

Insider Threats 2.0: The Oblivious Insider, A Case Study
IST 700 - Spring 2009 - Syracuse University School of Information Studies
Shay C. Colson

Introduction

IT security is a difficult game played on an ever-shifting playing field. Innovations and advances can mean great leaps in technological abilities and productivity levels, but it can also mean continual challenges for the security professional. As technologies move ever towards integration, security becomes more and more important. With the eventual advent of single sign on models (Sherwood, Clark et al. 2005), one type of threat becomes particularly dangerous: insider threats.

Insiders “can be among the most costly and the most damaging to a company's reputation,” one researcher wrote. “Insider attacks against IT infrastructure are among the security breaches most feared by both government and corporate security pros.” One study noted that 60 percent of IT security professionals believe their organizations are unable to “effectively assess or quantify insider threat risks,” even though “they realize the dire risks posed by this inability: privacy breaches, failed audits, and potential fraud or misuse of data.” (Greenemeier 2006; 2007) To add insult to injury, insider attacks are among the most difficult type of security breaches to detect and deter, simply because of their internal nature. You cannot lock down an organization for security purposes and expect to carry on with business-as-usual.

Of particular interest to security professionals has been one type of insider threat: the Malicious Insider. One security researcher offers the following definition of the Malicious Insider: “individuals within an organisation [sic] that mask their identity, their behaviour [sic], or both, for the purpose of compromising the security of the [organization].” (Fyffe 2008) In addition to the ever-present threat of the Malicious Insider, this paper will address the security concerns and security controls surrounding a new type of insider threat: the Oblivious Insider.

What (or who) is “The Oblivious Insider?”

Simply put, the Oblivious Insider (OI) can be anyone inside any organization. The Oblivious Insider could be sitting down the hall, they could be your boss, your CFO, or your receptionist. The Oblivious Insider could even be you. An Oblivious Insider is an insider who, through their actions, unknowingly compromises information confidentiality, integrity, and/or availability. Often these actions ignore, run counter to, or defeat existing security controls, making detection and mitigation that much harder. (Maybury, Chase et al. 2005)

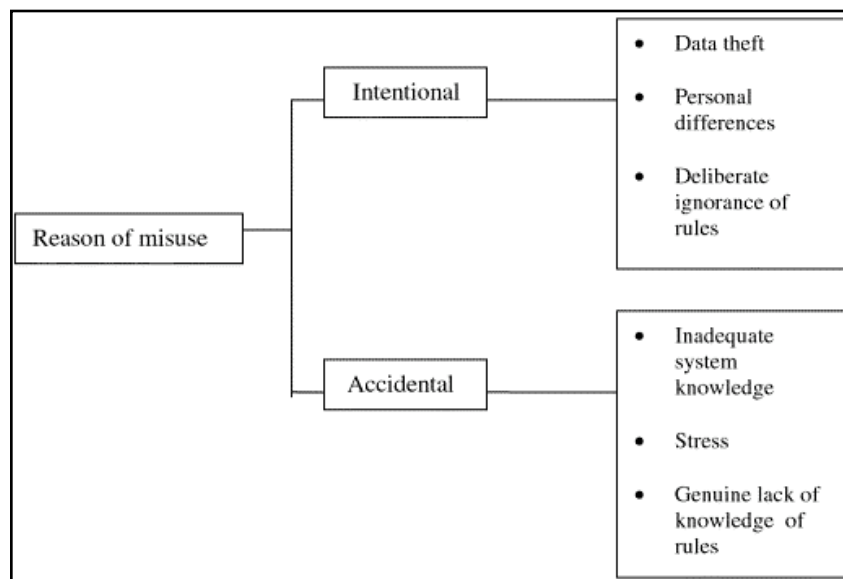
Employees with modus operandi similar to the Oblivious Insider have been discussed before by security researchers. These professionals emphasize “the importance of considering accidental misuse incidents as equally important threats to intentional ones. Indeed, the commercial world is full of unintentional misuse acts that resulted in large financial losses for well-known companies.” (Magklaras and Furnell 2001) Although the computer security community has created a plethora of taxonomies that describe computer intrusions in general,

little effort has been placed on the construction of a taxonomy that specializes in insider incidents. (Magklaras and Furnell 2001) Even less attention has been paid to insiders who do not have the previously mentioned malicious intent.

In their 2001 paper, Magklaras and Furnell offer the following visual categorization of *insider misuse* shown at right. While this is a good start to examining the issue, in my opinion, this diagram leaves off the single largest threat constituted by an Oblivious Insider's "accidental" misuse: Exploitation.

While "inadequate system knowledge," "stress," and "genuine lack of knowledge of rules" are all threats that must be mitigated, the Oblivious Insider's ability to be

exploited by an attacker can lead to far greater damages. See **Effective Attacks Against the Oblivious Insider** for discussion on how this exploitation plays out in organizations daily.



The Oblivious Insider vs. The Malicious Insider

My research indicates that the Oblivious Insider poses a greater threat to an organization than the Malicious Insider for a multitude of reasons:

- Sheer Numbers*: While one or two malicious insiders may be able to penetrate any given organization, that same organization is likely rife with Oblivious Insiders.
- Repeat Attacks*: While a Malicious Insider may get away with several small attacks, or perhaps even one large-scale attack prior to detection, the Oblivious Insider can strike multiple times, or even from multiple locations at once, making the threat that much more difficult to defend against.
- Misconception of Actions*: Many times, an Oblivious Insider will think that he or she is performing their job correctly, when in actuality, they are putting themselves and their organizations at risk. This becomes an increasingly common problem when employees are able to take work home, or access organizational information from a mobile device or home computer.
- Detection and Mitigation Difficulty*: Since any employee with, or without, authorized access to sensitive data can behave as an Oblivious Insider, there are no behavior detection patterns or set mitigation strategies that are known to be effective against this threat.

Effective Attacks Against the Oblivious Insider

While much research has been done on the problems posed by malicious insiders, and the specific counter-measures applicable to this threat, relatively few security researchers have addressed the threats posed by the Oblivious Insider. The reason that the Oblivious Insider poses such a threat is that an OI has legitimate access to many things within an organization, and their actions cannot be detected by any of the newly-developed behavioral analysis models that researchers are developing precisely because there is no malicious intent to discover.

Perhaps the most dangerous threat the the Oblivious Insider poses to an organization is their vulnerability to social engineering attacks. In his book, *Spies Among Us*, security consultant Ira Winkler discusses an actual penetration test that he carried out by manipulating Oblivious Insiders in a Fortune 500 company. (Winkler 2005)

Winkler and his associates were hired to perform a penetration test against the existing security controls at this particular (unnamed) organization. From a location physically outside the organization, one of Winkler's team members dialed the Help Desk, claiming to have a computer problem. The Help Desk asked for the penetration tester's Social Security Number in order to verify his identity. This is the first of the many red flags raised during this penetration test: using employee Social Security Numbers as Employee Identification Numbers.

The penetration tester quickly made an excuse to get off the phone, and then began dialing random employee desk phones. He told the employees that he was from the Help Desk, and that there had been a security breach resulting in all passwords being wiped out. He offered to change it back for the employees, if they would only verify with him their Employee Identification Number (SSN) and tell him what their old password was. According to Winkler, there was one woman who "was the only person, out of almost 100, who did the right thing" and refused to give out information over the phone. Perhaps even more troubling, this particular woman did not know if, or to whom, she should report this incident, thus perpetuating the behavior of the Oblivious Insiders seated at 99 out of 100 desks at this organization. (Winkler 2005)

Consider another potential attack against the Oblivious Insider: In many organizations today, top-ranking management personnel are older and less technology-savvy than the new hires of the very same organization. One study put the average age of Fortune 500 leadership team-members at 55.5. (Wiersema and Bantel 1992) As such, these managers have more responsibility and access to resources, yet likely have less technical expertise or training. Should these people behave as Oblivious Insiders, and at some point be exploited, the level and extent of the damage caused could be enormous.

Unfortunately, there are many ways an Oblivious Insider can put their organization at risk:

- Common technological faux pas such as opening unknown attachments on email messages, falling for phishing scams, or clicking malicious online advertisements.
- Accessing organizational data from home over an unsecured wireless network.
- Using a public terminal or access point to connect to the organization's network.
- Losing or misplacing a company-owned laptop or mobile phone with sensitive data.
- Not questioning the presence of strange people in organizational offices or locations.

- Disclosing potentially sensitive material in an online forum, blog, or unsecured email.

Indeed, the list goes on. While new IT security controls, policies, and procedures can counter some of these threats through firewalls, filters, and other means, new controls must be developed to minimize the risk posed by this new threat. Moreover, the traditional concept of “security controls” will have to be expanded to include aspects of an organization previously thought to have nothing to do with “security.” Effective counter-measures to the Oblivious Insider will require a complete re-thinking of an organization’s employee mentality, and a shift towards human-centric security controls.

Effective Security Controls Against the Oblivious Insider

In discussing security controls to counter or mitigate the threats posed by the Oblivious Insider, it is important to remember that these controls do not negate the need for separate protections against the threats of the Malicious Insider. Indeed, instituting a risk minimization strategy in regards to the Oblivious Insider *requires* that all other existing security controls remain in place. These pre-existing security controls are a good starting point for an anti-OI security policy.

The goal for any organization should be to encourage employees to shift their thinking in such a way as to shed the Oblivious Insider mentality that has become so pervasive. Recent research has begun to incorporate the threat posed by “accidental insider misuse actions.” (Magklaras and Furnell 2001) These “accidental misuse actions” are exactly what I have been describing in this study.

The key to working against the Oblivious Insider is engagement and vigilance by employees. In many organizations, enforcement of certain current security controls is lax. This may be the guard at the gate just waiving people through, or lack of follow-through on reported incidents. Whatever the case, the new anti-OI policy should begin by reviewing existing security controls and work towards 100% consistent enforcement. Not only will this provide a much needed boost to security measures already in place, but it will begin to instill a sense of security-mindedness in the mentality of employees.

As noted by Sherwood and his co-authors, stake-holder buy-in is hugely important in implementing a truly effective security control. (Sherwood, Clark et al. 2005) Difficulty can arise when the message from management or the security teams start to make it sound like *everything* is a security risk. As I have mentioned, it is important to both achieve a balance between availability and confidentiality, but also to know where an action falls on a scale of risk.

Security teams should initiate the creation of new security controls by drawing on the wealth of knowledge found within the organization at all levels, in all positions. It is likely that a high-ranking security officer, perhaps in combination with a similarly tenured Human Resources representative, could put together a working team of employees that are both representative of the diverse roles of an organization yet clearly *not* a threat as an Oblivious Insider. Working together, this team could provide feedback about the specific dangers an Oblivious Insider could pose in their particular unit or division, as well as work to develop custom-tailored OI prevention training modules. A security consultant with a knack for interpersonal skills could also be very

beneficial in this process, perhaps even providing an outsider's view helping to further minimize OI risks.

Another challenging aspect of defeating the OI threat is that the threat grows in conjunction with the size and geographic distribution of the organization. Defeating the Oblivious Insider may sound simple, as if it can be solved by placing "monitoring tools where appropriate. It sounds easy, but it is not, because there are so many touch points," and each touch point represents a potential vulnerability. (Rodier 2008)

Again, however, implementation will require a delicate touch. A full-out security blitz to eliminate Oblivious Insiders from an organization may prove too taxing, or could create an atmosphere of paranoia amongst employees. Better strategies would include targeted education through training for current employees, based on their risk as calculated by legitimate access levels to sensitive data. Newly-hired employees may be able to withstand more intense security training, allowing an organization's security officers to work against the Oblivious Insider from the bottom-up and the top-down simultaneously.

Conclusion

While the Oblivious Insider is causing some security professionals to lose sleep at night, in many cases the problems surrounding OIs will begin to resolve themselves if sound security policies and procedures are put in place, emphasized, and followed by members of an organization. As we have seen, it is important not only to have a procedure for reporting potential security breaches, but to encourage this practice as a constructive exercise, not one that could carry punitive damage for the reporting or offending employee. Once employees understand that this exists to promote and ensure the security of the organization, it will seem less like "tattling" and more like being a team-player. Defeating the Oblivious Insider requires participation from all members of an organization. With the proper security policies and controls, not only can the Oblivious Insider be neutralized, but the strength and effectiveness of the organization's security can be greatly increased.

Sources Cited

- (2007). "Addressing the Insider Threat." Community Banker **16**(8): 14-14.
- Fyffe, G. (2008). "Addressing the insider threat." Network Security **2008**(3): 11-14.
- Greenemeier, L. (2006). "Insider Threats." InformationWeek(1118): 25-25.
- Magklaras, G. B. and S. M. Furnell (2001). "Insider Threat Prediction Tool: Evaluating the probability of IT misuse." Computers & Security **21**(1): 62-73.
- Maybury, M., P. Chase, et al. (2005). Analysis and Detection of Malicious Insiders. International Conference on Intelligence Analysis. McLean, VA: 7.
- Rodier, M. (2008). Stopping the Inside Job -- Following the Societe Generale scandal, Wall Street firms have reexamined their internal security practices. But a number of factors, including the economic downturn and business pressures, continue to make rogue employees a very real threat. Wall Street & Technology: 26-26.
- Sherwood, J., A. Clark, et al. (2005). Enterprise security architecture : a business-driven approach. San Francisco, CMP Books.
- Wiersema, M. F. and K. A. Bantel (1992). "TOP MANAGEMENT TEAM DEMOGRAPHY AND CORPORATE STRATEGIC CHANGE." Academy of Management Journal **35**(1): 91-121.
- Winkler, I. (2005). Spies among Us. New York, Wiley.