All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

The threat reduction approach – Point - Counterpoint

Threats are actors – individuals – groups – or nature. They are the people and natural forces that cause event sequences producing negative consequences. While nature can usually be adequately protected against by adequate redundancy, humans are a more serious problem because they act with malicious intent and exploit complex sequences using feedback to make decisions about how to proceed. The threat reduction approach is to stop these threats from continuing to act maliciously.

How do we reduce the human threat?

Many in law enforcement have long believed that the solution to crime is the certain and rapid detection, arrest, prosecution, and punishment of those who commit crimes. In the information age society emerging today, we seem to be unable or unwilling to pursue this course. The result seems to be the emergence of increasingly skilled individuals and groups who continue to outthink and outwork defenders and do so with impunity. We seem to ask a great deal of defenders in the information security space – far more than we ask in any other space.

If we compare the information security space with the physical security space, we start to see the extent to which we push on defenders instead of on threats. I recently asked some risk management folks what they do to defend against drivers in cars intentionally killing them as they cross the street. The real answer is, nothing. We live in a society in which we are always at risk. If a malicious actor decides to kill some people, they can. They can simply sit in their car at a traffic light in a city, wait for a crowd to appear in the cross-walk, and hit the gas. This is a known vulnerability, but nobody is rushing to alter the operation of cars or require people walking to wear special defensive clothing so as to mitigate the threat. And if they put sensors in cars so they couldn't be driven into cross-walks when people were present, there would be a way to cover the sensor. Would we require that the sensors be perfect against any threat?

What we do to protect people from malicious drivers is to create laws and social mores. When someone does such a thing, they are rapidly hunted down, arrested, prosecuted, and put in jail for a long time. The media shuns them and speaks harshly about them, their families are embarrassed by the questioning, we call them psychologically unfit, we question their upbringing, and the list goes on. In short, the car company is not responsible for making cars that can never harm anyone. The impetus is put on the driver to do the right thing. While I don't favor shoddy computers or cars, trying to build the perfect computer against malicious abuse is like trying to build the perfect car against malicious driving.

Conclusions

While we can't expect perfection from law enforcement and we have to balance civil rights with the desire for justice, unless and until we start to use the system of justice to stop crime and criminals early in their evolution, we will continue to foster more crime, more criminals, and a society based on caveat emptor rather than honesty, liberty, and justice. We need to focus on creating the social norms and legal framework to stop the threats from doing it twice.

Counterpoint – by Charles Preston

This is a bad comparison, and the point you are making cannot be supported this strongly.

My reasoning is that, while I agree that offenders in cyberspace are often not appropriately arrested tried, convicted, and sentenced, there are several differences between most cybercrime and most other crime. Specifically:

- Cybercrime is most often an action against property, services, or ownership (intellectual property) not involving death and injury to humans. The legal systems I am aware of distinguish between property crimes and crimes against persons. In fact, statutes are classified under those terms. Sentences for property crimes, and the types of defense you are allowed to employ to prevent their completion, are quite different. You may often kill an attacker to prevent death or grave physical injury, but not to interrupt a crime against property. Where this distinction may get blurred is where the nature of the property crime is such that death or injury will likely result from property damage, such as sabotaging train tracks or aircraft or buildings.
- Many other crimes, and certainly your example of mowing down people in a crosswalk, place the victims and perpetrators in close physical proximity, and that is one reason why identification of the perpetrator is much more likely, much sooner, and with less effort, than skilled cybercrime. One implication of this is that evidence is stronger against most perpetrators of physical crimes. For example, there is almost never any doubt that a crime has actually been committed - the biggest question is proving who beyond a reasonable doubt. For most physical crimes, justice can be swifter and surer, with any attendant deterrent effect being more likely.
- Few physical felony crimes take place across international boundaries, where even jurisdiction can require a major legal effort, without any universally agreed on methods for solving the jurisdiction issue, much less highly important questions such as "this is a serious crime in jurisdiction A, but not a crime at all in jurisdiction B". If the alleged perpetrator is a subject of jurisdiction B, and was at all times within the boundaries of jurisdiction B, why should jurisdiction B allow extradition, despite a grand jury indictment in jurisdiction A, where no representative of the accused was present or allowed to present evidence? The answer to this in recent years has been that jurisdiction A is vastly stronger militarily, and coerces jurisdiction B.
- These legal questions can turn centuries of jurisprudence on its head, and have no clear resolution at this time, involving virtual cyberspace.
- An international system that might be available to help track cybercriminals would necessarily involve even more surveillance of ordinary and unsuspected Internet traffic than is perhaps now the case. Every question of security and crime and punishment involves benefit and loss.
- Cybercrime is different from crimes with a more physical nature because invulnerability can be substantially conferred with technical means, which don't apply to a 200 pound person vs a 5000 pound car. There is a technical evolution and learning process on the part of both the attackers and defenders that can take place at a far greater pace than humans adapting to crushing.

- Mens rae is readily inferred, and sometimes proven, in crimes against humans. Evil cannot be readily implied where technical controls were bypassed, or humans lied to, and system access for data copying was obtained. The degree of abstraction, in the absence of a clear trail of the most heinous of crimes, or terrorism, linked to cybercrime, will make passing laws and severe sentencing difficult.
- The subject of deterrence and explanation and prediction of who will commit crimes is still a puzzle to criminologists. By and large the theories have little good evidence. Senior and experienced forensic psychiatrists disagree on the potential for future violence from convicted or mentally unbalanced people, and the initial causes and predisposition to crime as well as proximate triggers to individual crimes are not well understood. Under these circumstances any idea of deterrence from legal system prosecution is speculative.
- While the threat of punishment undoubtedly plays a role in some people's decisions to not commit cybercrimes, the same threat probably has much less weight for true believers or sociopaths.

I believe most people don't commit major crimes because of a combination of their exposure to religious teaching and other socialization and a calculation of risk vs gain. Risk vs gain calculation is heavily influenced by opportunity, but opportunity can be limited by attention to security during design and operation of information systems. A well-informed system operator has the option to reduce the probability and magnitude of loss by commensurate expenditure and effort.