12-1-2008

Information Sharing: Hackers vs Law Enforcement

David P. Biros
Oklahoma State University

Mark Weiser
Oklahoma State University

Jim Burkman
Oklahoma State University

Jason Nichols
Oklahoma State University

DOI: 10.4225/75/57a8260aaa0da
9th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 1st December, 2008

Information Sharing: Hackers vs Law Enforcement

David P. Biros and Mark Weiser, Oklahoma State University
and Edith Cowan University
david.biros@okstate.edu, weiser@okstate.edu

Jim Burkman and Jason Nichols, Oklahoma State University
jim.burkman@okstate.edu, jason.nichols@okstate.edu

Abstract

The fields of information assurance and digital forensics continue to grow in both importance and complexity, spurred on by rapid advancement in digital crime. Contemporary law enforcement professionals facing such issues quickly discover that they cannot be successful while operating in a vacuum and turn to colleagues for assistance. However, there is a clear need for greater IT-based knowledge sharing capabilities amongst law enforcement organizations; an environment historically typified by a silo mentality. A number of efforts have attempted to provide such capabilities, only to be met with limited enthusiasm and difficulties in sustaining continued use. Conversely, the hacker community achieves rapid advancement due to its diligent emphasis on knowledge sharing through technology. The characteristics of knowledge sharing willingness and effectiveness within these two communities create a distinct advantage for hackers. In what follows, these two highly disparate communities are juxtaposed in terms of what drives their relative effectiveness in knowledge sharing efforts. The resulting conclusions lay a foundation for deeper empirical investigation into this phenomenon, which in turn may drive design decisions for emerging law enforcement knowledge sharing platforms such as the U.S.National Repository for Digital Forensics Intelligence.

Keywords

sharing, digital forensics, transactive memory, normative behavior.

INTRODUCTION

It is intuitively recognized that increased sharing of knowledge leads to better outcomes, and research to date has shown that knowledge creation and sharing is a key part of an organization's knowing cycle that positively impacts decision-making (Choo 2002). This paper evaluates the differences in knowledge sharing between the disparate communities of hackers and law enforcement.

Hackers as a group, whether they act for nefarious purposes or to improve security, are most likely to engage in hacking for social reasons, including knowledge sharing, teaching others, and attending conferences (Denning, 1992). Information sharing within this group has grown well beyond simple website postings: Black Hat and DefCon are two of several major conferences that were developed by the hacking community specifically for learning, sharing, and discussing their techniques. In fact, because of the level of sharing and the technical talent of the presenters, they are now considered premier events where all sides of the security debate can come together and communicate.

In contrast, there are few law enforcement (LE) sites to counter exploits that may be used in an illegal manner. Most, such as COPLINK, are used to share specific case information to tie commonalities across jurisdictions in order to identify repeat offenders of various crimes but are not focused on sharing and developing new techniques for solving those crimes. Others, like Cybercop, are much more free-form, providing forums for LE to collaborate and share knowledge in any way, but that same lack of structure is an impediment to analysts and investigators seeking to cull out very specific information relevant to a current case. Security restrictions on these sites also limit the kind of knowledge sharing that will lead to rapid discovery and implementation of counter-approaches. If knowledge-sharing is known to be desirable, what limits LE from doing so on a broader and more consistent basis? How could these limiting factors be moderated?

While studying the network security community, Jarvenpaa & Majchrzak (2005) found that information security personnel preferred to rely on a personal network of friends, or ego-centric groups, for their knowledge-seeking activities. It is proposed that the LE community employ the same behaviors. Rather than store and share their information in a broadly accessible manner on web sites or organizational repositories, LE professionals may, like network security specialists, simply prefer other knowledge-sharing approaches.

There have been some attempts by the LE community to share information, and a few researchers have attempted to build knowledge-sharing systems in support of cyber investigations. However, successful LE knowledge-sharing vehicles seem to be few and far between. This paper conceptualizes the knowledge-sharing behaviors of the hacker and LE communities. The communities are first scoped and their characteristics compared. Preliminary evidence is also offered to suggest why the hacker community out-shares the LE community to such a great extent. Finally, a research model is offered to help frame future research efforts.

SCOPING THE COMMUNITY

The word 'hacker' has evolved over the years from referring to individuals who are knowledgeable about computers to "…persons who deliberately gain (or attempt to gain) unauthorized access to computers." (Furnell and Warren, 1999, p 29). However, many suggest that hacking can go beyond simple access and be accomplished for unauthorized use, the perpetration of other crimes (i.e. child pornography), and the development of tools for carrying out those acts (Whitman and Mattord, 2005, Conklin et al, 2004, Denning, 1999). For the purpose of this study, "hacker" is defined as someone who gains (or attempts to gain) unauthorized access or use of information technology either to its own end or in support of perpetrating other crimes. This includes those who wish to breach information security mechanisms as well as those who have authorized access but seek to use the information technology in an unauthorized manner. For example, an employee who has authorized access to a company computer may hide contraband material in the slack space on the hard drive. The employee may not have used hacking techniques to breach the company's information security defenses, but they used their knowledge to commit another offense.

On the other side of the coin is law enforcement (LE). The term can mean anything from the uniformed patrol officer to a criminal investigator to a district attorney. For the purposes of this research, the definition of law enforcement is limited to those who are assigned or dedicated to the investigation of computer (cyber) crimes and those crimes in which information technologies were used to perpetrate the act. This group (hereafter referred to as LE or the LE community) includes criminal investigators, digital forensic specialists, prosecutors, and other law enforcement officials whose duty it is to support the investigation of computer-related crimes.

These two groups are frequently at odds. Hackers may perpetrate crimes and the LE community enforces the law and investigates crimes. Both groups require some computer knowledge and both can better achieve their objectives by sharing knowledge with others in their communities. Yet, the hackers seem to do a better job of disseminating information to others in their community. The following section offers a comparison of the two communities.

COMPARISON OF THE GROUPS

Hackers and LE personnel have differing motivations for what they do. Hackers seek to gain access and use information systems for a number of reasons. Denning (1999) suggests that they do it for thrills, status, control, power and intellectual discovery. She describes hacking as a "…social and educational*" activity (p. 47). However, like others, she notes that hacking has evolved to include more nefarious acts in recent years.

As a group, hackers enjoy traits that LE does not. For example, hackers can use pseudonyms or "handles" to identify themselves in their social communities. This enables them to benefit from personal anonymity and yet reap the rewards of recognition for their "handle". Table 1 compares the differences in group traits, based on the prior research mentioned.

Hackers	Law Enforcement (LE)
Anonymity	No Anonymity
Recognition (Hacker Handle)	No Recognition
Intrinsic Task-Load	Additional Task-Load
Virtual environment	No Virtual environment
Ego-centric groups	Ego-centric groups
Limited high stakes	High Stakes
Unclassified info	Some classified info

Table 1: Group Differences between Hackers and LE

Anonymity: Hackers share information through websites and communities of practice on the Internet. As noted, in order to maintain anonymity they use "handles." (Denning, 1999, p. 44). While anonymity provides them with a certain level of protection from legal prosecution, it also gives them more opportunities for information sharing. Anonymity has been shown to be critical in group information sharing and decision making (Roa and Jarvenpaa, 1991). It also provides for a domain of deindividuation where social cues are removed and individuals can behave in a manner outside of social norms (Zimbardo, 1969). Further, studies in group work have hypothesized anonymity to be a factor in eliciting group member ideas (George, et al., 1990; Nunamaker, et. al., 1991), and they proposed that "…anonymous communications will be more effective in groups where members are reticent…" (Roa and Jarvenpaa, 1991, p 12).

Recognition: Another factor proven to be a motivator for information and knowledge-sharing is recognition (Butler, et. al, 2004; Chan et. al., 2004; Thomas-Hunt et. al., 2003; Wasko and Teigland, 2002). Building on the Theory of Information Sharing (Constant, et. al., 1994), Chan and colleagues found that members of an on-line group often felt obligated to share knowledge and information when they were recognized as experts in a given knowledge domain (2004). Similarly, Jarvenpaa and Staples (2000) found that recognition and self-efficacy result in a culture of sharing. In the hacker communities, the handles become a pseudo-identity which the individual can use to enjoy the benefits of both anonymity and recognition.

Recognition within the hacker community is derived from a cultural norm to praise the discovery of a hack to a greater degree than the exploitation of a known hack. In other words, the community rewards the discovery of a vulnerability with increased reputation and social standing more so than it does the taking advantage of such a vulnerability after it has been discovered. By way of contrast, recognition in the LE community is frequently accrued to the department or organization rather than an individual.

Task-Load: Understandably, the action of adding information to a knowledge-sharing mechanism such as a webpage, community of practice or shared repository is, to many, simply an additional task in their work day. Disterer (2003, p. 221) notes that while culture is the biggest impediment to knowledge-sharing, it is also "…often seen as additional work." Further, Gil-Garcia and colleagues (2007) note that individual perceptions about expected benefits may play a role. Thus, potential knowledge contributors may need some intrinsic or extrinsic motivation to share.

Virtual environment: Interactions within the virtual world of the internet affords hackers both a sense of community that aids knowledge-sharing and the empowerment of anonymity with regard to rule-breaking behavior. Hackers have a strong knowledge-sharing ethic as evidenced by attempts to socially codify the community's purpose with a declaration of independence of Cyberspace (Barlow 1996) and a central "rule" that

enforces the social validity – even necessity – of sharing information and "freeing" information where it is not publicly available (Guadamuz 2002). Hackers appear to treat information as a public good; in the same manner, information sharing on the internet can be likened to a gift philosophy (Bays and Mowbray 1999) wherein a small content/knowledge donation made by each individual is matched many times over by the aggregate of all the contributions from all the users.

In these environments where knowledge is seen as a public good, such as in a Knowledge Management System (KMS), a variety of antecedents to knowledge-sharing have been studied (Marks, Polak et al. 2008). Of these antecedents, group identification has been shown to be a strong motivator for individuals to provide resources to a common good and can induce pro-self individuals to adopt pro-social behaviors (De Cremer and Van Vugt 1999). In the hacker context, pro-social behavior relates to helping the hacker community, not society at large. LE officials also have a strong sense of community that should similarly create group identification and enhance knowledge-sharing. One could surmise that the moderating effect of group identification on an individual hacker's propensity to share removes whatever edge LE might have enjoyed due simply to their community, however, that has not been fully studied.

Hackers also enjoy a form of anonymity that allows them to simultaneously separate their virtual world identifier (handle or avatar) from their acts, yet also accrue peer recognition and social capital through the persistence of their virtual world identifier through time. Anonymity alone can also act as a driver for hacking; absent other normative factors, individuals who operate under the condition of anonymity (non-identifiability and non-accountability) are more likely to engage in rule-breaking behavior (Nogami and Takai 2008).

Ego-Centric Groups: Knowledge-sharing is a natural phenomenon. However, the way knowledge is shared and with whom it is shared may vary from group to group. In their study of network security professionals, Jarvenpaa and Majchrzak (2005) found that individuals work in ego-centric groups. That is, they work with others whom they perceive are like them. In the network security field, it is common for one specialist to call on a friend for knowledge or information when it is needed. Rather than learn a network security procedure themselves, they rely on their friend or colleague to know what to do. This is what Wegner (1987) describes as Transactive Memory System (TMS) Theory. The users of the information know the knowledge they seek is stored in the minds of the members of their ego-centric network.

Stakes: It is reasonable to assume that the stakes for knowledge-sharing, in terms of risks and rewards, can vary from community to community. This is indeed the case when comparing law enforcement and hacker communities. Of particular interest in this comparison is the manner in which risks and rewards uniquely interact within each of these communities. On this topic, the literature groups rewards and risks into the categories of intrinsic and extrinsic. Intrinsic motivators are explored in depth through the lens of Social Exchange Theory (e.g. Blau 1967) and involve factors such as personal obligation, gratitude, and trust (Bock and Kim 2002). Extrinsic motivators, such as those examined through Economic Exchange Theory, involve factors such as monetary rewards and promotion. From this perspective, knowledge-sharing will take place when the benefits or rewards for doing so outweigh the costs or risks (Kelley and Thibaut 1978; Constant, Kiesler et al. 1994).

The structures and norms of these two communities are unique in that they create a critical interplay between intrinsic and extrinsic motivators. In the case of the hacker community, this interplay appears to have an amplifying effect with respect to knowledge-sharing, where consistently increased knowledge-sharing provides greater rewards while concomitantly reducing the extent of risk to which the hacker is exposed (as shown in Figure 1).

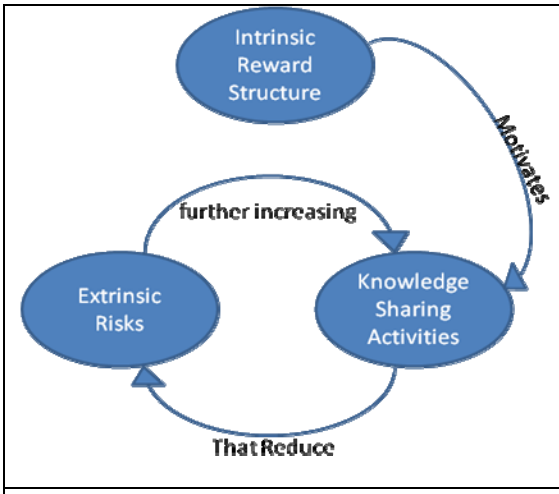

Figure 1: Risk/reward interplay in the hacker community

The benefits for knowledge-sharing in the hacker community are primarily intrinsic in nature and reward participants through improved reputation, recognition, and social standing within the community. However, the drawbacks for knowledge-sharing in this community are decidedly extrinsic in nature, stemming from the legal implications of using such knowledge to perform illegal acts. Through the structure of risks and rewards within the hacker community, and the emergent norms from the community itself, participants are driven to discover novel opportunities for exploitation rather than take advantage of such opportunities. Therefore, the most effective efforts to increase rewards will also mitigate the extent of the risk undertaken for doing so. It is worth noting as well that, while real intrinsic risks exist within the hacker community such as fear of criticism and fear of misleading the community (Ardichvili 2003), the anonymous nature of the community tends to reduce the extent of such risks.

The interplay between risk and reward is reversed for Law Enforcement, however, as reflected in Figure 2. As a hierarchical institution by nature, employees in the field of LE are frequently offered extrinsic rewards for knowledge-sharing including financial incentives, top-down mandates, and promotion.

Research would suggest that the impacts of extrinsic rewards are two-fold: First, such rewards are useful in the early stages of a knowledge-sharing effort, but decrease in effectiveness over time (Kelman 1958; Blau 1967; Kohn 1993). Second, extrinsic rewards can interplay with intrinsic risks in a similar fashion as seen in the hacker community, but with the opposite effect (Kohn 1993). Extrinsic rewards can imply a winner or set of winners, leaving the rest of the community with a sense that they have failed or lost. Within the context of the LE community, this can translate over time into increased intrinsic risk for the sharing of knowledge. This sense of risk is amplified after repeated sharing efforts result in the absence of reward for the majority of the community. This is coupled with a strong extrinsic risk for the use of shared knowledge in the LE community and the impact that such use can have on the outcomes of litigation if the knowledge turns out to be faulty.

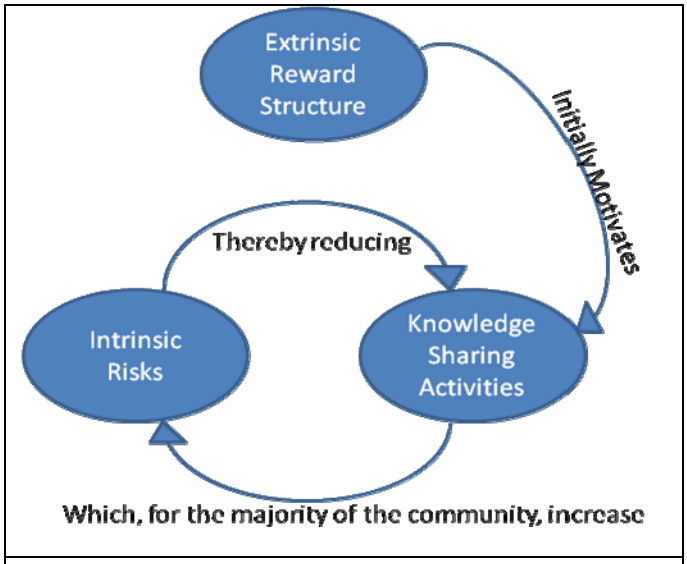

Figure 2: Risk/reward interplay in the LE community

The dynamics of these two communities create a context in which the risks over time for hackers are increasingly low while the rewards remain high. On the other hand, the rewards for knowledge-sharing in the law enforcement community appear to diminish while the risks increase.

Information Sensitivity: In the LE community, different agencies categorize the sensitivity of certain information in different ways. Within the Department of Defense and other Federal agencies, "classified information" is sensitive information, the access to which is limited to specific persons or groups of people by law. Executive Order 12958 (Bush 1993) defines levels of classification and puts special processes in place to grant formal security clearances for access to classified data. There is very specific guidance on marking and handling, as well as penalties for improper disclosure. The following three Classifications are defined in 32 CFR Ch. XXIV (32 CFR, 2008).

"Top Secret" is applied to information whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to national security

"Secret" is applied to information whose unauthorized disclosure could reasonably be expected to cause serious damage to national security

"Confidential" is applied to information whose unauthorized disclosure could reasonably be expected to cause damage to national security

Other countries and international organizations have similar schemes to classify extremely sensitive materials that require special handling. All other information is considered unclassified, although, that does not mean it is not sensitive and would not cause harm to persons or society if improperly released. Because of this, additional sensitivity levels are applied in law enforcement with different purposes:

"For Official Use Only" (FOUO) is not used in a consistent manner in the government, but the Freedom of Information Act (Hamre, 2003) defines it as "unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA)." FOIA specifically exempts law enforcement information which "would disclose techniques and procedures for law enforcement investigations…" The exemption exists whether an item is appropriately marked or not, however, many agencies regularly use this marking for clarity and control of the information. FOUO information is also normally restricted by policy or practice to individuals within the agency that created it and those with whom it is shared.

"Law Enforcement Sensitive" falls into the broad category of "Sensitive but Unclassified", according to the Department of Homeland Security (MD 11042, 2004). Generally, these documents are categorized as being

FOUO, but have specific applicability to law enforcement and prosecution. Most law enforcement investigative procedures and techniques, such as digital forensic processes, fall into this category. Access outside of the agency that controls the data may require non-disclosure agreements and an affidavit that the information is required for law enforcement purposes. Knowing that the receiving individual is appropriately vetted is particularly important to limit discovery by defendants.

In contrast, the hacker community has no regulative levels of information sensitivity. All information appears to be treated equally and there is no concern about information leakage (with the possible exception of a hacker's true identity). Also, there is no concern about penalties for improper disclosure as mandated in the LE community. This absence of the burden of judging information sensitivity before disclosure then reduces the task load of disseminating information to the community. Relative organizational structures have impacts well beyond categorization and dissemination of sensitive data, with influence across many different activities.

ORGANIZATIONAL STRUCTURE

Contemporary institutional theory holds that institutions "…consist of cognitive, normative and regulative structures and activities that provide stability and meaning to social behavior." (Scott, 1995, p. 33). The Hacker and LE communities are guided by very different organizational structures. On the one hand, the hackers have no formalized regulations or explicit protocols to guide their knowledge-sharing behaviors. Instead, they rely on a normative rule of engagement. According to March and Olsen (1989), while normative rules can include codes, paradigms, cultures, and beliefs, much of the focus of organizations remains based on social beliefs. In the hacker community, the operative social belief is that sharing information with others in the community is the norm.

In contrast, the LE community relies more on regulative rules of engagement. North (1990, p4) as quoted by Scott (1990, p36) suggests that regulative organizations "…consist of formal written rules as well as typically unwritten codes of conduct that underlie and supplement formal rules. " This regulative structure is the basis for the law enforcement community. It guides their behavior regarding sensitivity of information, knowledge-sharing, and the implications (i.e. stakes) of information sharing. The normative behaviors or prevailing dynamic in law enforcement institutions is a series of laws and policies by which members are to abide. These rules may run contrary to the sharing of knowledge. For example, rules that govern the protection of sensitive information may run contrary to knowledge-sharing initiatives. LE specialists may be reluctant to share information with individuals outside of their ego-centric groups for fear that it may be leaked to the general public. Specific efforts, therefore, must be made to create and encourage the use of specialized knowledge sharing networks that consider the special social constraints of LE.

KNOWLEDGE-SHARING NETWORK

Using the foundation of the regulative and normative pillars discussed by Scott (1995), the framework in Figure 3 depicts the driving forces behind the information sharing behaviors of the hacker and LE groups. The hackers' information sharing behaviors seem to be driven primarily by normative forces, whereas the LE behaviors are impacted by a combination of the regulative and normative pillars. These forces serve as a foundation for the factors that contribute to their information sharing behaviors.

In the hacker community, the norm is to share knowledge with others. Their culture and norms lead to factors that promote sharing. A somewhat virtual presence allows for the benefits of both anonymity and recognition, and the reward structure is very much intrinsic. Conversely, the LE community is founded on a culture of both regulation and norms. However, its history of not disclosing information (and knowledge) and the potential of leakage or compromise leads to a high stakes environment. Further, the LE community reward systems are primarily extrinsic in nature.

Figure 3: Knowledge-sharing Framework: Hacker vs. LE

ANECDOTAL EVIDENCE OF THE INFORMATION SHARING GAP

As shown in this framework of knowledge sharing, there appears to be fundamental differences in the bases from which hackers and LE operate, and these differences result in very different levels of effective knowledge sharing. Anecdotally, one security expert specializing in the Australian retail banking market bemoans the huge disparity between knowledge sharing between hacker and LE, and succinctly states "Bottom line; they play more like a team than we do and it puts us way behind. (Valentine, 2007)" As anecdotal evidence, he points out that LE attends the Black Hat hacker conferences like RuxCon and DefCon in search of cutting-edge learning, but the hacker community shows no interest in LE conferences. Valentine suggests that the hackers simply have little to learn from LE.

To be sure, LE has been the focus of legislative attempts to enhance knowledge sharing between various agencies since 9-11. One example of this was the swift passage of the Federal-Local Information Sharing Partnership Act of 2001 (HB 1615). Yet, as noted in the public administration sector, "…the presence of technology and the passage of legislation alone are not adequate to make this a reality…" (Zaworski, 2004). Similarly, in 2002 there were approximately 40 US government organizations collecting information but limited in sharing due to statutory and regulatory restrictions and the fact that "elements of the Intelligence Community (IC) verify information from each other (Luzwick, 2002)."

The United States Office of National Intelligence has taken a step toward changing the normative behaviors of the LE community through the adoption of a new Information Sharing Strategy (McConnell and Meyerrose, 2008). Unlike earlier strategies focusing primarily on the mechanics of information sharing, the new strategy specifically offers drivers to transition information sharing from a "Need to Know" approach to a "Responsibility to Provide" and also moves the scope of information sharing from agency-centric to a more collaborative enterprise-centric approach. This regulative approach, however, is placed in opposition to the very open, fast-flowing community of knowledge creation and sharing that exists in the hacker community.

There is likely no direct way to number the sites, groups, and information channels available to the hacker community. There are many entry-level sources such as Usenet newsgroups that cover a myriad of topics such as encryption, general hacking, viruses and copy-protection (Tomel, 2007). Google offers up 6.8 million hits on "hacker forums", and resources regarded by the hacker community as definitive in terms of both defining their culture and creating new hackers are openly available. One such definitive work explicitly offers as core hacker beliefs that "The world is full of fascinating problems waiting to be solved" and "No problem should ever have to be solved twice (Raymond, 2001)." This guide reiterates the notion that the hacking culture "runs on reputation" and is a gift culture, wherein "You gain status and reputation in it not by dominating other people, nor by being beautiful, nor by having things other people want, but rather by giving things away."

For hackers, the domain of information sharing is the Internet, apparently with little restriction. Though there are skill-based distinctions within the hacker community and a loose hierarchy of information access based on those distinctions, hackers from the least skilled to the "elite" work to make their knowledge publicly available (Coyne and Leeson, 2006).

SUMMARY AND FUTURE RESEARCH

Although specifically organized with rigid reporting requirements, rich data sharing has simply not occurred within the law enforcement community to nearly the degree present among hackers. At the heart of this disparity are the different perceptions of rewards and risks for knowledge sharing within the respective communities. Law enforcement structures are intended to increase the likelihood of successful investigation and prosecution, but rigid structure is seen as an impediment to a sustainable knowledge sharing environment. The exact reversal of law enforcement's risk and reward interplay found among hackers creates a great communication and sharing advantage to that group.

Many hacker sites exist and are widely known and referenced within that community, law enforcement, and academia. There are many examples of recognition, anonymity, virtual life and other salient features that have been shown to affect communication in other contexts as well. A broad-based empirical study of their impact on knowledge sharing, however, has not been done and would lead to a better understanding of the impact of each factor.

Efforts continue for improving the degree of knowledge sharing within the LE community. One such example is the National Repository for Digital Forensic Intelligence (NRDFI), an interactive platform for sharing best practices, tools, and tips amongst law enforcement professionals. Though in its early stages, enrollment is strong and interest appears high within the community. As development continues for this emerging platform, two critical directions for future research appear to support the effectiveness of NRDFI: First, the factors laid out herein must be examined empirically in order to understand their impact on the risk/reward structure that drives continued knowledge sharing in the hacker community and stifles efforts in law enforcement. Second, the knowledge gained through such empirical efforts must be translated into actionable design elements for continuing improvement of NRDFI in order to align the context of law enforcement knowledge sharing with the positive feedback exhibited in the hacker community's risk/reward profile. The goal of these efforts will be to propose new theoretical contributions through targeted studies, and then test these contributions by the implementation and analysis of appropriate design interventions within NRDFI itself. Success holds the promise of improved LE knowledge sharing and equal footing in the race for cyber-control.

REFERENCES

32 CFR Ch. XXIV. "Regulations to Implement E.O. 12356: Office of Science and Technology Policy Information Security Program," http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=2d5fe3870032b4142e44de447dc3bcf3&rgn=div8&view=text&node=32:6.2.8.19.1.2.31.2&idno=32, 2008

Ardichvili, A. (2003). "Motivation and Barriers to Participation in Virtual Knowledge-Sharing Communities of Practice." Journal of Knowledge Management 7(1): 64.

Barlow, J. P. (1996) "A Declaration of the Independence of Cyberspace." http://homes.eff.org/~barlow/Declaration-Final.html.

Bays, H. and M. Mowbray (1999). "Cookies, gift-giving, and the Internet." First Monday, 4(11):

Blau, P. (1967). Exchange and Power in Social Life. New York, Wiley.

Bock, G. and Y. Kim (2002). "Breaking the Myths of Rewards: An Exploratory Study of Attitudes About Knowledge-sharing." Information Resources Management Journal, 15(2): 14.

Bush, George W. "Further Amendment to Executive Order 12958 As Amended, Classified National Security Information", http://www.whitehouse.gov/news/releases/2003/03/20030325-11.html, 2003.

Butler, B.; Sproull, L.; Kiesler, S. and Kraut, R. "Community Effort in Online Gropups: Who Does the Work and Why? in S. Weisband and L. Atwaters (eds.) Leadership at a Distance, Lawrence Erlbaum Associates, 2004.

Choo, C. W. (2002). The Strategic Management of Intellectual Capital and Organizational Knowledge. C.W. Choo, Bontis, N. New York, NY, Oxford University Press: 79-88.

Conklin, W.A., White, G.B., Cothren, C., Williams, D., and David, R.L. Principles of Computer Security: Security+ and Beyond, Burr Ridge, IL: McGraw-Hill, 2004.

Constant, D.; Kiesler, S.; and Sprouoll, L.; " What's Mine is Ours, or Is It? A Study of Attitudes about Information Sharing; Information Systems Research, 5 (4), 1994, pp. 400-421.

Coyne, Christopher J. and Peter T. Leeson. "The Economics of Computer Hacking." Journal of Law, Economics, and Policy 1 (2006): 511-532.

De Cremer, D. and M. Van Vugt (1999). Social identification effects in social dilemmas: a transformation of motives. European Journal of Social Psychology, 1996. 29: 871-893.

Denning, D.E. Information Warfare and Security, Reading MA: Addison-Wesley, 1999.

Department of Homeland Security. "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," MD Number 11042, 2004.

Disterer, G., "Fostering Knowledge-sharing: Why and How?" Proceeding of the IADIS International Conference e-Society, 2003, pp. 219-226.

Furnell, S. M. and Warren, M.J., Computer Hacking and Cyber Terrorism: "The Real Threats in the New Millennium?" Computers and Security, 1999, 18, pp. 28-34.

George, J.F.; Easton, G.K.; Nunamaker, J.F., Jr.; Northcraft, G.B.; "A Study of Collaborative Group Work With and Without Computer-Based Support, " Information Systems Research, 1 (4), 1990, pp. 394-415.

Gil-Garcia, J. R., Chengular-Smith, I.S., and Duchessi, P., "Collaborative E-Government: Inpediments and Benefits of Information Sharing Projects in the Public Sector," European Journal of Information Systems, 16 (2), 2007, pp 121 – 134.

Guadamuz, A. L., "The New Sharing Ethic in Cyberspace." Journal of World Intellectual Property 5(1), 2002, pp. 129-137.

Hamre, John J. "DoD Freedom of Information Act (FOIA) Program," DoD Directive 5400.7, 2003.

Jarvenpaa, S.L., and Majchrzak, A. "Developing Individuals' Transactive Memories of Their Ego-Centric Networks to Mitigate Risks of Knowledge-sharing: The Case of Professionals Protecting CyberSecurity," Proceedings of the International Conference on Information Systems, 2005.

Jarvenpaa, S. L. and Staples, D.S., "The Use of Collaborative Electronic Media for Information Sharing: An Exploratory Study of Determinants," Journal of Strategic Information Systems, 9 (2-3), 2000, pp. 129-154.

Kelley, H. and J. Thibaut. Interpersonal Relations: A Theory of Intedependence. New York: Wiley, 1978.

Kelman, M. (1958). "Compliance, Identification, and Internalization: Three Processes of Attitude Change." Journal of Conflict Resolution 2: 51.

Kohn, A., "Why Incentive Plans Cannot Work." Harvard Business Review, 54, Sep.-Oct 1993.

Luzwick, Perry, "Trust Is The Key To Security: Until Governments And Businesses Establish Trust, Knowledge Sharing Will Be Poor And Terrorists And Hackers Will Continue To Have The Upper Hand." Computer Fraud & Security, 2002. pp 15-17

March, J.G. and Olsen, J.P., Rediscovering Institutions: The Organizational Basis of Politics, New York: Free Press, 1993.

Marks, P., P. Polak, et al., "Sharing Knowledge." Communications of the ACM 51(2), 2008, pp: 60-65.

McConnell, J.M. and Meyerrose, D. , "United States Intelligence Community Information Sharing Strategy", Office of National Intelligence, 2008

Nogami, T. and J. Takai (2008). Effects of Anonymity on Antisocial Behavior Committed by Individuals. Psychological Reports. 102, 2008, pp. 119-130.

Nunamaker, J.F.; Dennis, A.R.; Valacich, J.S., Vogel, D.R; and George, J.F.; "Electronic Meeting Systems to Support Group Work, Communications of the ACM, 34 (7), 1991, pp. 40-61.

Raymond, Steven E., "How to Become a Hacker.", http://catb.org/~esr/faqs/hacker-howto.html, 2001

Roa, V.S. and Jarvenpaa, S. L.; "Computer Support of Grous: Theory-based Models for GDSS Research,"Management Science, 37 (10), 1991, pp. 1347-1362.

Scott, W.R. Institutions and Organizations, Thousand Oaks, CA: Sage Publications, 1995.

Thomas-Hunt, M.C.; Ogden, T.Y. and Neale, M.A.' "Who's Really Sharing? Effects on Social and Expert Status on Knowledge Exchange Within Groups," Management Science 49 (4), 2003, pp. 464-477.

Tomel, Justin, "Hacker Usenet Newsgroups", http://e-articles.info/e/a/title/hacker-usenet-newsgroups/, 2007

Valentine, Andrew, "Good Guys Finish Last: Information Sharing is the Key to Fighting Security Intruders", http://www.retailbankingreview.com.au/they-play-like-team.php., 2007.

Wasko, M.M. and Teigland, R. "The Provisions of Online Public Goods: Examining Social Structures in a Network of Practice," in the Proceedings of the 23rd International Conference on Information Systems, 2002 pp 163-171.

Wegner, D. M. "Transactive Memory: A Contemporary Analysis of the Group Mind," in Mullen G. an Goethals, G. (Eds.) Theories of Group Behavior, Springer-Verlag, New York, 1987, pp. 185-208.

Whitman, M.E. and Mattord, H. J. Principles of Information Security, Boston: Thompson Course Technology, 2005.

Zaworski, Martin J., "The Challenges of Law Enforcement Information Sharing in the Post September 11, 2001 Era", PA Times, 27(7), 2004.

Zimbardo, P. G., The Human Choice: Individuation, Reason and Order versus Deindividuation, Impulse, and Chaos," in W.J. Arnold and D. Levine (Eds.) Nebraska Symposium on Motivation, University of Nebraska Press, Lincoln, 1969.

COPYRIGHT