented by a unique lab, were designed to contribute to the research outcome.












	HTTP SafeWebsite	HTTPS Redirect Website	HTTP SafeWebsite
Lab 1 Fake			
Lab 2 Genuine			
Lab 3 Change			
Desired Security			

FIGURE 9: RESEARCH VS. DESIRED SECURITY

SafeWebsite securely handled an attempt to gain access by means of a fake credential, represented by Lab 1. As shown in Figure 9, a fake entry started in clear text with the HTTP login to SafeWebsite (green bar) that immediately redirected to an HTTPS RedirectWebsite that attempted to authenticate a fake credential and terminated securely.

Lab 2 evaluated a genuine credential login that followed the HTTP to HTTPS redirection for a secure authentication only to return to HTTP and the entire SafeWebsite functionality unencrypted in clear text. This is shown as HTTP green redirects to HTTPS yellow and then redirects back to HTTP

green as shown in Figure 9. Significant vulnerabilities were disclosed as shown with the dotted red bar. Potentially exploitable vulnerabilities included user impersonation and session cookie hijacking.

Lab 3 analyzed a regularly supported function of changing a password only to discover, again, the reproduction of the vulnerabilities discovered in Lab 2 (HTTP green to HTTPS yellow to HTTP green) but additionally, a surprise to all, that user credentials were completely in clear text and exploitable (denoted by the solid red bar) as shown in Figure 9. These vulnerabilities could lead to user

hijacking, session hijacking, and SQL injection that would make all SafeWebsite databases vulnerable to exploitation.

This research demonstrates the manner in which websites, perhaps including SafeWebsite, that were initially designed without considering security best practices attempted a plug-in band aid of SSL/TLS authentication without considering all the associated interfaces with the main application. The net result is an indication to users that HTTPS TLS is employed and a continuation as though all is secure with sufficient complexity that the normal user does not look for the security padlock on all subsequent Web pages. This is a good example of “Security by Obscurity” that prevails more often than not on many websites where an introduction to TLS security at a key stage, like authentication, causes most users to assume that the remainder of the website remains secure.

Figure 9 demonstrates the Desired Security design recommended by all four teams that shows the continued use of HTTPS, even following authentication, for usage of all SafeWebsite functions.

The greatest concern by all the team members was that this reported research was done in a passive mode with well-known open-source penetration testing tools that are publicly available. Additionally, there is concern with what might be done with other readily available tools that could cause significant compromise.

It took several years for major internet Web providers such as Google and Yahoo to use HTTPS for their email products. The transition was not easy because of the additional computation time required to send all traffic over an encrypted SSL/TLS tunnel. They found, however, that security benefits for the users outweighed performance and they ultimately implemented security best practices (Schoen, 2013; Shillace, 2010).

ACKNOWLEDGMENT

The authors are grateful to the National University administration, staff, and faculty for providing support for cybersecurity research. We appreciate the students who performed these labs as part of the MS CSIA program.

REFERENCES CITED

- Agile (2013). Agile Software Development, Retrieved December 28, 2013 from http://en.wikipedia.org/wiki/Agile_software_development
- Agile Manifesto (2001). Retrieved August 5, 2013 from <http://agilemanifesto.org/February2001>
- Bittman (n.d.). Gartner Group, Retrieved 2012 from http://www.gartner.com/technology/symposium/orlando/hot_topic_bittman.jsp.
- Boyle, R. & Panko, R. (2015). *Corporate Computer Security, 4th Edition*, Pearson, ISBN: 978-0-13-354519-7, Upper Saddle River, NJ 07458
- Bradley, T. (2015, January). Security Through Obscurity, Retrieved January 2, 2015 from <http://www.google.com/url?q=http://netsecurity.about.com/cs/generalsecurity/a/aa060103htm&sa=U&ei=b2WnVIKhJsWKyASDwYC YAw&ved=OCDAQFjAF&usg=AFQjCNfXpPkhMdFqGuqsEfi0htWGhemKQ>
- Breithaupt, J., & Merkow M., (2014, July). *Information Security Principles of Success*, Pearson Prentice Hall, 2014, Upper Saddle River, NJ 07458
- CNSS (n.d.). National Centers of Academic Excellence in IA Education (CAE/IAE) Criteria for Measurement. Retrieved August 22, 2013 from http://www.nsa.gov/ia/academic_outreach/nat_cae/cae_iae_program_criteria.shtml
- Dey, P., Romney, G., Amin, M., Sinha, B., Gonzales, R., Farahani, A. & Subramanya, S.R. (2012). A Structural Analysis of Agile Problem Driven Teaching, *National University Journal of Research in Innovative Teaching*, Vol. 5, (pages 89-105)
- Lamping, U., Sharpe, R., & Warnicke, E. (2014). Chapter 6. Working with captured packets. Retrieved June 29, 2014 from http://www.wireshark.org/docs/wsug_html_chunked/ChapterWork.html (Reprinted from *Working with captured packets*, by U. Lamping, 2014, : Free Software Foundation)
- Masnick, M. (2014, August). White House Going With Security By Obscurity, Retrieved January 2, 2015 from http://www.google.com/url?q=https://www.techdirt.com/articles/20140820/15163928269/white-house-going-with-security-obscurity-as-excuse-refusing-to-release-healthcaregov-security-detailsshtml&sa=U&ei=b2WnVIKhJsWKyASDwYCYAw&ved=OCCoQFjAE&usg=AFQjCNf7ZQ3BueQjEbaKp2GUBcQh_acg
- Merkow, M. & Breithaupt, J. (2014). *Information Security: Principles and Practices*, 2nd Edition, 2014, Pearson Prentice Hall, Upper Saddle River, NJ, 07458 ISBN: 978-0-7897-5325-0
- Miessler, D. (2015, January). Security and Obscurity, Retrieved January 2, 2015 from <https://danielmiessler.com/blog/security-and-obscurity-does-changing-your-ssh-port-lower-your-risk>

NIST Server (2008, July). NIST SP 800-123, Guide to General Server Security – SP800-123.pdf retrieved January 10, 2014 from <http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf> p. 2-4

NSA.gov. (n.d.). National Centers of Academic Excellence in IA Education (CAE/IAE)Criteria for Measurement. Retrieved August 22, 2013 from http://www.nsa.gov/ia/academic_outreach/nat_cae/cae_iae_program_criteria.shtml

NUCSIA.nu.edu. (n.d.). Cyber Security and Information Assurance. Retrieved August 23, 2013 from <http://community.nu.edu/csia>

Romney, G.W. (2009). The Integration of Ruby on Rails as an Agile Teaching Tool in ITCurricula. ASEE/PSW-2009 Conference, San Diego, CA

Romney, G.W., Dey, P.P., Amin, M. & Sinha, B.R. (2013). The Flexibility, Agility and Efficiency of Hypervisors in Cyber Security Education, *IEEE ITHET 2013 Conference*, Antalya, Turkey, IEEE Xplore 10.1109/ITHET.2013.6671036

Romney, G.W., Amin, M.N., Dey, P.P. & Sinha, B.R. (2014, April). Agile Development Using Cloud IaaS and PaaS in Computer Science Curricula, *ASEE/PSW-2014 Conference*, Long Beach, CA, April 24-26, 2014

Romney, G.W., Romney, M.D., Sinha, B.R., Dey, P.P., & Amin, M.N. (2014, May). The Power of Rails and Industry Collaboration in Cyber Education. National Cybersecurity Institute Journal (NCIJ). @Excelsior College, 2014. Vol.1 No.1, Pages 56-70, ISSN 2333-7184. <http://ncij.wp.excelsior.edu/>

Schoen, Seth. (2013, January). Yahoo! Mail Makes HTTPS Available. Retrieved January 10, 2015 from <https://www.eff.org/deeplinks/2013/01/yahoo-mail-makes-https-available>

Shillace, S. (2010, January). Default https access for Gmail. Retrieved January 11, 2015 from <http://gmailblog.blogspot.com/2010/01/default-https-access-for-gmail.html>

TCPDUMP (2014). Retrieved June 29, 2014 from <http://www.tcpdump.org/manpages/tcpdump.1.html>

Wireshark (2014). Retrieved November 20, 2014 from wireshark.org

AUTHORS

Gordon W. Romney (Gordon@romney.tv, gromney@nu.edu) is professor of cybersecurity at National University, San Diego, California, in the School of Engineering and Computing and is a Certified Ethical Hacker (CEH). He is a BA physics graduate of Princeton University and contributed to seminal 3D Computer Graphics PhD research at the University of Utah.

Dustin L. Fritz (dustin.1.fritz@gmail.com) is the CISO of Santa Clara County, California, a CISSP, CEH, ECSA, CHFI with an MS in Cyber Security and Information Assurance from National University, San Diego, California. He is an adjunct professor at National University in the MS CSIA program.

The Exclusiveness of Malicious Software Called Spyware and Exploring Mitigating Techniques

Aron Schwartz

ABSTRACT

This research paper was written as a requirement for graduation from Towson University's Information Assurance program. The subject in this paper is spyware, a type of malware that spies on victims' systems and monitors their activities without their knowledge or consent. The paper discusses what spyware is, how it is malicious, its basic and advanced abilities, and how it can harm its victims. One part of this paper discusses the groups of spyware creators and how spyware can send information back to them via covert communications. The paper also discusses ways to mitigate and prevent the spread of spyware. These suggestions include using whitelists over blacklists, proper and effective personnel training, and utilization of security systems such as IPS and IDS sensors.

EXECUTIVE SUMMARY

Computer technology has changed the world and how people interact, some for the better, some for the worse. One thing that has gotten progressively worse is spyware, a type of malware that violates victims' privacy by installing malicious code/programs onto victims' computer systems without their knowledge or consent. Spyware programs gather information about their victims, including but not limited to: system information, keystrokes, Internet browsing habits, passwords, personally identifiable

information (PII), banking information, business plans, email information and usernames. This information is gathered and dispersed in various ways—sometimes via covert channels—to the spyware's owner's command and control (C&C) servers. Once the information reaches its destination, no one really knows what happens to it. Spyware affects individuals and companies alike; no one is safe from spyware victimization. Commercial and government entities along with individuals and criminal organizations can utilize spyware for various purposes that range from data gathering and business to criminal and espionage activity.

Spyware is a pervasive and persistent type of malware that has evolved and improved as technology has improved and will continue to get progressively worse as time goes on. However, there are ways to deal with spyware. Detection and prevention methods include but are not limited to utilizing antimalware and antivirus programs, Intrusion Detection or Prevention Systems (IDS and IPS, respectively), monitoring incoming and outgoing network communications, routinely checking hardware for proper configurations, ensuring that hardware is not maliciously configured for espionage purposes, and effective user training. Technology and organizational policies also need to evolve as threats evolve and worsen.

This paper will examine what spyware is, what it does, how it infects systems, how it gathers victims' information, what it can do with the information, and how the information is sent to human attackers. Covert channels—which are used to send information from a compromised network to an attacker—will be discussed. Solutions and methods

to detect spyware will be discussed in addition to the future of spyware and what it will take to prevent new infection.

INTRODUCTION TO SPYWARE

Spyware is a type of malicious software that steals information from victims' systems and sends it elsewhere. Brown (2011) explained that spyware is type of malware is a combination of the words "spying" and "software." Spyware exists because in the Information Age, information has value (Boldt, 2010). Information that can be stolen includes but is not limited to financial data, personally identifiable information (PII), computer data files, keystrokes, and passwords (Brown, 2011). Spyware is defined as anything that resides on a computer system that tracks, reports, and monitors a victim's activities. It is usually nonintrusive—victims are usually unaware of its presence unless they search for it—which adds to its stealth capabilities. In most cases, without detection software, users will never notice that they have been infected with spyware. It captures information from its victims and reports it to someone else (Brown, 2011). Boldt (2010) defines spyware defined as, "any software which employs a user's Internet connection in the background (the so-called backchannel) without their knowledge or explicit permission."

Spyware is a type of software that is considered by some to be in the grey zone of software—it can be used for malicious or legitimate purposes. It invades its victims' privacy because it ignores their right to be left alone. The term spyware is used to describe tracking software deployed without adequate notice, consent, or control from the user. This type of software is distributed with a specific intent that negatively affects victims in various ways (Brown, 2011).

Spyware collects information for legitimate purposes as well as for illicit financial gain. It can also destroy its victims' systems and—if financial information is stolen—can take organizations or individuals years to restore the damage from spyware infection. It can impair user control over material changes that affect

user experience, privacy, or system security and use of system resources (Boldt, 2010). In addition to gathering data, spyware can also show messages on a computer screen and monitor visited websites and behavior. Spyware can come in many forms including Trojans, part of illicit downloads, infected websites, links from phishing email scams, and from other software downloaded from the Internet (Brown, 2011).

An application is considered spyware in one of two cases: if the application acts deceptively or makes irreversible changes to one's systems. The application can also engage in objectionable behavior without prominently disclosing to the user that it will engage in such behavior in clear and non-technical language (Boldt, 2010).

Businesses can employ spyware to collect and distribute information for financial gain, but there are other kinds of attackers who utilize spyware for malicious purposes. Criminal groups such as organized crime mainly attack systems for monetary gain by using spyware to commit identity theft. They, along with spies, can conduct industrial espionage and attempt large-scale financial theft by utilizing spyware (Leith 2013).

Obviously, foreign intelligence services utilize spyware for its espionage capabilities. They can also develop information warfare programs, doctrines, and capabilities. These intelligence services utilize spyware to make a significant impact on their targets by disrupting and monitoring supply, communications, and economic infrastructures. Industrial spies can also utilize spyware to acquire intellectual property and proprietary knowledge (Brown, 2011).

Phishers can be individuals or groups that execute phishing schemes by applying spyware to steal victims' identities or information for profit. Spammers, like phishers, can distribute unsolicited emails with hidden or false information to do everything from sell products and spread spyware to other machines without a user's consent or knowledge. Last but not least, terrorists and terror groups such as ISIS and

Al Qaida utilize spyware to generate funds, gather sensitive information, support their cause, and attack their enemies (Leith 2013).

SPYWARE CAPABILITIES

Stealing Capabilities

Spyware can track, report, and monitor its victims' activities regardless if a user is offline or online. It can also utilize keylogger software whose detecting capabilities include, but are not limited to, storing users' keystrokes, steal passwords, copy critical files, steal financial and other data, and intercept emails. This malware can expose all of a user's online accounts and cause personal and business financial disruptions (Brown, 2011).

In order to provide attackers with victims' information in a covert manner, spyware communication circuits can be embedded in the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol. Brown (2011) said that, "spyware components are embedded within the sequential and combinational communication circuit structure during synthesis, rendering the distinction or dissociation of the spyware from the original circuit impossible."

Breeds of Spyware

Just as there are breeds of animals, there are breeds and types of spyware. Cookies can be considered spyware because they are used to track user behavior across Internet sites. Cookies can only be retrieved by the website that initially stored them but many sites use the same advertisement provider, which allows cookies to gather much more user information than mentioned above. Web bugs are usually invisible images embedded in webpages that locate a connection between end users and specific websites. Both cookies and web bugs are passive, rely on existing web browser functions and contain no code of their own (Boldt, 2010).

Adware displays advertisements based on user activity that can display everything from commercial content to pornographic ads. They can also report aggregate or anonymous behavior to third parties. Tracks are considered information recorded by an operating system or application about user actions. Although not harmful by themselves, they can be mined by malicious programs and can tell a great deal about a user (Boldt, 2010).

Browser hijackers try to change victims' Internet browser settings such as the start page, search functionality, etc. They mainly affect Windows operating systems (OSs) and can utilize several mechanisms to achieve their goals: install browser extensions, modify Windows registry entries, change or replace browser preference files. This type of spyware can also replace content on websites with promotions from the spyware creators. Spybots are the forerunners to modern spyware; they monitor user behavior, collect log activity, and transfer all of this information to third parties (Boldt, 2010).

System monitor functions are self-explanatory; their functions also make them powerful administrative tools for compiling system diagnostics. Keyloggers are a form of system monitors and were originally designed to record all users' keystrokes to discover passwords, credit card numbers, and other sensitive information (Boldt, 2010).

Other Capabilities

As mentioned above, spyware has become more invasive, its actions more covert, and it steals more information than ever before due to technological improvements. These improvements are driven by money and how quickly one can procure it through technological innovations or implementation. Spyware is no different, and because its creation and actions are driven by profit, it will remain a popular type of malware and will be in use for years to come. More legitimate applications and enterprise applications are being downloaded, thus more spyware is created to infect Internet browsers. Brown (2011) reported that, "any application installed on a computer can perform any action the logged-in user

is authorized to perform.” It logically follows that if there was an exploitable vulnerability in a piece of software, a spyware creator could exploit the vulnerability, gain control of the application, and perform all the actions the application is permitted to perform (Brown, 2011). If workstations and servers are infected with spyware that create vulnerabilities, these vulnerabilities can also be exploitable by other more destructive kinds of malware such as worms, ransomware, and code injection. Worse yet, spyware could allow additional malware to spread through an organization or a victim’s social network (Boldt, 2010).

One or even multiple instances of spyware can consume the computing energy and hard drive space on an infected system, which slows systems down and decreases user productivity. Systems can become unstable, system performance degrades, and copies can be created to make removal difficult. Some instances of spyware are designed to secretly load when an infected system boots up. Victims’ network bandwidth can drop due to a continuous stream of ads—especially ones with lots of in-depth graphics and details—and transportation of personal information. There is even spyware that borrows system processing and hard drive space that is then combined with other victims’ computing resources into a distributed supercomputer that can be rented to the highest bidder. All of these actions can interrupt users from their daily computer activities and negatively influence their overall computer experience (Boldt, 2010).

With all of this information, one would surmise that spyware capabilities are approaching those of a virus or a Trojan; it is installed involuntarily or covertly and can cause destruction on a system. Spyware can also pose as legitimate software—like a Trojan would—such as security software or other required software. Much like a virus, spyware doesn’t stop its activities even if its carrier program (i.e. a file sharing tool) is deleted or terminated. Spyware creators even provide their spyware with the ability to self-update, which allows spyware creators to introduce new abilities over time, including anti-malware evasion capabilities such as polymorphic techniques. Malicious actions of

spyware have increased; spyware also has the ability to spread copies via stolen users’ associates’ emails. Thus, even if a user’s system is secure, he can still be infected by spyware from his friend’s system because his friend has his email address. Spyware does not just infect their victims’ associates, but their businesses and their associated businesses can be affected as well because spyware is designed to convey commercial information to as many users as possible (Boldt, 2010).

Due to its deceptive nature, spyware can even infect a computer by pretending to offer victims a useful service. Some spyware even targets children by offering tools to allow parents to monitor what their child does online only to display targeted ads based on a child’s Internet browsing habits (Brown, 2011). Some spyware could display ads for adult material, which could be displayed inadvertently to children if they use the same infected computers as their parents (Boldt, 2010).

An additional complication is that anti-virus programs do not define spyware as a virus since it does not usually cause destruction. This makes it that much harder for spyware to be found by conventional anti-virus software, especially if the software uses signatures to discover viruses. This, compounded with the fact that spyware is becoming more invasive and gain more destructive capabilities, makes security problematic to preserve (Boldt, 2010).

HOW SPYWARE FUNCTIONS

Coding and Hooking Processes

Spyware can gain information on its infected system and users by monitoring the functions called by a program by intercepting system calls. Brown (2011) explains that this process is called *hooking*: “the analyzed program is manipulated in a way that in addition to the intended function, a so-called hook function is invoked. This hook function is responsible for implementing the required analysis functionality, such as recording its invocation to

a log file, or analyze input parameters.” Functions that form a comprehensive set of capabilities such as communicating over a network are sometimes grouped into an Application Programming Interface (API). The OS uses APIs to perform common tasks; these can be utilized in user mode to make system calls, which is when a user mode application requests the OS to perform a small but specific set of tasks on its behalf. Once a system call is invoked, the system switches into kernel mode. After verifying that the calling application has the authorization to perform the requested action, the task is carried out by the OS on the application’s behalf (Perdisci, 2010).

In many OSs such as Windows, there is a Native API that resides between the system call interface and the Windows API. The Native API changes with each update or service pack and is commonly used by higher-level APIs such as the Windows API to execute system calls or process results. Legitimate applications commonly communicate to the OS through Windows API, but spyware might interact with the Native API directly to evade monitoring solutions. Spyware creators code their spyware to cover all different versions of the Native API, which requires a very extensive knowledge of how Windows functions internally. It is also possible to design spyware to skip the Native API and invoke calls directly from the spyware. Spyware that executes in kernel mode can directly invoke functions without passing through the system call interface. It can also implant hooks into the system to be notified when specific events occur (Perdisci, 2010). Hooking actions are detrimental to a system’s security because antivirus software usually does not monitor the system call interfaces or APIs, which increases spyware’s covert nature (Brown, 2011).

In addition to hooking system calls and APIs, spyware must be able to communicate its information back to some source such as a server. To do that it can access and manipulate file input/output functions (I/O) such as CreateFile and WriteFile because they provide the basic interfaces for opening and closing a communication resource and performing read/write operations. Spyware can perform this action by performing a call to CreateFile specifying COM1 or

some device name and write to the returned handle. The process could use the DeviceIoControl to send command codes to a device.

What Spyware Does with Stolen Information

The information stolen from spyware-infected machines is often sold to third parties. This information can also be used by businesses for marketing purposes, especially if the data is correlated to specific users. This allows businesses to market products and services to users based on their Internet browsing habits, what they spend their money on, where they shop, etc. This information can be sent to numerous servers that belong to a multitude of companies (Boldt, 2010). Spyware also utilizes the HTTP protocol as a means for communicating with its authors or owners and can perpetrate additional actions through the protocol (Brown, 2011).

HOW SPYWARE INFECTS HOSTS

Spyware can infect target systems in many ways, but they share a common theme: they are installed covertly without users’ knowledge or consent. Rootkits can be used because they are built into operating systems and can be used to gain unauthorized access to a system while concealing their actions and presence from users and system administrators. Rootkits can conceal files, registry entries, and memory addresses from the OS or other running programs. Because they are built into an OS they are not considered malware, but can be utilized by malware. In this case, rootkits can install spyware that will be undetected by the user or any antivirus programs (Brown, 2011).

There are even viruses that download a large payload of spyware onto victims’ computers as part of their functions. This was the case with a virus called W32.spybot.worm (Provos, 2007). Spyware can make its variants and alias—altered forms of itself that are concealed in other places on a system

that are et al. not normally reviewed or disguised as legitimate files—in folders and places users will not look at (Brown, 2011).

Spyware must spread to be effective, and the creators can be very creative in how spyware spreads. It can be downloaded or installed from websites, via email or come as part of a software installation. Some spyware is designed to exploit software and operating system vulnerabilities and enter through open ports to infect computer systems. Spyware can also be used by worms to steal information and can act as part of a malicious payload for other types of malware, including logic bombs (Brown, 2011).

Adware can be driven by spyware, which targets users based on their web activities and—when users click on their links or ad pictures—can install more spyware onto a system. Pop-up ads can be conduits for Active-X drive-by downloads, which are very popular spyware distribution mechanisms. A drive-by download occurs when a user accesses a website infected with spyware and forces computers to download spyware, usually without any further interaction from a user. Websites can be infected when attackers identify web browsers such as Microsoft Internet Explorer that enable them to insert small pieces of HTML into web pages. The HTML code is used as a mechanism to test large collections of exploits against anyone who visits the website. These websites can be created to be malicious, or legitimate websites could be infected with spyware. The number of potential victims has increased because web proxies and network access translation (NAT)-controlled devices do not interfere with infection. However, discovering infected websites has fortunately become more difficult due to the increasing size and complexity of the Internet and requires significant resources. Although it is relatively easy to create a malicious website, it is difficult to maintain, especially if the spyware creators need to update their spyware (Brown, 2011; Damodhare, 2013; Perdisci et al., 2010; Munro, 2012)

Ads can be designed to look like Windows Internet Explorer notification boxes to trick users into clicking on them. If a user clicks on these ads, the ad will change the user's browser security settings and

download spyware onto the computer. Ads can even advertise offers to “optimize your system” and even if a user clicks on the “No” button, they still click on the ad, which is enough to push the spyware to download. Ads and websites often advertise links for streaming pornographic or free movies and direct users to pages resembling a media player such as Windows Media Player. The page then asks users to download and run a certain codec, which is actually a spyware binary (Munro, 2012). Users can also download legitimate programs, but spyware could piggyback onto a system with the legitimate software program without the user's knowledge or consent (Damodhare, 2013).

Attackers can also insert malicious HTML code into posts on web bulletin boards instead of creating malicious sites. If the inserted HTML contains an exploit or spyware, it can expose all the visitors to the posts or profile pages. The HTML is usually arbitrary and can include iframe and script tags. Attackers can use automated scripts that exploit the lack of sanitization on the websites and insert thousands of posts with malicious iframes into web boards (Munro, 2012).

In many cases, users unknowingly download spyware programs that masquerade as legitimate programs, such as programs that are required for the application or service users want. Users could be asked to download seemingly innocuous programs in order to stream or download media from websites.

Spyware creators can also cheat the ranking algorithms that web search engines use to sort pages and increase the likelihood of users visiting their infected websites. If a spyware-infected page is listed at a top position for query results, users will be more likely to visit the page (Perdisci, 2010). These are social engineering tactics; they utilize ads and website links to convince users to unknowingly download spyware. Perdisci (2010) stated that, “all techniques that lure a user into deliberately executing malicious code on her machine, possibly under false pretenses, are subsumed as social engineering attacks. There are virtually no limits to the creativity of attackers when social engineering is involved.” Other social

engineering tactics include but are not limited to thwarting webserver security measures, utilizing user-generated content and creating malicious widgets (Perdisci et al., 2010). The main idea behind tricking users into downloading spyware is that if useful software is provided for free, they will download the software without questioning it or being aware of the bundled components they download. Sometimes spyware comes bundled with legitimate software that includes an end user licensing agreement (EULA), which contains information about the bundled software and its capabilities. Users are often loath to read the EULAs due to their length and formal language (Boldt, 2010).

Shareware—particularly file sharing applications—are used as conduits for spreading spyware. Some companies that produce and benefit from spyware work with the shareware producers and pay them to incorporate spyware into their shareware. Sometimes spyware gets bundled with the shareware without the shareware producers' knowledge or consent (Damodhare, 2013).

SPYWARE'S ESPIONAGE CAPABILITIES

Spyware can be classified as different types based on how it does or does not interact with the system it infected. Depending on how different types of spyware interact or do not interact with the OS also affects its stealth capabilities. Type 0 spyware does not interact with any part of the operating system (OS) or other processes using any undocumented methods. Type 1 spyware modifies system resources that were designed to be constant, such as in-memory code sections of the kernel and other processes. Type 2 spyware does the opposite; it modifies system resources that were designed to be dynamic and change constantly. This type of spyware does this by modifying function pointers in many kernel data structures so the spyware code gets executed instead of the original OS or application code. This type of spyware is harder to find because it manipulates system data that is designed to change and it is impossible to automatically verify the integrity of

the whole data section using a hash or data signature. Data sections cannot be signed or hashed (Brown, 2011).

Type 3 spyware is very stealthy because it doesn't interfere with the data or kernel code; there are no hooks in the system leading to the spyware. This type of spyware is completely disconnected from the system code. It could reside somewhere in the memory/RAM and appear as random data, which makes it that much harder for an integrity scanning tool to discover it. Type 3 spyware can take full control of a running system and interfere with it; current examples of this type of spyware utilize hardware virtualization technology (Murphy, 2014).

Because spyware is installed covertly on their victims' systems and sends out information covertly, it is difficult to ascertain exactly what kind of information is being sent (Boldt, 2010). Because technology improves and computer technology can theoretically double every two years, malware can utilize more intrusive and covert actions. Brown (2011) stated that, "anything new, anything unknown, can easily get past a standard IT security system. Any malware utilizing code that hasn't been previously identified as malicious gets through without a problem."

When spyware is executed it can place itself or its variants—altered forms of itself that are usually not scanned by antivirus software or disguised as legitimate folders—into folders that users and scanners will not look at. Sometimes spyware will modify the source code of a legitimate product or modify the actual compiled software by adding spyware into the installation procedure. Thus not only does spyware damage computer systems, it can also damage the reputation and integrity of legitimate software manufacturers (Brown, 2011).

Spyware can remain covertly hidden on computer systems because the instances have methods of evading detection by signature-based anti-virus scanners. These scanners are the primary weapons used against spyware; they match a pre-generated set of malware signatures against a user's files. There are two problems with this: human analysts usually create these signatures, which leaves room for error. The

signatures also prevent the detection of unknown threats because no signatures exist for them. Additionally, signature-based antimalware scanners cannot discover specifically tailored malware. This malware could be used in whaling schemes where the CEO and other executive-level personnel in a company can be targeted with specially made spyware (Perdisci et al., 2010).

Other anti-spyware analysis tools such as intrusion detection and prevention systems (IDS/IPS) are used, but spyware creators devise evasion techniques that prevent the spyware from being analyzed. Some techniques include self-modifying or dynamically generated code as well as capabilities that detect the presence of analysis (Perdisci et al., 2010). Spyware authors will also try to camouflage their code by using multiple layers of obscurity to make reverse engineering and detection by antivirus and web analysis tools more difficult (Brown, 2011).

Packer programs are being implemented in new instances of spyware instead of self-modifying code. These programs automatically change an executable into a syntactically different but semantically equal representation. The packer creates the semantic equivalent by obscuring or encrypting the original binary and hides the result as data in a new executable. The unpacking or decrypting code is added to the data, which decrypts and restores the data upon execution. These restoration actions take place in the memory, which prevents any unpacked versions of the binary to leak into the hard drive. Post unpacking, control is handed over to the unpacked original binary, which performs its intended tasks (Perdisci et al., 2010).

Spyware capabilities that allow it to persist and execute upon system boot are connected to auto-start extensibility points (ASEPs)—code in systems that allow programs to be automatically invoked upon OS boot or when an application is launched. Spyware instances can add themselves to one of the available ASEPs (Perdisci et al., 2010). Spyware can persist in an infected machine by working with another spyware program that is separate but could have been downloaded simultaneously. Victims attempt to destroy the spyware, but the other

spyware will kick in and respawn the other spyware, making it fully functional again. It can also work with its own programming so if it discovers that anti-spyware removed registry keys that it modified or added, it can quickly reinstall them. Some spyware such as Gromozon have the ability to block anti-spyware programs from being installed on a computer or prevent them from running (Brown, 2011).

Spyware can come as a plugin to Internet Explorer (IE) as a browser helper object (BHO) also known as a toolbar. This capability allows attackers to obtain bank account details from users or fetch a list of websites the user visited to deliver customized advertisements to convince said users to make nefarious purchases. BHOs usually retrieve information like this by subscribing to IE's events. These browser events are sometimes fired when a user navigates to a new website by clicking a link or when a page has been fully downloaded and rendered. Some events fire to indicate that a form has been submitted and allow a user's login credentials to be collected (Perdisci et al., 2010). BHOs can obtain the same privileges as the host system that they infect and can penetrate personal firewalls. Thus, any spyware-generated traffic from the BHOs can be difficult to detect because it could be seen as browser traffic (Boldt, 2010).

Covert channels were briefly discussed before; they are the networking channels that function in the background that spyware exploit to send their victims' information to external sources such as command and control (C&C) servers. Historically, timing channels are similar to covert channels, which are mechanisms for communicating information secretly or are difficult to detect. Packet networks are designed to communicate via packet content and their headers, but not the timings. Thus the timing channel used by packet timings affords a side channel that can be used for covert communications. Due to the changes in the 802.XX technology, most computers these days contain a cognitive radio device that runs radio control software. This makes it vulnerable to spyware software or hardware, which utilize covert communication schemes that spy on chip data by exploiting the timing channel—mainly Carrier Sense Multiple Access with Collision

Avoidance (CSMA/CA). These schemes can work in many ways, such as embedding themselves in a machine's media access control (MAC) protocol and avoiding packet transmission collisions by utilizing Carrier Sense Multiple Access with Collision Sense (CSMA/CS)'s back-off rule. This back-off rule confuses packet timings via queuing and introduces a nonstandard disorderly channel that interferes with timing-based communication (Kiyavash et al., 2013).

In the CSMA/CA strategy, the transmission channel is always sensed before any transmission is sent. If the channel is sensed busy, the sender waits until the channel is idle and enters a random backoff period before retrying. The transmission occurs only if—during a fixed period of time equal to a distributed interface state (DIFS)—the channel is sensed idle. If the channel is busy during or instantly after the DIFS, the channel is continuously monitored until it is sensed idle for a DIFS period. CSMA/CA initiates a random backoff interval before transmitting to avoid collisions. For each packet transmission a backoff method is utilized and an acknowledge (ACK) message is transmitted by the receiving system upon successful packet transmission. The ACK is automatically sent at the end of the packet, after a short-time interface space (SIFS) (Kiyavash, 2013).

Spyware can activate by using a trigger, which can come from internal or external sources; it does not need to be constantly active. Spyware's active duration is called the *spying interval*. An internal spyware trigger comes from the hardware and two choices for internal triggers are the states of the registers in the design and the system clock. If a trigger is implemented at the hardware level and integrated into the design of a network interface card (NIC) or computer radio chip, it is impossible to detect the signals by studying radio output. The most common method of sending a spyware activation trigger from external sources is usually executed via covert communication channels (Kiyavash et al., 2013).

The prevailing technology used to develop power-efficient and low-cost communications circuitry is the Application-Specific Integrated Circuit (ASIC) and at least three parties are involved in an ASIC supply chain system: the design company, a

third-party fabrication house and the end user. The design company can insert spyware during circuit synthesis. The spyware and its trigger could be created as point functions, and can be well hidden within the space of the design. So long as the circuit performs its input and output tasks, the secretly stored spyware cannot be distinguished postsynthesis due to its point function capacities (Kiyavash et al., 2013).

Sometimes an organization will use eavesdropper software called *wardens* to monitor its communication channels. Given the close integration of spyware in a computer radio chip's design, the warden will see the exchange of packets but will fail to discover the covert communications in the packet timings. The receiver of the spyware information—which knows about the parameters of the encoding scheme—can decode the information conveyed through the timings. The spyware must be designed to work with the random interarrival time delays in the CSMA/CA protocol, which acts as noise to the packet timings. Sometimes this digital noise is caused by a special case of a first come first served (FCFS) queuing timing channel called the *exponential server timing channel* (ESTC), where service times are independent, identically distributed and memoryless. Kiyavash (2013) stated that, “the ESTC has the smallest capacity among all FCFS queuing channels with the same average service rate, hence a covert communication scheme that can survive the ESTC is most likely robust to other types of queuing noise.”

CSMA/CA is an excellent vector for covert timing channel communications because it constitutes communications at the MAC or Data Processing layers (layers 2 and 1, respectively) of the Open Systems Interconnection (OSI) model and can be implemented in hardware or software. Either way, the MAC needs to interact with the physical layer (PHY), which can be modified without affecting the MAC or displaying any changes to upper layers. The physical layer can also mislead the MAC by providing false timing information to it and can notify the MAC that the medium is busy when in fact it is idle. The MAC layer simply queries the physical layer for medium status and timing

information. One of the most important aspects of espionage at this layer is that the front transmission and packet reception must be conducted at the physical layer. Spyware can be integrated and executed at the physical layer, which is modified so the timing of the sent packets are altered in order to send out stolen information covertly to external recipients (Kiyavash et al., 2013). Brown (2011) reported that, “the spyware components are embedded within the sequential and combinational communication circuit structure during synthesis, rendering the distinction or dissociation of the spyware from the original circuit impossible.”

Victims try to discover the spyware either by attempting to discover spyware circuitry on the radio chip or detecting the timing channel. By closely integrating spyware into a computer chip, neither of these measures is practical (Kiyavash et al., 2013). Users cannot detect spyware by observing power consumption because they can be obfuscated; spyware could be consuming power without advertising that it is consuming power. Kiyavash (2013) reported that, “the specific power consumption number is very dependent on the implementation.”

Countermeasures for covert timing channels consist of detection and disruption. Detection, which was mentioned in the paragraph above, uses statistical tests that distinguish between legitimate and covert traffic. Disruption (such as jamming) of covert timing channels is executed by active eavesdroppers that attempt to prevent covert communication, but at the cost of system performance.

There are many detection methods used to find covert channels, which include the following: the Kolmogorov-Smirnov (K-S) Test, Regularity Tests and Entropy Tests. The K-S Test is used to determine if two datasets—or one dataset and a reference—differ greatly. To detect covert channels, legitimate traffic (without covert communications) is compared to data that has been collected from sources where covert communications are supposedly taking place. If the data from the sources where covert communications might be taking place is noticeably different from the legitimate traffic, then it is declared that a covert channel has been found.

Regularity Tests are based on the belief that covert communications are more regular than legitimate traffic. Entropy Tests hypothesize that the presence of a covert timing channel has an affect on the entropy of a non-covert signal. Another covert channel detection includes the Berk mean-max ratio that tests for covert timing channels. Kiyavash, (2013) stated that, “the mean–max ratio test assumes that the legitimate interpacket delays follow a normal distribution which is often not true for real network traffic.”

In the article that the author utilized for this report, the spyware that was created by the researchers could not be detected by any of the detection methods described above. This is due to the fact that the encoder that the researchers created has a very small overhead and has no impact on the overall power of the platform it was installed on. The spyware was small enough that it could be inserted into non-critical paths in the system radio chip, thus had no affect on the delay of the digital circuitry because it did not affect the critical path of the digital design. Critical path timing determines the speed of the chip. Additionally, the best clarity is achieved when less covert packets are inserted sporadically into traffic, which reduces the covert communication transmission rate.

Spyware capabilities have been explained previously, but their initial information-gathering capabilities can be expounded and amplified with additional malware and added functionality. Spyware can be considered crimeware, which is software written to automate computer crimes and can be used to steal financial data and PII for criminal use. There is also spyware that allows attackers access to an infected machine remotely, especially if the user allows others to remote into their system. Crimeware can spread by using software such as Nmap to search for open ports on a target network and use the ports to install the software remotely (Brown, 2011).

One piece of malware that has spyware capabilities and stood out from other types of malware is Flame. It is the largest piece of malware to date—it is about fifty times the size of an average malware instance. It contains roughly 20 modules in all, some

of which are installed upon initial breach. Flame's creators control which modules are installed on which endpoints in order to gather the most sensitive information from the most valuable places without setting off any antivirus alarms. Not only can Flame self-replicate and infect other systems, it can obtain highly valuable intellectual property from individuals and organizations within seconds of gaining system access. It can also take computer screenshots and log keyboard activity within seconds of accessing a system. It can use five different encryption algorithms and three compression programs to connect to C&C servers. It can scan WIFI and other network traffic for usernames and passwords; Flame is so advanced that it uses cutting-edge technology to find all traditional antivirus programs on the market. It does this in order to use a list of three hundred and forty-six different processes to alter its activity and continue its covert operations (Engele, 2012).

Remarkably, Flame was not designed to clone and propagate itself. The program was designed to obtain specific information from a specific target; the creators did not want Flame to spread like wildfire through networks, enterprises and onto portable devices. Flame is one component that remains inactive until activated by the attacker; he has complete control over where the program goes and what it would do once it infiltrates a target. This adds to Flame's stealth abilities to remain undetected for years. Flame can even be commanded to replicate itself onto removable media if the attackers wish it to do so (Engele et al., 2012).

HOW TO PREVENT SPYWARE INFECTION

After all that has been said previously about spyware concerning its invasive and stealth capabilities, its expanding capabilities and the emergence of a new generation of spyware such as Flame, users and administrators might consider spyware infection prevention and mitigation to be impossible.

There are ways to prevent and mitigate spyware infection, such as utilizing antivirus software, IDS and IPS systems, modifying policy, checking and maintaining hardware, informing and training personnel to be more security-minded. It will not take much capital to purchase what is needed to prevent spyware infection, but it does take time, effort and a thorough understanding of spyware and its capabilities.

The most basic means of preventing spyware infection is to use antivirus software, specifically signature-based software. Signature matching is used to match and identify known threats; antivirus companies must maintain a database of signatures. Personnel then create signatures and compare them against potential threats. Once an antivirus company collects a sample of a new threat to analyze, the human analysts must first determine whether the sample they have—which is so far unknown—poses a threat and analyzes it. If the sample does pose a threat, the analyst will try to find a pattern that will enable them to identify the sample; this is the signature. The pattern will probably be generic enough to match other variants of the sample, but it will not falsely match legitimate software and OS processes. This process is trivial and error-prone, so a better idea would be to utilize an automated approach to rapidly discern between samples that require further analysis and those that are a modification of known threats.

Automatic analysis can occur in two different ways: *dynamic* analysis utilizes techniques that execute a sample and observe its actions and *static* analysis never actually executes the sample (Perdisci et al., 2010).

It is always a good idea to install and activate antivirus software on individual systems; in fact, this should be one of the first things installed on computer systems. An even better idea would be to use a desktop image with preloaded applications that includes antivirus software. Make sure users know to update the antivirus software constantly, or setup the software to automatically update at specific times so users don't have to perform this task. In

addition, users should have personal firewalls activated and updated with the latest rules and access control lists (ACLs).

One option is to also have antivirus software that can be called *collaborative reputation systems* that focus on informing users so they can distinguish between legitimate and illegitimate software based on their individual preferences. If users install new software and are provided with knowledge and tips from previous users of the new software they're installing, they can gauge whether the software is malicious or not. Users can get a good sense of the developer and can investigate the software in question if they are provided more information. These systems can handle individual user knowledge and refine it into a shared knowledge database, similar to IMDB, EBay or Amazon. Users can rate and explain their experiences with certain products and their vendors. One way this system can be effective is to utilize an automatic information push system instead of a pull system where users have to manually pull information. It should also compliment the installation process of an OS so it can notify the user each time previously unknown software tries to execute or install onto a system. When this event occurs, the execution or installation should halt until the new program's information is relayed to the user so the user is properly informed of the new program's capabilities (Boldt, 2010).

This system would mitigate spyware by clarifying individual user knowledge in the system into reputation assessments that will be collectively shared. Both users and legitimate vendors can benefit from this system. Legitimate software vendors can use the system to clarify, promote their software, and explain how it can impact a user's systems. Users would automatically receive suggestions of useful software that has been well received by past users as well as warnings about questionable software (Boldt, 2010).

Here are some general tips on how to prevent or avoid infecting systems with spyware: when browsing the Internet and users encounter any popups or ads and are interested in them, right-click on the ad or link to check its location. Users should always activate popup blocker features in their web

browsers if it is available (Brown, 2011). Users can go to websites such as IP Void (www.ipvoid.com) and URL Void (www.urlvoid.com), copy the location and paste it into the search bars in the websites if it is an IP address or URL, respectively. These websites will use various security sensors to determine if the IP address or URL a user submitted is malicious. Typically the older the URL is, the less malicious and more trustworthy it is. The author is using trustworthy in this manner this because it is a standard belief that absolutely nothing is trustworthy on the Internet due to the plethora of security vulnerabilities. If something looks too good to be true, it usually is too good to be true. If users want to do research on spyware news or preventative techniques, they should view blogs from webmasters and others in the cyber security field. The information can be invaluable and is usually free advice (Damodhare, 2013).

If a user wants to open a USB but the does not know its contents, they should open a file explorer and type in the drive letter in the address bar to prevent any malicious code executions. USBs, CDs, DVDs, Blu-ray disks and external drives should be scanned with antivirus software before users access them. Always scan files downloaded from the Internet because users do not know what is in it or could be hidden, waiting to be executed. Any action a user makes with files could execute malware. Only use one antivirus software instance on an individual computer system at a time. Multiple antivirus applications will conflict with each other, causing them to be ineffective and can create system performance issues. If users do have antivirus software, do not use any antispware, antimalware or antispyware in addition to it. If a system's antivirus has disabled itself without user interaction, the system has been infected with malware. Observe the background processes when the system slows down or malfunctions and shut down any suspicious processes (Brown, 2011). A layered security strategy is advisable, especially since known and unknown threats require different solutions. There is no silver bullet or single, simple solution to all known and unknown problems (Engele et al., 2012).

To deal with new, highly advanced and highly aggressive spyware such as Flame, users must take a proactive path—they should utilize the concepts behind application control and whitelisting security strategies—as opposed to a defense that’s more reactive. Utilizing a proactive *default deny* strategy should keep spyware such as Flame out of networks. This is an excellent strategy to utilize so long as it is maintained, and security hardware and software have the updates to handle new threats. In a proactive security system, enterprise networks using an application whitelisting program would have disallowed installation of the Flame file (WUSETUPV.EXE) even if a valid security certificate were present. Additionally, the file would be reviewed by the IT department, which can approve all programs before allowing the programs access to any systems. This would prevent spyware such as Flame and its variants from gaining access to a network. Using security software that has whitelisting capabilities will prevent highly advanced malware and zero-day attacks (Engele et al., 2012).

Whitelisting allows access to a predefined list of programs or can grant access to a network based on a complicated set of rules. This function provides more effective protection against sophisticated persistent threats and spyware and offers greater authority and comprehension of the programs used in an enterprise. IT departments use traditional antivirus software that provides them with little authority over what users are installing on their systems. Many companies prohibit employees from browsing to sites such as Facebook and 4Chan to avoid executing malware and malicious code. But usually users have carte blanche to install any applications that are not explicitly banned or blacklisted. Organizations utilizing application control and whitelisting know exactly which applications might be running on their systems because this function makes it impossible for users to install anything else unless they obtain prior approval and add the application to the whitelist. Scripts and executables can be managed with digital signing so that even if a custom script executes that originates from a program that has been digitally signed previously, it would be permitted to execute (Engele et al., 2012).

Internet Browsers

Spyware routinely targets Internet browsers by installing toolbars that monitor users’ websites and browsing behavior. In addition to the antivirus and spyware prevention software and techniques described previously, the author recommends using software that applies dynamic analysis techniques to identify events that execute in response to browser events. The system is implemented as a program that provides an interface that convinces a spyware toolbar to believe that it is running inside IE or another browser. When the system identifies and catalogues the event handlers, some events are simulated and the software starts monitoring the components’ reactions. All executed event handlers are checked to see if it includes system calls that allow information to get leaked to an attacker. If a system call is identified, then the toolbar or component is categorized as malicious (Perdisci et al., 2010).

To ensure that users do not visit any malicious websites, Google, Inc. applies simple heuristics to lists of webpages to determine which pages attempt to exploit web browsers. These pages are then flagged as potentially malicious and are monitored via virtual machines to see if drive-by downloads are being initiated when these pages are visited. If drive-by downloads or other malicious actions are being conducted on websites marked as potentially malicious, they will be labeled as malicious in search results to prevent users from visiting them. Additionally, Google keeps track of the malicious webpages and the discovered malware binaries (Munro, 2012).

Of all the Internet browsers that are targeted by spyware, Microsoft’s Internet Explorer is one of the most targeted due to a multitude of security holes in the software and it is still widely used by millions of users (Provos, 2007). Other popular browsers that are not as targeted as IE are Mozilla Firefox, Google Chrome, the Tor browser and Apple’s Safari. Users can enhance their browser’s security features by activating pop-up blockers and blocking ad tracking and analysis software.

Antivirus and Other Antimalware, Detection Methods

Antivirus and anti-malware software come in all shapes and sizes, but it is a very good idea to choose software that has withstood the test of time, has adjusted and increased its security and infection prevention capabilities, and can scan systems without interfering with user productivity. Users should check reliable software review sites such as CNET and ZDNet for information on antivirus and antimalware software. It is a good idea to use a combination of countermeasure tools and strategies because there is no one strategy or tool that will offer full protection (Boldt, 2010).

In addition to the antivirus software described previously, users can also utilize programs that use historical observation to define and prevent spyware infection. This capability is conducted by monitoring specific system configuration parameters, such as the registry and Internet browsers. Users will be alerted to any changes to these aspects of their systems and can choose whether or not to allow the changes. This capability does not require users to constantly update their antivirus or antimalware programs because it relies on what's on their computers currently and changes that occur on their systems (Provos, 2007).

One problem with this capability is that the antivirus does not know which files and downloads are potentially harmful and which are innocuous. This capability is useful if users are trying to monitor spyware and see the system calls that are made to monitor, acquire, compile and disperse information on a user's system (Provos, 2007).

Instead of—or in addition to—antivirus software that function on users' computers, gateway antivirus software can be utilized to monitor data packets that are transferred into and from desktops/endpoints. In order for software like this to function effectively and not degrade network performance, it should meet some requirements. Slow file transmission and fast transmission cannot affect OS file processing by the gateway antivirus that is already running. If many files are being scanned, the antivirus engine should be able to send multiple files using a file

trickling method (Brown, 2011). File trickling or HTTP trickling is a tool that prevents a client from timing out during a file transfer or during virus scanning. It forwards specific amounts of unscanned HTTP traffic to a client to prevent an Internet browser window from timing out while antivirus software scans the files (Brown, 2011). If many files are transmitted at full speed, the gateway antivirus should be able to send every file in order to avoid a long connection waiting state. Simultaneously it should limit its transmission rate but not affect the transmission rates for other connections. If a connection experiences an anomaly or a virus is found, the antivirus should prevent itself from sending the file immediately (TechLibrary, 2013).

Some of the benefits of a gateway antivirus program include the ability to scan emails and their malicious payload before they can infect systems and non-stop protection—signatures are constantly updated, and compressed files can be decompressed and analyzed. Protocols such as HTTP, HTTPS, FTP, TCP, UDP, SMTP, and POP3 are scanned. This gateway antivirus software can also promote safer browsing by preventing malicious file downloads and execution of malicious code (TechLibrary, 2013).

Antivirus software should further enhance their capabilities by utilizing Hookfinder's abilities; it is software that can detect hooking techniques and produce reports on where the system hooks are and how they were implemented. Hookfinder observes a process and detects implemented hooks if it sees that control flow is rerouted to certain processes by earlier changes to the system. It employs data and address taint tracking techniques to perform its monitoring duties; it also can perform detailed impact traces. Perdisci (2010) stated that traces comprise "all instructions that involve tainted data and enables the reconstruction of the method that was used to implant the hook into the system." Based on the trace impact, Hookfinder can display information such as the name of the function that implanted the hook. It can give detailed information on hooks that have not been previously encountered instead of relying on previous knowledge on hooking processes (Perdisci et al., 2010).

Network Security

In addition to antispyware software and endpoint security, the first line of defense on a network is usually a firewall. Firewalls can come in a large variety and can be either software or hardware-based. They are usually placed physically and logically in front of routers to control traffic and access to network systems from the Internet. Personal firewalls protect a computer by blocking malicious attacks while allowing users to perform work using the Internet. Firewalls can alert users of any intrusions and protect critical data from being accessed, stolen, modified or destroyed by attackers (Brown, 2011).

Applications, packets and other objects that travel into and out of a network that must be managed are placed into an access control list (ACL) as firewall policies. Administrators can actually create many ACLs that are configured to allow, block, monitor or shape network traffic based on the list of applications. Applications can be controlled independently or separated into categories and contained as groups (Brown, 2011).

In addition to using gateway antivirus software, users should also consider using software or hardware such as IDS or IPS called network-level behavior clustering systems that scan HTTP and HTTPS packets on their networks because spyware can use the protocol to transmit and receive information to and from its owners. These systems can show similarities between spyware and malware instances that may not be discovered by current system-level behavioral clustering systems (Logasundari et al., 2014)

In addition to these systems, users can also incorporate watermarking to see if spyware or other malware are transmitting on covert channels within their network. Watermarking is used to trace packet flows in a network to discover the source of an attack or attack the obfuscation of a network flow. They exploit timing channels by inserting an identifiable mark that can withstand network effects such as jitters and signal changes, but can remain undetected to an external monitor. There are two types of watermarks: interval-based and inter-packet

delay. Interval-based watermarks work on an interval and can withstand packet loss, but can be detectable via multi-flow attacks. If an attacker monitors a few flows, he can detect the watermark as an unusually broad number of empty time periods that started during the watermark embedding process. Inter-packet delay watermarks change every single delay but are vulnerable to packet loss due to de-synchronization (Mer, 2013).

Active and passive methods are used to analyze traffic. Passive analysis uses the original characteristics of packet flow, but often requires analyzing a large number of packets because the flows can be affected by timing changes during network transmissions. Active analysis strategies inject a signature into the interpacket delays (IPDs) of the traffic flows, which are then divided into interval-based schemes or IPD-based schemes. In IPD schemes, watermark bits are enclosed in the inter-arrival times of the packets (Mer, 2013).

User Training

The most common vulnerability in any network is the user, because they are the ones who unknowingly click on malicious links on webpages and allow their machines to become infected with spyware. Spyware and other malware will continue to persist on networks and endpoints so long as users are uninformed of malware and social engineering attacks. It must be up to information security and IT departments to properly educate users about proper web usage and malicious actions that could affect them, the organization and others.

Information security personnel need to create a user security awareness plan that clearly and succinctly explains the user's role in security. The plan must make users aware of their responsibilities and effectively educate them about best practices. Two benefits of a program such as this are improving employee conformity and increasing the ability to hold employees accountable for their actions. This program should also aim to reduce errors and emissions as well as fraud and unauthorized activity (Brown, 2011).

Users must be made aware of their organization's security policy and how it is enforced within their network, otherwise users will not follow policies and procedures if they are not made aware of them. The program must stimulate users to care about security and remind them of security practices in addition to what could happen should they disobey security policy. Users must be aware that security is part of their organization's mission; security is used to protect an organization's information and that a few extra steps—such as locking computers when they are not in use—go a long way in terms of keeping a network secure. Security awareness messages need to be communicated in a fun and interesting way so users do not tune out the messages, become distracted or bored. Thus, the method of communicating awareness should be changed every so often to pique user interest in the program (Aravindhan, 2013).

A security awareness program should also consist of posters and other marketing media placed throughout work areas to remind users of their duty to maintain information security. Users can also be stimulated to be vigilant for any malicious websites or phishing scams that they encounter and should be rewarded for their actions.

How to Protect Information from Spyware

A good way to prevent spyware from stealing passwords to databases and other valuable resources is to utilize one-time passwords. A one-time password (OTP) is a password that is valid for one login session or transaction and are not vulnerable to replay attacks. A replay attack is when an attacker records an OTP that was already used in a login session but cannot use it again because it is invalid. OTPs were created to make it harder if not impossible for attackers to eavesdrop on transactions and obtain static passwords. OTPs can be time-synchronized (users must input a password within a certain period of time or time will expire and another password will be generated), challenge-based (user must input a value such as a PIN number to cause the OTP to generate) or based on cryptographic processing where passwords are generated from a synchronized parameter such as RSA tokens (Brown, 2011).

Users can also utilize Bump in the Ether (BitE), which prevents malware from accessing important input (i.e. via keyloggers) and securely delivers the input to an application. BitE allows user input to avoid common attack vectors by utilizing a trusted tunnel from the input device to an application. The tunnel is carried out via a trusted mobile device that works together with a host platform. This assumes that the user's mobile device is not infected with spyware or other malware. BitE requires that an association be created between a user's trusted mobile device and his host platform. This must be done for each trusted mobile device and host platform pairing. Applications must also be registered on the host platform for BitE; this action must also be done for each application the user wants to work on. The tunnel is encrypted end-to-end, from a user's mobile device to an application on a host platform (Aravindhan, 2013).

Last but not least, users can utilize an authentication protocol called oPass, which utilizes a user's mobile device and SMS/texting services to counter spyware and password reuse attacks. This protocol requires each website a user wants to authenticate into to possess a unique phone number and a telecommunications provider to assist with registration and recovery phases. Users only need to remember a long-term password to login to all the websites. That's the main concept of oPass—to free users from having to remember each password and type them into every website they authenticate to. oPass uses a user's mobile device to generate OTPs and utilizes the texting service to transmit authentication communications (Aravindhan, 2013). The advantages of using oPass include users not having to input their passwords into any computer at all. The protocol uses texting, which is an out-of-band communication interface; it establishes a secure channel for message exchange. oPass also uses OTP, which is created by the user's mobile device and use a permanent password to access their phones (Aravindhan, 2013).

CONCLUSION

Spyware is privacy-invading malware that steals a myriad of information from a user or an organization. It can include keylogger code, record browser information; can steal passwords and intellectual information, and financial information. As technology improves, so have spyware capabilities; it can now spread to other systems connected to or associated in some way to the system it initially infected and decrease overall system performance. This malware can interfere with the OS via hooking procedures and can remain undetected on a system via polymorphic code, utilize regeneration abilities, and can hide in places where antivirus software might not look. Stolen information can be dispatched to outside sources such as C&C servers via HTTP or covert channels. Because spyware steals information that can be used for financial gain, it will remain very popular in the future.

It may seem difficult to fathom, but there are some very useful tools and strategies that can be employed to combat and prevent spyware infection. Users should utilize antivirus software that have withstood the test of time and utilize advanced capabilities to discover unknown spyware. Watermarking can be utilized to find covert channels and communication in addition to gateway antivirus scanning and IDS/IPS. Users can combat unknown and zero-day spyware and malware with whitelists, which contain software and code that are allowed onto an organization's network as opposed to a blacklist, which lists software that are not allowed. It is much easier to define software allowed because disallowed software lists will continue to grow and will be harder to monitor and control. Last but not least, the most prevalent and dangerous vulnerability in any network must be addressed: users. To assist IT departments with preventing spyware infection, security awareness programs should be created and integrated into organizations so users acquire knowledge on proper Internet browsing habits and their roles in their organization's security.

Spyware will always be prevalent on the Internet, but organizations must understand it and integrate the technologies mentioned above to prevent

infection. Infection can lead to stolen important information (such as intellectual property and business documents) and irreparable damage. There is no silver bullet for spyware and there will never be one because the instances have become more advanced and complex. Only through a well-integrated combination of security technology, prevention mechanisms, and user security awareness will spyware infection be prevented. Organizations must be fluid and adjust their technologies and policies as spyware threats change, or infection will be inevitable.

REFERENCES

- Almeida, F. (2012). Web 2.0 Technologies and Social Networking Security Fears in Enterprises. *International Journal of Advanced Computer Science and Applications (IJACSA)*. Retrieved from <http://arxiv.org/pdf/1204.1824.pdf>.
- Aravindhan, K., Karthiga, R.R. (2013). One-time Password: A Survey. *International Journal of Emerging Trends in Engineering and Development (IJETED)* (1.3 ed., pp. 613-623). Retrieved from <http://rpublication.com/ijeted/jan13/61.pdf>.
- Boldt, M. (2010). *Privacy-Invasive Software*. Karlskrona, Sweden: Blekinge Institute of Technology. Retrieved from [http://digitalamedier.bth.se/tek/aps/mbo.nsf/bilagor/boldt_thesis_v1_02_pdf/\\$file/boldt_thesis_v1.02.pdf](http://digitalamedier.bth.se/tek/aps/mbo.nsf/bilagor/boldt_thesis_v1_02_pdf/$file/boldt_thesis_v1.02.pdf).
- Brown, B. C. (2011). *How to Stop E-Mail Spam, Spyware, Malware, Computer Viruses, and Hackers from Ruining Your Computer or Network*. Ocala, FL: Atlantic Publishing Group.
- Damodhare, S. B., Gulhane, V.S. (2013). Intelligent Malware Detection System. *International Journal of Advanced Research in IT and Engineering (IJARIE)* (2.3 ed., pp. 70-85). Retrieved from <http://www.garph.co.uk/ijarie/mar2013/8.pdf>.
- Engle, M., Scholte, T., Kirda, E., and Kruegel, C. (2012). A Survey on Automated Dynamic Malware Analysis Techniques and Tools. *ACM Computing Surveys* (pp. 1-49). Retrieved from http://www.seclab.tuwien.ac.at/papers/malware_survey.pdf.
- Kiyavash, N., Koushanfar, F., Coleman, T.P., and Rodrigues, M. (2013). A Timing Channel Spyware for the CSMA/CA Protocol. *IEEE Transactions on Information Forensics and Security* (8.3 ed., pp. 477-487). Retrieved from http://colemans.ucsd.edu/wp-content/uploads/2013/09/KKCR_TIFS_2013.pdf.
- Leith, H. M., Piper, J. W. (2013). Identification and Application of Security Measures for Petrochemical Industrial Control Systems." Retrieved from <http://www.sciencedirect.com/science/article/pii/S0950423013002015>.
- Logasundari, C., Menaka, V., Madhubala, R., and Misal, G. (2014). Design and Detection of Covert Timing Channels and Spyware Using Warden Technique. *International Journal of Innovative Research in Computer and Communication Engineering (IJIRCC)* (2.1 ed. pp. 3629-3638). Retrieved from http://ijircc.com/upload/2014/icgict14/575_Logasundari.pdf.

- Mer, H. V., Mehta, S. (2013). Gateway Antivirus Implementation using Open Source Along with Performance Testing and Improvement Analysis. International Journal of Science and Research (IJSR) (2.2 ed., pp. 168-170). Retrieved from <http://ijsr.net/archive/v2i2/IJSRON2013397.pdf>.
- Munro, K. (2012). Deconstructing Flame: the Limitations of Traditional Defenses. Computer Fraud and Security (10th ed., pp. 8-11). Retrieved from <http://www.sciencedirect.com/science/article/pii/S1361372312701021>.
- Murphy, G. (2014). Spyware Removal Tricks and Advice.
- Perdisci, R., Lee, W., and Feanster, N. (2010). Behavioral Clustering of HTTP-Based Malware and Signature Generation Using Malicious Network Traces. Atlanta, GA: Georgia Institute of Technology. Retrieved from https://www.usenix.org/legacy/event/nsdi10/tech/full_papers/perdisci.pdf.
- Provos, N., McNamee, D., Mavrommatis, P., Wang, K., and Modadugu, N. (2007). The Ghost In The Browser Analysis of Web-based Malware. Google, Inc. Retrieved from https://www.google.com/?gws_rd=ssl#q=The+Ghost+In+The+Browser+Analysis+of+Web-based+Malware.
- Rutkowska, J. (2006). Introducing Stealth Malware Taxonomy. COSEINC Advanced Malware Labs. Retrieved from <http://www.net-security.org/dl/articles/malware-taxonomy.pdf>.
- TechLibrary. (2013). Understanding HTTP Trickling. Juniper Networks, Inc. Retrieved from http://www.juniper.net/documentation/en_US/junos12.1/topics/concept/utm-antivirus-full-application-protocol-scan-http-trickle-understanding.html
- Ward, D. O. (2013). Awareness and Training Management. Towson, MD: Towson University. PowerPoint Presentation.

AUTHOR

Aron Schwartz (aks229@gmail.com) graduated with his MS in Information Assurance from Towson University in December 2014. He enjoys family outings, taking care of his pets, and participating in social activities in the Washington, D.C., area. He is currently working in the cyber security field and wishes to expand and continue his career in said field.

Bibliometric Analysis of the Scientific Literature on MOOCs Self Directed Learning (SDL) and Educational Taxonomies

Teresa Ferrer-Mico | Miquel Angel Prats-Fernandez

ABSTRACT

The aim of this study is to locate the scientific literature related with MOOCs (Massive Open Online Courses), Self-Directed Learning competence, and different taxonomies used when designing open online courses. The articles used are from January 1, 2008, to July 31, 2014.

INTRODUCTION

MOOCs (Massive Online Open Courses) are starting to become more popular and known since the first one offered in 2008 by the University of Manitoba. The term MOOC distinguishes a particular type of online course delivery: MOOCs are courses offered for free, online, and at a large scale. The instructional approach is different from a traditional face-to-face class, and even online standard courses. For example, no effective teaching time is allocated for the students; self-paced and independent learning are encouraged and used as teaching-learning methodologies (Haggard, 2013).

There are ongoing discussions and unanswered questions about their effectiveness and appropriateness for higher education and for-credit programs (Brinton et al., 2013). Its value and learning impact is also questioned from pedagogical and curriculum

design perspectives. Dropout rates are still a major concern within this field of study, being around 80% as an average. We are inclined to think that dropout rates can decrease if SDL is better understood and the MOOCs are designed to align with Marzano's educational taxonomy (Marzano & Kendal, 2008).

Educational taxonomies are frameworks created to easily classify items measuring the same educational objective. Educational objectives are the final goals of the education process; they indicate the level of knowledge and understanding reached during the learning process. Historically there had been different proposals and approaches when creating these taxonomies (Bloom, 1956; Simpson, 1966; Anderson & Sosniak, 1994; Marzano, 2001). Each of the taxonomies classifies the learning domains from simple to complex and from concrete ideas to abstract conceptions. Mastering the first levels of these classifications is a prerequisite to move further up, gaining understanding of more complex domains.

Particularly, Marzano's taxonomy (2001) focuses on three domains from simple to complex: Cognitive, Metacognitive, and Self. Within the Cognitive domain the student will be able to retrieve, comprehend, analyze, and use new learned concepts. Within the Metacognitive level the student will be able to set their own goals, monitor their own learning process, as well as monitor for clarity and accuracy. Within the final domain, Self, the student will be able to examine importance, efficacy, and their own emotional response and motivation. Designing MOOCs under Marzano's educational taxonomy framework would target students' self-skills and facilitate own independent learning. MOOCs involve a high degree

of SDL skills and autodidaxy, (Haggard, 2013), therefore a deeper study of this competency will give insights about the relation between the taxonomy and the MOOC design.

The concept of SDL is understood as the learner's ability to guide his/her own learning (Hartley & Bendixen, 2001) and includes different perspectives and models related with different authors (Song & Hill, 2001). It has been described as a goal, a process, a teaching method or a mere learner characteristic (Candy, 1991). It is also known as Inquiry Method or Independent Learning (Knowles, 1975).

An analysis of scientific publications related with MOOCs, SDL competence, and educational taxonomies had been performed to report what type of research is being done within this field, who is doing the research, where it is taking place, and document trends in the publications over time. We opened the research to more taxonomies than just Marzano's with the aim of noting design purposes and strategies more than just counting each of the taxonomies that had been used.

This research will set the baseline, and will help identify gaps in the field of research. Three databases had been used: ERIC, EBSCOhost, and Business Source Complete. The goal of the present study is to analyze the pattern of scientific literature on MOOCs, SDL, and taxonomies over a seven-year period (2008–2014).

MATERIALS AND METHODS

Data Collection

This research presents a bibliometric analysis of articles indexed in ERIC, Business Source Complete, and EBSCOhost databases between 2008 and 2014. All articles are related with MOOC's, SDL competence, and Taxonomies. These databases were selected due to the interdisciplinary characteristics of the research and by volume of articles within the field. The research approach is similar to other methods already applied to bibliographic researches

(Gao, Luo, & Zhang, 2012; Williams, Terras, & Warwick, 2013; Liyanagunawardena, Adams, & Williams, 2013). To accept the articles as reliable for this research the following criteria had to be met:

1. Research focused on MOOCs, SDL, and design in the form of taxonomies
2. No editorial or MOOC review papers were included, avoiding personal opinion reviews
3. Articles written in English

MOOCs are a raising topic nowadays and the publishing rate is expanding exponentially (Rodriguez, 2012). Just a first research about MOOCs presented 2,381 articles and we also obtained 6,090 for SDL competence. Due to the characteristics of the field, and time and relevance limitations, the authors decided to limit the research adding constrictions as per what competence the article focused on and what type of design approach was used. Therefore the final analysis includes MOOCs, SDL competence, and design.

A different variety of research strategies had been used with the aim of retrieving the maximum number of relevant articles. First, we used MOOC, and Massive Open Online Courses as well as SDL and Self Directed Learning. In ERIC database we searched for:

("Massive Open Online Course*" AND "Self-Directed Learn*" as well as "Massive Open Online Course*" AND "taxonom*"). Researches were limited from 01/01/2008 to 07/31/2014.

Similar research was performed in the other databases EBSCOhost and Business Source Complete:

("Massive, Open Online Course*" AND "Self-Directed Learn*" as well as "Massive, Open Online Course*" AND "taxonom*").

The search options also included document type: Journal Article and search modes: Boolean/phase.

Two researchers (Ferrer and Prats-Fernandez) reviewed the selected articles to verify agreement and consistency with the research; duplicates were also removed during this process. Some of the articles were not MOOC- or SD- related but identified by the search algorithm. For example,

we retrieved papers related with “Multiple Optical Orthogonal Code Sequences” or “Management of Organizational Change” and “Service Dominant Logic” as well. The following classification, Table 1, presents the selected papers classified by year of publication and database.

TABLE 1: YEAR OF PUBLICATION AND DATABASES

Year of publication	ERIC	EBSCOhost (full text from publisher)	Business Source Complete	Total	Total [%]
2008 to 2010	1 (in 2009)	0	0	1	3.6
2011	2	0	0	2	7.1
2012	2	0	1	3	10.7
2013	0	7	0	7	25
2014	0	13	2	15	53.6
Total	5	20	3	28	100.00%

RESULTS

The bibliographic search about MOOCs, SDL, and taxonomies between 2008 and 2014 produced 28 relevant articles: 5 retrieved from ERIC, 20 retrieved from EBSCOhost, and 3 from Business Source Complete.

Publication Year

No articles were retrieved from 2008 or 2010, one article was retrieved from 2009, 2 articles from 2011, 3 from 2012, 7 articles from 2013, and 15 articles until July 31, 2014.

Journals

A total of 11 different journals published the 28 articles on MOOCs, SDL, and taxonomies. Table 2 presents the 11 journals that published the articles by year. The journal that has published the most articles is *Journal of Online Learning and Teaching* (n=9) followed by *International Review of Research in Open and Distance Learning* (n=4) and *Distance Education* (n=4), the remaining eight journals published an article each during 2013 and 2014.

TABLE 2: JOURNALS AND YEAR OF PUBLICATION

Journals	2008 to 2010	2011	2012	2013	2014	Totals
Electronic Journal of e-learning			1		2	3
International Review of Research in Open and Distance Learning	1	2	1			4
Distance Education				1	3	4
Communications of the ACM			1		1	2
Journal of Online Learning & Teaching				4	5	9
Education + Training				1		1
Open Learning				1		1
Science of Computer Programming					1	1
Academy of Management Learning & Education					1	1
eLearning & Software for Education					1	1
Educational Researcher					1	1

Institution of the First Author

In Table 3 the articles are classified by the affiliation of the main author and by the publishing journal. Most authors were affiliated with a face-to-face university (71.0%), followed by online universities

(21.0%), and research institutions and independent consultants (8%). We found a high number of international studies (78%) followed by U.S. studies (22%).

TABLE 3: AUTHORS' CLASSIFIED BY TYPE OF INSTITUTION AND PUBLISHING JOURNAL

	Online	Face to face	Independent consultant Research Center
Electronic Journal of e-learning	UOC—Spain: (Esposito, 2012)	University of Leicester – U.K. (Nkuyubwatsi, 2014) University of Tasmania – Australia (King, Kelder, Doherty, Phillips, McInerney, Walls, Robinson & Vickers, 2014)	
International Review of Research in Open and Distance Learning	Athabasca University – Canada (Kop, 2011) Athabasca University – Canada (deWaard, Abajian, Gallagher, Hogue, Keskin, Koutropoulos & Rodriguez, 2011)	University of Florence – Italy (Fini, 2009)	U.K. (Tschofen & Mackness, 2012)
Distance Education	Athabasca University— Canada (Baggaley, 2013)	University of Oslo – Norway (Andersen & Ponti, 2014) École Polytechnique Fédérale de Lausanne – Switzerland (Li, Verma, Skevi, Zufferey, Blom & Dillenbourg, 2014) University of Alberta – Canada (Adams, Yin, Vargas-Madriz & Mullen, 2014)	
Communications of the ACM		MIT – U.S. (Seaton, Bergner, Chuang, Mitros & Pritchard, 2014) University of Massachussets Lowell – U.S. (Martin, 2012)	
Journal of Online Learning & Teaching	The Open University – UK (Beaven, Hauck, Comas- Quinn, Lewis & de los Arcos, 2014)	University of Victoria – Canada (Irvine, Code & Richards, 2013) Queen's University – U.S. (Stewart, 2013) University of Montreal – Canada (Fournier, Kop & Durand, 2014) Glasgow Caledonian University – U.K. (Milligan, Littlejohn & Margaryan, 2013) Oxford Brookes University – U.K. (Waite, Mackness, Roberts & Lovegrove, 2013) University of Helsinki – Finland (Saadatmand, Kumpulainen, 2014) James Madison University – U.S. (Ross, Sinclair, Knox, Bayne & Macleod, 2014) The American University in Cairo – Egypt (Bali, 2014)	

TABLE 3 CONTINUED: AUTHORS' CLASSIFIED BY TYPE OF INSTITUTION AND PUBLISHING JOURNAL

	Online	Face to face	Independent consultant Research Center
Education + Training		University of Technology at Sydney – Australia (Clarke, 2013)	
Open Learning		Pompeu Fabra University – Spain (Daza, Makriyannis & Rovira-Riera, 2013)	
Science of Computer Programming	UNED–Spain (Santos, Boticario & Perez-Marin, 2014)		
Academy of Management Learning & Education		Case Western Reserve University – U.S. (Passarelli, 2014)	
eLearning & Software for Education			Pontydysgu Bridge to Learning – UK (Perifanou, 2014)
Educational Researcher		MIT – U.S. (DeBoer, Ho, Stump & Breslow, 2014)	

TYPES OF STUDIES

All the articles in this research are related with MOOCs, SDL, and design taxonomies due to our focus interest and the journals where had been published. In Table 4 we present a classification by type of research using the one suggested by Liyanagunawardena, Adams, and Williams (2013) in their systematic study of MOOCs. The categories are as follows:

1. Introductory research: the article gives general background information on the research topic
2. Concepts discussions: includes discussion papers on different research topics such as advantages and disadvantages or possible challenges within the field
3. Case studies: case studies focused in one or multiple MOOCs
4. Educational theory: focuses on pedagogical issues and models applied to MOOCs
5. Technology: articles that discuss software use and MOOC's implications from a technology standpoint.
6. Participant focused: research about aspects involving the learners
7. Provider focus: research about aspects involving the providers
8. Other: In this category we have included articles about ethical issues present in MOOCs, design proposals.

TABLE 4: ARTICLE CLASSIFICATION

Categories	2008 to 2010	2011	2012	2013	2014	Totals
1. Introductory research				1		1
2. Concepts Discussion				1	1	2
3. Case studies				2	3	5
4. Educational Theory		2	1	1	4	8
5. Technology	1		1		1	3
6. Participant focused				2	6	8
7. Provider focused						
8. Other						
· Ethic issues			1			1
Total						28

From Table 4 we can see that the studies are mainly focused in two categories “Educational Theory” (28.6%) and “Participant focused” (28.6%) that count for a 57.2% of the total. These numbers show that the trend in MOOC research had been focused on learners, and design and pedagogy, closely followed by “Case studies” (17.9%), “Technology issues” (10.7%), and “Introductory concepts” (7.1%). Finally, “Introductory research” and “Ethical issues” count for 3.6% each.

DISCUSSION

The goal of this study is to present the trends in literature related with three concepts: MOOCs, SDL competence, and design taxonomies. It is particularly relevant on connecting these three fields of research and selecting appropriate and representative articles. Our first research about MOOCs between 2008 and 2014 retrieved thousands of articles (2,381), and even more for SDL competence (6,090). When we combined the terms and also added the taxonomy term, the results were more manageable, retrieving 30 articles. Two of the retrieved papers were never used: one was an

abstract from a dissertation, not being able to access, and the other one found to be irrelevant focused on Virtual Reality and not MOOCs, therefore our final group of papers was 28.

The percentage of papers integrating these three concepts seems to be increasing during the last few years, making the first six months of 2014 worth 53.6% of the total of articles published within this particular window since 2008 (Table 1). ERIC database provided 5 relevant articles, EBSCOhost provided 20 articles, and we retrieved 3 articles from Business Source Complete for a total of 28 relevant papers for this research. The increasing trend in the field seems to be aligned with the current situation in higher education where there is an increase in post secondary education institutions and a decrease in budget, making MOOCs more appealing for institutions and non-traditional students (Irvine, Code, & Richards, 2013). Research on design, technology, and the main competencies students should master in order to be successful in these types of environments is also an increasing research field (DeBoer, Ho, Stump, & Breslow, 2014), and this idea is reflected in the high number of research studies that we classified as Educational Theory (around 30% of the papers); see Table 4.

We could access 20 articles directly from each of the publishers' through EBSCOhost, 5 articles were retrieved from ERIC database, and 3 from Business Source Complete. From Table 2, we can see that the journal with more articles in this research (n=9) is *Journal of Online Learning and Teaching*, followed by *International Review of Research in Open and Distance Learning* (n=4) and *Distance Education* (n=4) making these three journals relevant in the field of MOOCs, SDL, and educational taxonomies. All three are peer-reviewed publications focused on online higher education with an emphasis in open resources.

When classifying the articles by type of institution (see Table 3), 18% of articles were written by authors belonging to U.S. institutions while 82% were written by authors from other parts of the world. This finding is aligned with the fact that there is an increasing interest in creating and researching MOOCs in Europe and internationally (Gaebel, 2013). Being present in the online education field and having international incidence motivates European institutions to invest in MOOCs and their research. There are also economic reasons; the European Commission is investing money and offering resources for its study and investigation. In this sense, U.S. institutions are under a higher

pressure to obtain revenue from MOOCs, while developing new business and education models, than international institutions more focused on not being left behind and keeping up with U.S. development speed.

The high percentage of international researches found in the present study might be also related with the usage of the SDL term. The Bologna process opened the doors to a competency-based global environment for higher education in Europe, increasing research on competencies and educational taxonomies that could foster proper curriculum design to fulfill the program requirements (Sursock & Smidt, 2010).

Figure 1 shows the distribution of articles by country, giving visual information on the interest in publishing about MOOCs, SDL, and taxonomies. USA, Canada and UK had published 6 articles, 3 from Spain, 2 from Australia, and 1 each from Switzerland, Norway, Italy, Finland, and Egypt. One of our research criteria was that the articles had to be written in English, but authors from Canada, Spain, Switzerland, Norway, Italy, Finland, and Egypt might be publishing in journals that accept articles in languages other than English. Those had not been researched within this investigation.

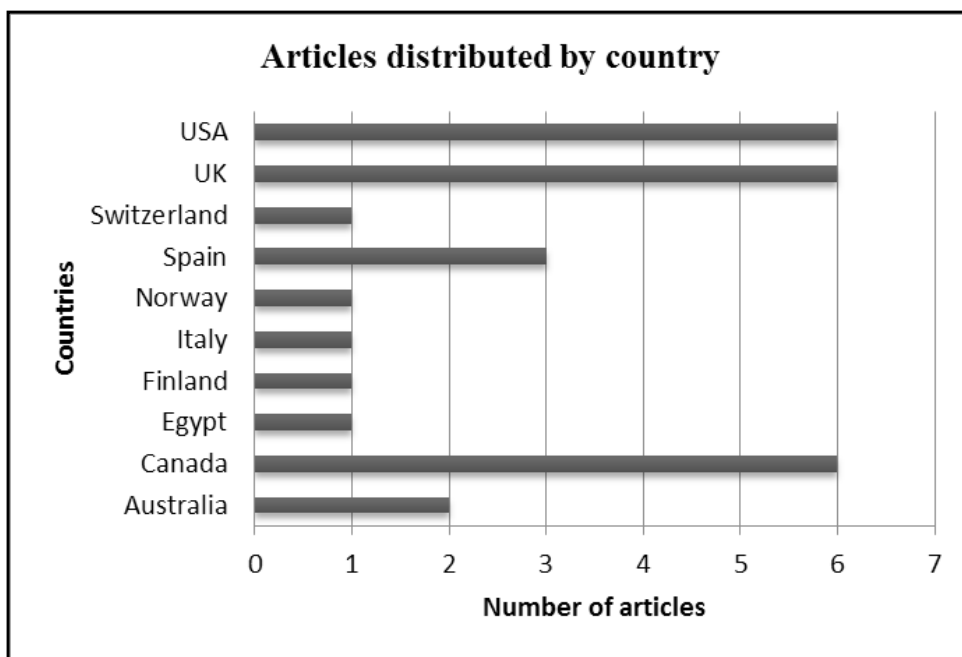


FIG.1: ARTICLES DISTRIBUTED BY COUNTRY

Related with our initial goal of setting a baseline and identifying gaps in the field of research, we would like to conclude that:

Years 2008–2010 set the starting point on MOOC research. The following years show an increasing number of publications, as a reflection of increasing interests in the field.

There is not a high number of articles related with MOOC providers (Learning Management Systems) in our research. This fact could be influenced by the chosen databases, the research strategy, or key words used. We suggest more research within this window.

The topic “Introductory research” also shows low number of publications. This could be because we are not interested in MOOC generic research but in a particular skill and design within MOOCs. This low number is expected and understandable.

The topics “Concepts discussion” and “technology” have also low publication numbers. A modification in the key words might be able to give insights within these fields.

REFERENCES

- Anderson, L.W., Sosniak, L., A. (1994). *Bloom's taxonomy: a forty-year retrospective*. Chicago, IL: University of Chicago Press.
- Bloom, B. (1956). *Taxonomy of educational objectives: the classification of educational goals; handbook I, cognitive domain*. New York, NY: David McKay.
- Brinton, C., G., Chiang, M., Jain, S., Lam, H., Liu, Z., & Wong, F. (2013). Learning about social learning in MOOC's: From statistics analysis to generative model. In Press.
- Candy, P. C. (1991). *Self-direction for lifelong learning: A comprehensive guide to theory and practice*. San Francisco: Jossey-Bass.
- DeBoer, J., Ho, A., D., Stump, G., S., & Breslow, L. (2014). Changing “Course”: Reconceptualising educational variables for Massive Open Online Courses. *Educational Researcher*, 43(2), 74.
- Gaebel, M. (2013). MOOC's: *Massive Open Online Courses*. Retrieved from http://www.eua.be/Libraries/Publication/EUA_Occasional_papers_MOOCs.sflb.ashx
- Gao, F., Luo, T., & Zhang, K. (2012). Tweeting for learning: a critical analysis of research on microblogging in education published in 2008-2011. *British Journal of Educational Technology* 45(5), 783-801.
- Haggard, S. (2013). The maturing of the MOOC: literature review of Massive Open Online Courses and other forms of online distance education, Department for Business Innovation and Skills <https://www.gov.uk/government/publications/massive-open-online-courses-and-online-distance-learning-review>
- Hartley, K., & Bendixen, L. D. (2001). Educational research in the Internet age: Examining the role of individual characteristics. *Educational Researcher*, 30(9), 22-26.
- Irvine, V., Code, J., & Richards, L. (2013). Realigning higher education for the 21st century learner through multi-access learning. *Journal of Online Learning & Teaching* 9(2), 172.
- Knowles, M. (1975). *Self Directed Learning: a guide for learners and teachers*. New York, NY: Association Press.
- Liyanagunawardena, T., Adams, A., & Williams, S. (2013). MOOC's: A systematic study of the published literature 2008-2012. *International review of Research in Open & Distance Learning*, 14(3), 202.
- Marzano, R. (2001). *Designing a New Taxonomy of Educational Objectives*. Thousand Oaks, CA: Corwin Press.
- Marzano, R., J., Kendal, J., S., (2008). *Designing and assessing educational objectives*. Thousand Oaks, CA: Corwin Press Inc.
- Rodríguez, C. O. (2012). MOOCs and the AI-Stanford like courses: Two successful and distinct course formats for massive open online courses. *European Journal of Open, Distance and E-Learning*. Retrieved from <http://www.eurodl.org/index.php?p=archives&year=2012&halfyear=2&article=516>
- Simpson, B. (1966). The Classification of Educational Objectives: Psychomotor Domain." *Illinois Journal of Home Economics* 10 (4):110-144.
- Song, L. & Hill, J. R. (2001). A conceptual model for understanding self-directed learning in online environments. *Journal of Interactive Online Learning*, 6(1), 27-42.
- Sursock, A., & Smidt, H. (2010). *Trends 2010: A decade of change in European higher education*. Brussels, Belgium: European University Association.
- Williams, S., Terras, M., & Warwick, C. (2013). What people study when they study Twitter: Classifying Twitter related academic papers. *Journal of Documentation*, 69 (3).

AUTHORS

Teresa Ferrer-Mico (tferrer@excelsior.edu) is a PhD (ABD) student at the PSITIC research group at Blanquerna University in Barcelona, Spain. Her research interests are Self-Directed Learning, Scratch Programming, MOOCs, and online learning and motivation. She works as an academic program coordinator at Excelsior College in Albany, New York.

Miquel Angel Prats-Fernandez (miquelpf@blanquerna.url.edu) is currently the director of Graduate Studies in Early Childhood Education at Blanquerna University, in Barcelona, Spain. He is also a professor of Educational Online Technology at the same university and the head of PSITIC research group focused on education, society, innovation, and technology. He is a pedagogical advisor for CETEI (Technology Center Ituarte, Cornellà, Spain).

Security in Cyberspace: Part II:

NCI Cyber Symposium Series

Dr. Jane A. LeClair | Matthew Flynn

The escalating threat of cyber warfare between nation states continues to be an important topic of conversation in the cyber community. U.S. government agencies have been attacked, the digital systems of defense contractors breached, and important elements of U.S. critical infrastructure are routinely being probed for weaknesses too often by assailants that remain unknown. To address this issue, on January 27, 2015, the National Cybersecurity Institute (NCI) in Washington D.C., hosted a gathering of notable cyber experts from the military and both private and governmental agencies to discuss the ongoing threats to digital systems in the United States, but by implication, across the globe. The symposium, titled Security in Cyberspace, was held at the main offices of NCI at 2000 M St, NW in the nation's capital. It was the second of three scheduled symposiums each addressing what must be considered in some respects an emerging cyber war. But is this the best terminology to characterize the ongoing security struggles in cyberspace? And even if one uses this label in reference to the varied and often hard-to-define security breaches in cyberspace, what does a cyber war look like? These questions and others became the topic of discussion that Tuesday in Washington D.C.

The event was hosted by Jane LeClair, the chief operating officer of NCI, who introduced the speakers following an informal conversation among the attendees. The panel of guests included Tom Lerach from McAfee, Matthew Flynn from the Marine Corps University, Paul Joyal of National Strategies Inc., and William Williford from Naval Sea Systems Command. The challenge facing all participants was finding commonality in purpose and means when navigating the complex world of network security. Given the differing backgrounds of the participants, divergent points of view were expected to both shape the problem but underscore the need to engage in a conversation seeking congruence in measuring the threat and in advocating better policy. The symposium, in conjunction with the engaged audience of some 20 participants, each braving the threat of impending snow flurries, achieved this purpose to the extent of making clear the need for more discussion of the matter. Ultimately, as is the design of the three-part series, a course of action

needs articulation to forge unity of purpose. That goal is something NCI looks to facilitate in the next iteration of its cyber symposium series.

This second of three symposiums was opened by remarks from Robert Clark from the U.S. State Department, who kicked off the panel discussion by framing the conversation around how the cybersecurity industry has changed and matured over the past 5–10 years. Clark made special note that the current cybersecurity situation was a serious one and this despite the great strides security practitioners have made in bolstering U.S. defenses in that domain. He also made mention of the fact that cybersecurity was an evolving issue and that everyone with a vested interest needed to be working on the same page to combat the threats. The State Department's role in training personnel across the U.S. government to meet this objective is a program he hoped could be complemented by similar efforts in the private sector.

Following Clark's opening remarks, William Williford from Naval Sea Systems Command addressed the gathering. He heads a multibillion-dollar effort to ensure the U.S. Navy can defend its enormous network, guarding its command and control, a clearly vital aspect of naval operations. William offered stern warnings of the dangers of cyber vulnerabilities and cautioned that the activities of hackers needed to be taken very seriously. To provide better security, he stressed the need for a "cyber-safe workforce," that training must "attack this the right way" and that entailed making sure security practitioners strove to achieve "information dominance." He noted that the issue was a complex one that required a "cyber awakening," an integrated effort by everyone involved in cybersecurity. Williford mentioned the problems of hackers attacking control systems and how the most important elements in a system needed to be identified, isolated from attack, and therefore defended. Efforts needed to be made to segregate control of information systems, educate the workforce to ensure all understand the processes involved, and to take the drastic step to unplug wherever possible. Overall, he was confident that the cyber systems in U.S. naval forces were up to the challenge.

Paul Joyal, speaking from his extensive knowledge of the political and military machinery of major foreign powers, looked to shift the discussion to a more conceptual basis, a need to think of the "philosophy" behind the machines. He gave a very thought-provoking discussion of the evolution of cyber attacks and their impact on U.S. national security. He warned that "information technology has lowered the barrier between war and peace." He noted that cyber technology is being used by some state actors, even non-state actors, to identify U.S. vital assets and seek out U.S. network vulnerabilities. This "low intensity conflict" allows aggressive actors in cyberspace, in particular Russia, to use malicious software to infiltrate targeted networks to achieve an ideological dominance derived from information operations. Such an approach has achieved a level of doctrine in some states, so that information warfare has become the opening battleground in any war, not just a cyber war. Consequently, better cyber security is a must, awareness of the full nature of the

threat essential, and the United States must guard against the coming reality that any kinetic action against a sovereign state will first begin with an overwhelming cyber attack.

Tom Lerach from McAfee was the third speaker at the symposium and he spoke at length about how bad actors are gathering data on an increasingly rapid scale, raising complications about our understanding of the Internet of Things (IoT). He noted the threat posed by big data and the threat inherent in the increasing use of 'the cloud' by a vast majority of organizations. These developments fostered a "dark side of the Internet." He was particularly concerned with what efforts organizations have made to 'vet' the administrators and IT professionals who oversee security. All told, networking today when set in a poor security environment allowed "anonymous data" to gather, providing malicious actors a space and a means to compromise network functionality. Among his concerns were the ease of access to systems due to poor user passwords and the tendency of systems that, when rebooted, revert to their original administrative passwords. He also noted the importance of continual monitoring of systems for intrusion, especially for day-one malicious software. In his opinion 'fencing' has value, but it must be buttressed with aggressive actions to thwart those with malicious intent. Important systems and data need to be identified, well-guarded, and segregated from non-essential operations. He concluded by noting that our adversaries are skilled and relentless in their search for data, and we need to be ever vigilant in protecting what is vital to our security.

The final speaker at the event was Matthew Flynn from the Marine Corps University. Flynn acknowledged the ongoing issue of foreign powers seeking to infiltrate U.S. digital systems on all levels, especially in the corporate and government areas. He mentioned, in particular, the activities of China in gaining access to information that can be leveraged for future use in both the commercial and military realm. But he also emphasized the larger parameters of such a struggle in cyber space, a battle to control that medium hinging on a greater understanding of "cyber ideology." Better network security means protecting and advancing connectivity, an idea that

some state actors cannot accept at face value given their restrictive government practices. A complete security picture reminds one that the technical use and functionality of the Internet carries with it a cultural reality too often ignored by those leading the quest for better security in cyberspace. Protection of networks is a necessity, and this effort needs to improve, but safeguarding the implications of the very use of that medium should always be the key aspect of cyber defense. People across the globe want to be connected, and this mandate is contested by many who do understand how better network security may well grant bad actors in the domain the reprieve they seek when confronted by “connectivity.” In sum, Flynn stressed that security should not work at cross-purposes of itself.

Questions from the audience ranged from the technical to the theoretical. Those involved in network defense questioned Mr. Leach’s means to this end. Others expressed a few misgivings about the state of readiness of U.S. naval forces. In general, shared trepidation about delivering better network security continues to advance at the expense of the underlying premise or philosophy undergirding the Internet. The “openness” at large in that medium raises issues of balance, the topic of the third and final symposium of calendar year 2014–2015.

As the guest speakers at this symposium clearly indicated, U.S. national assets in the form of data on digital systems are constantly being attacked by foreign powers and others. In doing so, these threat actors are seeking both commercial and military advantage now and into the future. Defending data is an ongoing and evolving proposition that requires the best efforts from everyone with a vested interest in U.S. national security. This symposium, hosted by NCI and offering various perspectives from experts in the field of cyber security, sought to increase the awareness of the cyber professional’s role in delivering that secure space. That end will be one of computing and greater user awareness, the combination underscoring that people matter most in the Internet of things. The January 15, 2015 symposium “Security in Cyberspace” can be seen in its entirety at <http://www.msn.com/?cobrand=dell13.msn.com&ocid=DELLDHP&pc=MDDCJS>.

AUTHORS

Jane A. LeClair (jleclair@excelsior.edu), EdD, is currently the chief operating officer at the National Cybersecurity Institute (NCI) at Excelsior College in Washington, D.C., whose mission is to serve as an academic and research center dedicated to increasing knowledge of the cybersecurity discipline. LeClair served as dean of Excelsior’s School of Business & Technology prior to assuming her current position. Before joining Excelsior College, LeClair held positions in education and in the nuclear industry, bringing her teaching energies to a number of other colleges while having a full-time career in the nuclear industry. Her work in the industry brought her to the attention of the International Atomic Energy Agency (IAEA) with whom she continues to collaborate. LeClair has also been actively involved in a variety of professional organizations. She is well known for being a vocal advocate for attracting and retaining more women in technology fields. Her areas of interest include social engineering, women in cybersecurity, and cybersecurity training.

Matthew J. Flynn (mflynn92@gmail.com), PhD, accepted a faculty position with the Command and Staff College, Marine Corps University, in July 2012. He has taught at a number of universities and most recently served as an assistant professor at the United States Military Academy, West Point, in both the Military and International Divisions of the History Department. Flynn is a specialist in comparative warfare of the U.D. and the world. His publications include a recent co-authored study titled *Washington & Napoleon: Leadership in the Age of Revolution* (Potomac Books 2012), and books such as *First Strike: Preemptive War in Modern History* (Routledge, 2008), and *Contesting History: The Bush Counterinsurgency Legacy in Iraq* (Praeger Security Int., 2010). Together these works examine a wide range of foreign policy issues across time and in a global context. Flynn received his PhD from Ohio University in 2004 after advanced study in civil-military relations with OU’s distinguished Contemporary History Institute. His general areas of interest are great power status, preemptive war, cyber warfare, and piracy.

