www.Criminologia.org

TELEMATIC JOURNAL OF CLINICAL CRIMINOLOGY

Telematic Journal of Clinical Criminology - www.criminologia.org International Crime Analysis Association

Anno di pubblicazione 1999

Organized Computer Crime and More Sophisticated Security Controls: Which Came First the Chicken or the Egg?

By Marc Rogers, Graduate Studies, Dept. Of Psychology, University of Manitoba, 1999 – www.infowar.com

An interesting trend seems to be appearing within the area of computer crime. The trend is the increase in organized criminal activity. In the past the primary threat to computer systems was the criminal insider. Recent surveys indicate that the threat of the lone insider is being equaled by outside attackers using Internet connections as the points of attack. Along with the increase in the external threat there has been an accompanying increase in organized criminal activity. There have been several documented accounts of criminal organizations attacking banking institutions, committing wide scale fraud, and taking advantage of the Y2K issue to commit computer related crimes.

The increase in organized criminal activity has been positively correlated with the sophistication of security controls. The computer security industry has interpreted this to mean that organized criminal activity has caused the requirement for stronger and more sophisticated security controls. The computer security industry has taken a correlation and ascribed as causal relationship. Unfortunately correlation does not provide sufficient evidence for determining causation. As such it becomes a case of what came first the chicken or the egg? An alternate model of causation would be to postulate that the increase in sophisticated controls has lead to the increase in organized criminal activity. This alternate hypothesis will be briefly examined.

An accurate measure of the amount of organized activity is impossible. There have been some attempts to estimate the financial impact of general computer crime on the corporate world, but unfortunately compiling accurate, valid, and meaningful statistics in relation to computer attacks is problematic. There are several factors that influence the accuracy of surveys and research into computer crime rates. One such factor is that victims are hesitant to admit they were attacked, and fewer still report the attacks to authorities. The common belief among researchers is that reported figures are an under-estimation of the true problem. The CSI/FBI indicated that in the most recent survey they conducted that the cost of network security breaches in general was in excess of $126 Million USD. This is a significant number and becomes even more staggering when we consider it to be an under-estimation.

What is apparent from the studies and surveys to date is that with the rapid increase in E-commerce offerings more businesses are becoming cognizant of security. E-Commerce is viewed by many, as the natural progression for business, with groups stating revenues will be in the billions of dollars. E-commerce has an interesting corollary, it may be a factor in the increase of general computer crimes. The increase in E-commerce offerings results in an increase in online credit card activity, virtual wallets, personal information databases, etc. These items are prizes or goals for the computer criminals. E-commerce has effectively raised the stakes by increasing the rewards of successful attacks.

The increase in the stakes has changed the traditional security notions regarding costs of attacks. Simply stated the " cost of the attack", refers to the amount of effort required to obtain a specific goal (i.e., password file, root account, credit card database, etc.). It is theorized that if the effort outweighs the goal then the attacker will not be interested. This concept has directly led to the practice of increasing the sophistication of safeguards to protect sensitive systems, data, and information. However, the increase in sophistication of safeguards combined with the increase in the potential value of the goal may have an unintentional negative side effect, the increase in organized computer crime.

The basis for making such a hypothesis regarding the effect of sophisticated safeguards is founded on psychological and criminological theories offered to try and understand traditional corporate and organized crime. During the 1970’s there was a great deal of interest in corporate crime, and the activities of criminal organizations such as the Cosa Nostra. Several studies were conducted to attempt to explain why organizations became involved in criminal activity. These studies concluded that an increase the sophistication of controls (i.e., better safes, harder to forge currency) and more valuable prizes (i.e., more money being stored) was positively correlated with an increased sophistication of the criminals. Eventually the “cost of the attack” and the level of sophistication was too much for individuals. The high value of the prizes became enticing for criminal organizations. As an organization, these entities could overcome the sophistication required to break or circumvent the safeguards and obtain the goal.

A more recent illustration can be seen with credit card fraud. The addition of security controls such as holograms made it impractical for an individual to forge, but very practical for large-scale organizations who create forged cards in bulk. As a result there are several criminal organizations specializing in credit card fraud.

As stated previously, within the computer security arena the controls protecting sensitive assets are becoming more sophisticated (i.e., two-factor authentication, session encryption, VPN, firewalls, etc.). The level of effort and sophistication to circumvent these controls is considerable. In fact the effort and sophistication may be great enough that the industry has pushed the requirements into the realm of criminal organizations. The attraction for organized crime is very apparent. The end result of a successful attack can be thousands of credit card numbers, millions of dollars, proprietary code, or sensitive personal information.

The alternate hypothesis is plausible and just as defensible or indefensible as the mainstream security industry hypothesis. Both require correlation to be misconstrued as causation. However, if this alternate hypothesis is correct, then the current practice of increasing the sophistication of controls alone is insufficient to combat the problem. Introducing more legislation and stiffer penalties for computer crime will also be insufficient. The “more of strategy” doesn’t address the underlying problems. Criminal organizations view the controls, and laws as hazards of the trade, not as deterrents. What needs to be combined with controls and legislation is an understanding of the causes of organized and individual criminal activity. It is safe to say then that computer crime and computer security may not be just a hardware, software problem, but a peopleware problem as well.

----

[1] Assuming the attacker is not motivated out of revenge etc.