Association for Information Systems
AIS Electronic Library (AISeL)

SAIS 2015 Proceedings | Southern (SAIS)

2015

They Are Not All Enemies: Detecting and Deterring Non-Malicious, Privileged IT User Threat Using an interdepartmental Approach

Xiang Liu
Marymount University, xliu@marymount.edu

Diane Murphy
Marymount University, dmurphy@marymount.edu

THEY ARE NOT ALL ENEMIES: DETECTING AND DETERRING NON-MALICIOUS, PRIVILEGED IT USER THREAT USING AN INTERDEPARTMENTAL APPROACH

Xiang (Michelle) Liu
Marymount University
xliu@marymount.edu

Diane Murphy
Marymount University
dmurphy@marymount.edu

ABSTRACT

The various types of insider threats likely result from different motivations and intentions and involve distinct stakeholders. Thus, a "one size fits all" approach may not be effective for the mitigation of all types of insider threats. In this paper, we take one segment of insiders: the non-malicious, privileged IT users, specifically the IT professionals given "superuser" access. Our goal is to develop a collaborative, multi-disciplinary approach to detect and deter such security threats. We first review the IS Threat Vector Taxonomy where the focus is centered on different types of insider threat. We then take a closer look at non-malicious, privileged IT users and the reasons for noncompliance behavior. Finally, we develop a potential interdepartmental strategy to detect and deter these insider threats.

Keywords

Insider threat, privileged user, non-malicious, deter, comprehensive approach

INTRODUCTION

There has been an increased focus on insider threats in recent years with major incidents such as those perpetrated by Edward Snowden, as well as many data breach incidents that point to involvement of employees or service providers. Many organizations seem unable to effectively detect and prevent such information "exfiltration". These insider threats are a growing concern in all types of organizations and have been raised at the national security level with the development of a National Insider Threat Policy (Obama, 2012).

How serious are these threats in government and industry? Surprisingly, 90% of attacks against organizations are insider attacks (Hong, Kim, and Cho 2010). A survey in the banking industry reporting that insider threats were much more prevalent than two years previous, mainly because privileged insiders are becoming prime targets for cybercriminals and turn "rogue". The study also highlighted contractors and partners as increasing insider threats (Crosman, 2013). In addition, a recent government report noted that 44% of government agencies handling classified data did not meet minimum standards for an effective insider threat program (Johnson, 2013).

To better understand factors affecting data leakage in the global business environment, Cisco commissioned a study that polled more than 2,000 employees in 10 countries. The findings revealed that data loss resulting from employee behavior poses a much more extensive threat than many believed (Cisco, 2008). Additionally, the Software Engineering Institute (SEI) conducted a study and found that some 82% of insider threat incidents were handled internally without legal action. It might be due to the belief that the damage level was insufficient to warrant the cost of prosecution or that there was a lack of evidence definitely identifying the responsible individual (SEI, 2012).

Such concerns are heightened by the increased practice of "whistleblowing", for example, through Anonymous and Wikileaks. It is also important to note that not all insider threat incidents are malicious: often the insider is negligent or skips security measures to make life easier or try to be more efficient due to workplace pressures (Wall, 2013).

Different types of insider threats likely result from different motivations and intentions and involve different stakeholders. Thus, a "one size fits all" approach may not be effective for the mitigation of all types of insider threats. In this paper, we take one segment of insiders: the non-malicious, privileged IT users, specifically the IT professionals given "superuser" access. Our goal is to develop a collaborative, multi-disciplinary approach to detect and deter such security threats based on identifying and tracking human vulnerabilities.

In the U.S., 35% of data breaches were considered to be a result of employee or contractor negligence (human factors), compared with 37% as a result of malicious insider threats (Ponemon Institute, 2013). Insider threats have increased, in part, because of the increased reliance on the supply chain and the increased number of people with privileged access. (Murphy & Murphy, 2013). As businesses rely more and more on electronic transmission of data across the world, it becomes imperative to recognize the impact of the virtual aspects of the supply chain on the business and the increased potential for data breaches and insider threats from anywhere in that supply chain (Wall, 2013).

In the next section we will review the IS Threat Vector Taxonomy where the focus is centered on different types of insider threat. We then take a closer look at non-malicious privileged IT users and the reasons for noncompliance behavior. Finally, we develop a strategy to begin to detect and deter these insider threats.

THE IS THREAT VECTOR TAXONOMY

Insider threats encompass different motivations and situations. The threat taxonomy was developed originally by Loch et al. (1992) and extended by Willison and Warkentin twenty years later (2013). As shown in Figure 1, internal human threats fall along a continuum, with passive and non-volitional violation of security policies at one end and intentional, malicious computer abuse at the other end. In between these two extremes is the type of insider threat we focus on: volitional behaviors that are not necessarily motivated by malicious intentions. Four characteristics depict this type of behavior: intentional behaviors (e.g. violating policy because they do not perceive it applies to them); accidental events such as human error or power outages; self-benefiting actions without malicious intent (e.g., using default passwords to save time and effort); and voluntary rule breaking (e.g., failing to comply with the security policy to make data backups because of time constraints) (Guo et al. 2011).

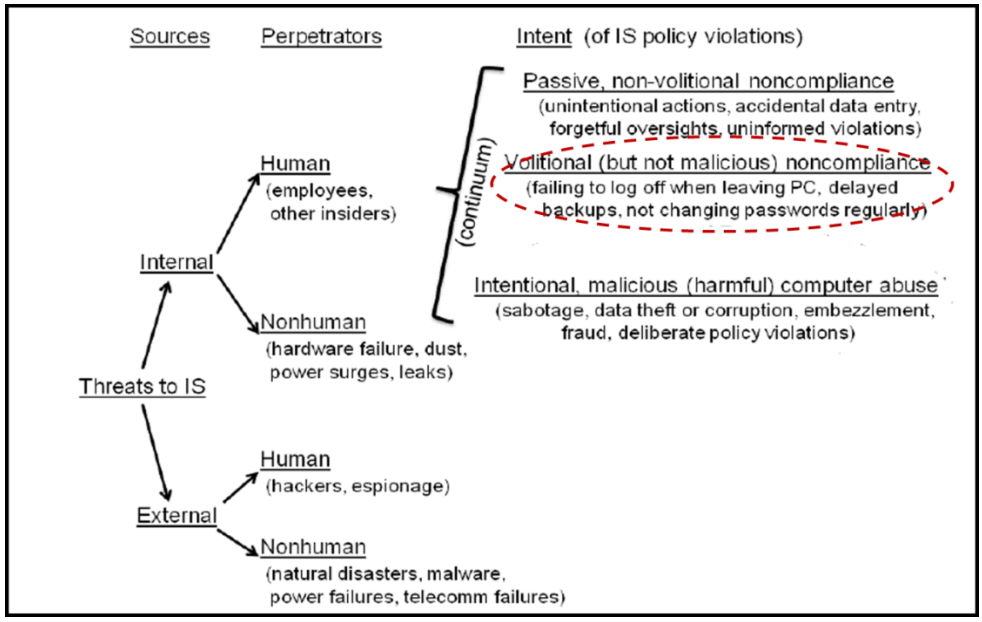

Figure 1. IS Security Threat Vector Taxonomy (Adapted from Willison & Warkentin 2013)

The US-CERT (Computer Emergency Readiness Team) disclosed that from 2009 to 2013, the number of reported breaches of federal computer networks (i.e., the .mil and .gov domains) rose by 73% (https://www.us-cert.gov/). Based on an analysis of information obtained through Freedom of Information Act (FOIA) requests, at least half of these U.S. government IT security incidents were the result of mistakes made by workers, including the incidents of violating workplace policies; losing or having stolen devices containing sensitive information; and sharing sensitive information without malicious intention (The Associated Press, 2014, November 10). Motivations and drivers behind these behaviors are conspicuously different from the malicious system sabotage and abuse by so-called "enemies within". Examining these insider threats is important for "responding legally to related problems when they arise and for preventing them from re-occurring" (Wall, 2013, p.108).

There are some repositories of insider incident reports such as from Privacy Rights Clearinghouse (2013) and from the SEI (2013). However, these generally represent only those for which legal action was taken, known to be only a small percentage

of the total cases. As the number of insider attacks is increasing, current reactive security practices do not seem to be effective. What is needed is a more proactive and collaborative approach to detect an insider threat from a privileged insider and for action to be taken against the individual with human vulnerabilities to deter the incident from occurring again.

A CLOSER LOOK AT PRIVILEGED USER RISK

Of particular concern is the threat posed by IT professionals who have "superuser" access and the knowledge, skills and opportunity for exploitation. In today's networked world, the privileged IT user includes current or former employees, interns, contractors, consultants, as well as workers from suppliers, outsourced service providers, including those working in other countries, and other business partners. A recent study defined a privileged user as "anyone who has elevated access to data, systems and computer assets within a company" (Raytheon, 2014, P.5). It includes database administrators, network engineers, IT security practitioners and cloud custodians.

Privileged IT users pose the most extensive threat of damage and greater security risk due to factors such as given in the table below (Raytheon, 2014):

Greater access to assets including both computing devices such as laptops and USB devices and intellectual property such as confidential customer information
Common mentality that the privileged user are somehow "above the law" and not subject to security restrictions
Authorized to make changes and access data at high levels and remove any trace of these actions
Inadequate or no monitoring or self-monitoring

Table 1. Why Privileged IT Users Pose Greater Security Risk

In addition, there are other environmental factors which make them potential insider threats including those shown below:

The shortage of qualified IT professionals which makes the hiring process focus on IT skills rather than personality factors
The high turnover rate in the profession with most IT employees changing jobs every 2 to 3 years
The large amount of contracting work and consulting assignments with short-term time-frames
The sense of ownership about their work and their desire to take that with them to their next assignment

Table 2.Environmental Factors Causing Potential Insider Threats

Other important factors affecting the behavior of privileged IT users include the nature of the work (Akersredt, 2003); outsourcing to other parts of the world; routinely copying files to USB or private email to work at home or on another site; skipping security measures to get something done; very technical activities that can only be done by one person; workplace pressures to solve problems quickly, and so on. Privileged users are skilled IT individuals who are capable of violating security policy with a high probability of not being quickly discovered.

Who monitors privileged users? In most cases, the IT department does the monitoring and so they end up monitoring themselves: not a great incentive to the IT privileged user who either is doing the monitoring or is being monitored by one of their colleagues.

AN INTERDEPARTMENTAL STRATEGY TO DETECT AND DETER THREAT

Firstly, we need to understand what factors are likely to drive a privileged user's violation of security policy. Insider noncompliance does not just happen to anyone in the organization; they occur in response to the environment and past behavior and are reinforced by the lack of consequences of the behavior, such as a low number of prosecutions. It is necessary to identify and investigate the precipitating factors of a worker's intention to violate security policy, in other words, understanding the human vulnerabilities. When examining today's threat landscape, one unchanged theme is that humans

remain one of the weakest link in the information security chain because, in most cases, the threat comes to fruition due to a human decision instead of a technological one (Global Knowledge, 2015)The theory of planned behavior provides solid theoretical foundation for such context (Bulgurcu et al., 2010; Guo et al., 2011).

Various research activities have shown that sanctions, and their perceived severity, are negatively associated with the intention to engage in deviant behaviors (Cole, 1989; Nagin & Pogarsky, 2001). Contemporary deterrence theory asserts that perceived risks and cost of both formal and informal sanctions (e.g., social disapproval) are important factors in preventing deviant activity (Pratt et al., 2006). The theory further corroborates that a detailed, comprehensive security policy with noncompliance consequences is an effective countermeasure.

One problem in most organizations is that the IT department makes the rules, selects and supervises the staff, and monitors them for compliance. If issues arise, the IT management usually contacts the Human Resource (HR) to carry out any necessary disciplinary or termination action.

Our approach to detect and deter insider threats involves ensuring that this self-monitoring ends and that a separate organization is involved in managing closely the privileged IT users' behaviors and actions. In large security-conscious organizations, a Chief Security Officer (CSO) may be appointed who does not report to the IT chain of command, but directly to the CEO. For smaller organizations, or to provide support to the CSO model, we propose that the best office to manage the insider threat challenge is a security-trained HR department. It is believed that they can add value to the detection of privileged IT users as insider threats because of additional aspects that they may affect an individual's actions, including the employee's working environment and behavior and certain confidential information such as results from the background check prior to employment, stress, shift work hours, wage garnishment, and prior performance issues. These can be identified as human vulnerabilities and handled similarly to the way technical vulnerabilities are identified and managed. Similarly, the contracts department should be given responsibility for the monitoring of suppliers, contract workers, and consultants with privileged access and obtain additional information from their vendors on people who require privileged IT access.

The proposed strategy requires the following specific actions as illustrated in the following figure.

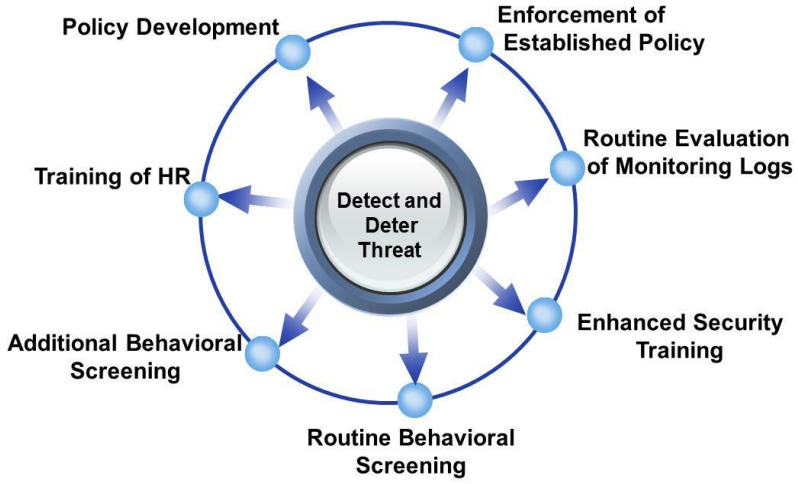

Figure 2. An interdepartmental strategy to detect and deter threat

Policy Development

While most organizations have a general computer use policy, this policy does not include the additional requirements that apply only to privileged IT users. Policy details will need to be tailored and might encompass the following aspects: use of default passwords, attempts to gain authorized access to accounts beyond the scope of job responsibilities, creating multiple administrative level accounts and passwords, creating unnecessary shared accounts, attempts to bypass technical standards, use of hacking tools, accessing materials or attempts to access materials not appropriate to job responsibilities, undue curiosity or searches for information about matters not within the scope of the insider's need to know, unauthorized attempts to remove materials from the work area, unauthorized work at home, and lax security habits. The policy will also include details of enforcement actions in the case of violations of the policy.

Training of HR and Contracting Personnel

HR and contracts personnel will need individualized training to support this initiative including computer security concepts such as social engineering; interpretation of the privileged users policy; role of the privileged IT user and the non-malicious actions that they might take and their impact on the organization's security and compliance; connections between human behavior and potential security violations; and use and interpretation of results from security monitoring tools. The trained personnel will be expected to take refresher training every 6 months to ensure they stay current in the ever changing cybersecurity threat field and the available monitoring tools. HR professionals have become increasingly tech-savvy over the past few years and several organizations have hired forensic psychology professionals into their ranks (For more information refer to http://jobs.personneltoday.com/article/essential-skills-for-hr-professionals/).

Additional Behavioral Screening on Hiring

While the standard background check will identify major red flags such as criminal activity and credit issues, it does not look at the character of the person, their ethical values, their potential for bad behavior in the case of stress, their likelihood to give out valuable information in the case of social engineering, or the likelihood of going "rogue". While some of this might be covered in the interview process, a more formal behavioral screening will standardize testing and provide data for subsequent assessments.

Routine Behavioral Screening

While most organizations look closely at potential employees, there is usually no further check on employee behavior, unless there are some security clearance requirements. However, personal circumstances do change and so it is recommended that there is a routine behavioral assessment. This may be administered routinely (e.g., every six months) or given on an ad-hoc basis, in much the same way that drug testing is administered in some organizations.

Enhanced Security Training

A separate security training program should be developed for privileged IT users who have enhanced access to the organization's systems and information. This training should cover the legal and policy framework for the organization, highlighting compliance issues, recommended actions in given workplace situations, and the possible policy enforcement actions. This can be delivered online and both internal and external workers should be required to pass a scenario-based quiz before obtaining their privileged access. Updated training program should be available on an annual basis.

Routine Evaluation of Monitoring Logs

HR and contracts personnel must be trained to review system logs and interpret actions for the privileged users that they are monitoring. Monitoring might include unsuccessful login attempts into mission-critical applications, on or off premises, firewall and IDS/IPS logs, web proxies, antivirus alerts, access to important records, particularly after-hours, change management records, help desk trouble tickets, and use of personal cloud-based storage solutions. It is important to note that suspicious actions may not be a direct action of the privileged user, but may be a symptom of their account being compromised.

Enforcement of Established Policy

HR, in collaboration with IT management and with legal advice, must be prepared to follow through with the policy's enforcement actions. This is an important component of deterrence but statistics show that cybersecurity incidents are considerably underreported to law enforcement (SEI, 2012).

IMPLEMENTATION CONSIDERATIONS

The HR and contracts functions both handle personally confidential information, which is not made generally available to others in the organization – this information includes clues to the organization's human vulnerabilities. As such, it is necessary to consider how the HR function can become more security conscious, whether by training or by hiring knowledgeable individuals. It also puts some responsibility on the IT security department to provide information to the HR department in an easily understandable format, such as through a dashboard. As others in the organization, they do not need the same level of detail that might be analyzed by a security professional. Instead, they need a summary of security logs and security incidents that they can correlate with the known human vulnerabilities. There is a cost associated with such measures which needs to be quantified but is considered an essential part of a comprehensive insider threat deterrence strategy.

The involvement of multiple parts of an organization is considered a longer term initiative and needs to be monitored and assessed in coordination with other security initiatives as all parts of the organization's become more security aware. The first step is seen as assessing the current security awareness of HR and contracts organizations and a survey of this population is a work in progress by the authors.

CONCLUSION

Insider threats have multiple origins, one of them being the non-malicious (volitional) privileged IT user. Because of the potential damage to the organization caused by these users' violating security policy and/or their access accounts being compromised, organizations need to implement additional countermeasures to detect and deter these threats. Of particular concern is to have shared responsibility for monitoring the behavior and actions of these users, involving the HR and contract department as needed. Human vulnerabilities leading to insider threats need to be studied further and given as much focus as technical security vulnerabilities.

REFERENCES

1. Akersredt, T. (2003). Shift Work and Disturbed Sleep/Wakefulness. *Occupational Medicine 53*(2), 89-94.
2. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. [Article]. *MIS Quarterly, 34*(3), 523-A527.
3. Cisco. (2008). Data Leakage Worldwide: The High Cost of Insider Threats. Retrieved on January 2, 2014 from http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-506224.html
4. Cole, C. A. (1989). Deterrence and consumer fraud. *Journal of Retailing, 65*(1), 107–120.
5. Crosman, P. (2013, September 25). Insider Threat Rises, Info Security Officers Say. *American Banker,* Retrieved on December 18, 2013 from ProQuest.
6. Global Knowledge. (2015). Human Vulnerabilities in Our Current Threat Landscape (pp. 1-7): The Hacker Academy, a Division of Blackfin Security Group.
7. Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. [Article]. *Journal of Management Information Systems, 28*(2), 203-236.
8. Hong, J., Kim, J., & Cho, J. (2010). The Trend of the Security Research for the Insider Cyber Threat. *International Journal of Future Generation and Networking 3*(2), 31-40.
9. Johnson, N. (2013). Agencies Struggle to Launch Insider Threat Programs. Available from Federal Times, Sept 3. Retrieved on January 4, 2014 from http://www.federaltimes.com/article/20130903/IT01/309030002/Agencies-struggle-launch-insider-threat-programs
10. Loch, K., Carr, H., & Warkentin, M. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. *MIS Quarterly*, *16*(2), 173-186.
11. Murphy, D., & Murphy, R. (2013). *Teaching Cybersecurity: Protecting the Business Environment*. Paper presented at the 2013 Information Security Curriculum Development Conference, Kennesaw State University, GA and published in the proceedings in the ACM Digital Library.
12. Nagin, D. S., & Pogarsky, G. (2001). Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence and evidence. *Criminology*, *39*(4), 865-891.
13. Obama, B. (2012). Memorandum on the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs: November 21, 2012, Retrieved on January 3, 2014 from www.fas.org/sgp/obama/insider.pdf.
14. Ponemon Institute. (2013). Big Data Analytics in Cyber Defense. Ponemon Institute Research Report. Retrieved on from http://www.ponemon.org/library/big-data-analytics-in-cyber-defense
15. Pratt, T. C., Cullen, F. T., Blevis, K. R., Daigle, L. E., & Madensen, T. D. (2006). The empirical status of deterrence theory: a meta-analysis. In F. T. Cullen, J. P. Wright & K. R. Blevins (Eds.), *Taking Stock: The Status of Criminological Theory* (pp. 37–76). New Brunswick, NJ: Transaction Publishers.
16. Privacy Rights Clearinghouse. (2013). Chronology of Data Breaches – Security Breaches 2005-Present: Accessed from http://www.privacyrights.org/data-breach.
17. Raytheon (Producer). (2014). Privileged Users: Superman or Superthreat?:A Privileged User Risk Whitepaper. Retrieved from http://www.raytheon.com/capabilities/rtnwcm/groups/gallery/documents/digitalasset/rtn_159602.pdf
18. SEI. (2012). 2012 Cybersecurity Watch Survey: Software Engineering Institute, Carnegie Mellon University. Retrieved on December 30, 2013 from http://www.cert.org/archive/pdf/CyberSecuritySurvey2012.pdf.
19. SEI. (2013). Unintentional Insider Threats: A Foudational Study, August 2013, CMU/SEI-2013-TN-022: Software Engineering Institute, Carnegie Mellon University. Retrieved on December 30, 2013 from http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=58744.

20. The Associated Press. (2014, November 10). Efforts to protect US government data against hackers undermined by worker mistakes *The Guardian* Retrieved on from http://www.theguardian.com/technology/2014/nov/10/us-government-hacking-cybercrime-workers-crime
21. Wall, D. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security Journal, 26*(2), 107-124.
22. Willison, R., & Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. [Article]. *MIS Quarterly, 37*(1), 1-20.