New Type Of White Crime: Insider Hacking

Abstract

Insider hacking consists of cybercrimes against entities initiated by individuals who hold a legitimate trust relationship with that entity. The responsibility of preventing insider hacking falls to information technology (IT) or information security departments staffed by computing professionals. The same can be said about research into the prevention of insider hacking, computing-centric academics/professionals do the work. While this seems logical, established behavioral methods for reducing crime have largely been ignored. In this paper, the author places insider hacking into the context of the white-collar criminology literature then pulls from crime science, applying a situational crime prevention model to inform future research on insider hacking.

Crime definition

Even using the perspective of law, these computer-enabled insider activities may indeed be illegal, but do not fall under the umbrella of cybercrime. The Computer Fraud and Abuse Act applies to insiders only when the offender acts with “intentional conduct” defined as “knowingly transmitting a program, information, code, or command resulting in damage to a protected computer.” Damage is met when victims spend at least $5,000 to investigate and/or remedy an incident (a low bar when you factor in the cost of IT personnel). One definition of a protected computer, “affects interstate or foreign commerce or communication of the United States,” can be interpreted as any computer connected to the Internet. This law would not apply to the computer-enabled crime.

The Computer Fraud and Abuse Act applies only to outside hackers for simple unauthorized access to data or systems, called reckless or negligent conduct by the law. Insiders are exempt from crimes of unauthorized access. Unable to rely on any legal deterrents or law enforcement for investigations and punishment, organizations must take its own steps to prevent unauthorized insider access to sensitive organizational information.

IT Sabotage

The IT sabotage crimes represent a new kind of white-collar crime. SEI defines IT sabotage as “an insider’s use of IT to direct specific harm at an organization or an individual”. Specific actions of IT sabotage include deleting files, locking individuals or groups of individuals out of systems/files, publishing sensitive information (customer data, corporate communications, etc.), planting viruses, disabling services/devices, and defacing web pages. IT sabotage represented 45% of the insider computer-based crimes on the SEI survey in 2009, and 29% in 2012. This drop likely represents an application of some easy prevention methods by organizations over the previous three years. Throughout the rest of this paper, IT sabotage will be referred to as insider hacking.

In the majority of cases (70%), offenders did not use their own accounts instead hacking

others' accounts, creating new accounts, or using shared accounts (generic accounts for which multiple individuals know the credentials). Most offenders took steps to conceal their actions (beyond not using their own accounts), like deleting or modifying log files. Log files are automatically created text files documenting successful and failed access, changes to those systems, and by whom. The attacks generally took place outside of working hours and originated remotely rather than onsite. In most cases, insider hackers showed other signs of trouble. There were conflicts in the workplace, a decline in work 54 performance, tardiness, and absenteeism. Management often ignored problems; in some cases employees were sanctioned for problems in the workplace and subsequently increased their hacking activity.

Prevention

Judging by the fact that insider hackers refrain from using their own accounts, perform their hacks off-work time, and alter log files; offenders are sensitive to the risks of detection and are aware of the ability of systems and networks to track the activities its users.

The data all suggest that much of the insider hacking activities were preceded by other personnel problems in the workplace; conflicts, performance, tardiness, absenteeism. As such, these indicators should be watched closely for IT staff. Noticing any of these behaviors should result in increased monitoring of their activities on the systems. While such action may seem to infringe on the privacy rights of employees, corporate ownership of the computing resources and network use policies follow the law to allow monitoring.

Conclusion

Recognizing the difference between computer crime and computer-enabled crime could go a long way towards advancing the prevention of insider hacking. The computer-enabled crime should parallel crime prevention techniques for their associated non-cyber white-collar crimes instead of being lumped in with insider hacking. A more granular look at computer crimes will advance the study of the prevention of insider hacking.

Reference

1. Silowash, G., & Shimeall, T. J. 2012. Common Sense Guide to Mitigating Insider Threats 4th Edition. Pittsburgh, PA.
2. Computer Fraud and Abuse Act (CFAA) (1986). Pub. L. No. 99-474, 100 Stat. 1213 (Oct. 16, 1986), codified at 18 U.S.C. §1030
3. Cappelli, D., & Shimeall, T. J. 2009. Common Sense Guide to Prevention and Detection of Insider Threats 3rd Edition. Pittsburgh, PA.
4. Fischer, L. F. (2003). Characterizing information systems insider offenders. In Proceedings of the 45th Annual Conference of the International Military Testing Association (Pensacola, FL, November 03-06, 2003). IMTA, Seoul, South Korea, 289–296.