



Net Demographics
infectionvectors.com
July 2006

Overview

Criminology has used forecast models for quite some time in order to not only predict future crimes, but also predict what offenders may be a threat to society in the future. Initially known as criminal profiling, the practice involved interviews between trained psychiatrists and incarcerated subjects. Later, this has made way for the inclusion of standardized, repeatable criteria such as a worksheet of questions/descriptors. This latter practice has lessened the impact of subjective data used in determining dangerousness.

Within the information security world, practitioners are often searching for objective data with regard to threats. There is likely a significant amount we can learn from law enforcement, however, that would apply to IT security. This article takes a brief look at what factors from the criminological world may help form objective prediction models within the Internet security discipline.

Criminological

Current crime predictions (those for the physical world) generally rely upon geographic data – researchers track where crimes are committed, then extrapolate where future crimes may be committed. This type of analysis also incorporates sociologic and economic factors to aid forecasting in similar areas. These are good criteria when deciding what streets are most likely to be the location of hold-ups. However, they don't fit into the traditional approach to Internet prediction modeling especially well.

When considering Internet crime, a forecaster may include such things as the technology available to the general public, the ease of obtaining exploit code, and the motivations of potential criminals. Demographic information would appear as less relevant, although the arrests of malware coders seem to be almost exclusively young males.

With regard to economic issues, would these seem relevant? In big cities, it is often the lower-income areas that are considered to be the highest risks for crime – how about the Internet? Access to the necessary technology is the only constraint to committing the crimes (beyond having the technical knowledge for the action). And access to an Internet-connected computer is not much of a constraint anymore. With the ability to anonymously interact with anyone, the Internet removes the geographic limitations to crime. It may be that the wealthier locations (a desirable target of theft/fraud-based crime) are now more likely to be part of cyber crime scenes.

Is economic status a good indicator of criminal proclivity on the Internet? In the physical world, some analysts draw such a correlation. How about in the context of an individual whose only illicit activities take place online? Take for example the Windows Meta File (WMF) graphics rendering flaw from December 2005 (which spawned MS06-001 in January 2006). If someone crafted an exploit, but did not release it as part of a money-making scheme, would the economic status of the individual be considered as a potential reason? If the global economy (or the financial situation of the fictional coder above) was in much worse shape, would the WMF flaw have spurred broad-based attacks instead of the limited damage we actually saw?

Solving crimes also takes on a new element with regard to Internet-based activities. As noted in an IC3 (Internet Crime Complaint Center) report in 2005, finding a criminal that could be anywhere in the world gives a new wrinkle to traditional law enforcement (jurisdictional issues, tracking a criminal on the move, etc.). Solving Internet crime is not the primary focus of most IT security professionals, preventing crime is their charge.

Model Citizen

So where is the overlap between law enforcement and Internet security? Profiling is the obvious choice based on the context of this article. When crafting a risk assessment, the dangerousness of each threat being modeled is difficult to quantify for most decision makers. Using a model that incorporates only objective (verifiable and quantifiable) data sets is the first step. These correlate to the standard interview questions used by criminal psychologists/psychiatrists. That data is then analyzed by the professional and given additional dimension, shaped by their experience and knowledge. The same idea would work for security professionals, instead of profiling criminals, the focus would be vulnerabilities (as both represent a threat, and presumably a quantifiable danger to their respective ecosystems). The mechanisms for matching such a system to a business model can be constructed by the risk management team or the CIOs themselves. More information on threat profiling as well as building an objective “dangerousness” score is available at <http://www.infectionvectors.com>.

References

IC3 2005 Internet Crime Report: Prepared by the National White Collar Crime Center and the FBI.

http://www.ic3.gov/media/annualreport/2005_IC3Report.pdf