The John Marshall Journal of Information Technology & Privacy Law

Volume 23
Issue 4 *Journal of Computer & Information Law - Summer 2005*

Article 1

Summer 2005

Distributed Security: Preventing Cybercrime, 23 J. Marshall J. Computer & Info. L. 659 (2005)

Susan W. Brenner

Leo L. Clarke

ARTICLES

DISTRIBUTED SECURITY: PREVENTING CYBERCRIME

SUSAN W. BRENNER AND LEO L. CLARKE†

I. INTRODUCTION

Computer technologies have eroded the nation-state's ability to enforce criminal laws as they apply to attacks on communications between computers, on data stored on computers and on real-world systems that are controlled by computers. These attacks elude the efforts of national law enforcement agencies and pose a serious threat to national economies and infrastructures.[1] The enforcement problem presented by these attacks demonstrates that society needs to rethink how it should enforce criminal laws to prevent computer-mediated crime.[2] Our current model of criminal law enforcement, with its origins in real-world urbanization, does not, and cannot, meet the needs of protecting society from cybercrime.[3]

In this article, we examine how and why society's current law enforcement model is inadequate and propose a new model that can deal effectively with cybercrime. We argue that nation-states can control cybercrime more effectively by replacing the current, hierarchical model with a system of "distributed" security that uses criminal sanctions to require (i) computer users and (ii) those who provide access to cyberspace, to employ reasonable security measures to prevent the commission of cybercrimes. We argue that criminal sanctions are preferable, in this context, to civil liability,[4] and we suggest that a system of adminis-

† Susan W. Brenner is an NCR Distinguished Professor of Law & Technology at the University of Dayton School of Law. Leo L. Clarke is an Associate Professor at the Thomas M. Cooley Law School.

1. *See e.g.* Spencer Swartz, *Secret Service: Internet Fraud Threatens U.S. Economy*, http://www.usatoday.com/tech/news/computersecurity/infotheft/2005-02-18-fraud-threat_x.htm (Feb. 18, 2005); *see also infra* § IV.

2. *See infra* § IV.

3. *See infra* § IV.

4. *See infra* § VII.

trative regulation backed by criminal sanctions will provide the incentives necessary to create a workable deterrent to cybercrime.[5] For example, we argue that: prohibiting Internet access except through licensed Internet service providers, imposing certification and reporting requirements on larger organizations, requiring transparency regarding security-related characteristics of information technology products and mandating cyber-risk insurance, are necessary if society is to control cybercrime.[6]

Before we proceed with our analysis, we need to define several terms: "Law enforcement," means the process used to maintain order in society;[7] "Criminal law enforcement" deals with "crime," which is activity that threatens social order;[8] "Crime" includes crimes against persons, like rape, assault and murder, and against property, like fraud, arson and theft, that have plagued societies throughout history, as well as "newer" crimes against the state, like riot, treason, sabotage, and against morality, like gambling, drugs and obscenity.[9] We also include as "crimes" conduct that implicates a society's relations with other societies, though "crime" has traditionally dealt only with internal disorder; economic espionage and terrorism are examples of such non-traditional crimes.[10] Finally, we use "cybercrime" to denote a subset of "crime:" "cybercrime" refers to "crimes," the commission of which involves the use of computer technology.[11]

II. LAW AND ORDER

Human societies must maintain order if they are to survive. Traditionally, "order" has had two complementary aspects: internal and external.[12]

External order encompasses a society's relationship with its physical and biological environment.[13] Like other systems, human societies must organize and implement the efforts of their members to deal with physical threats (earthquakes, droughts, fires) and threats posed by competing societies.[14] Historically, human societies have dealt with external

5. *See infra* § VIII.
6. *See infra* § VIII.
7. *See infra* § II.
8. *See infra* §§ II & III.
9. *See infra* §§ II & III.
10. *See* 18 U.S.C. §§ 1832, 2332b (2005) (addressing economic espionage and terrorism).
11. *See infra* § IV.
12. *See* Susan W. Brenner, *Toward A Criminal Law for Cyberspace: Distributed Security*, 10 B.U. J. Sci. & Tech. L. 1, 8-11 (2004).
13. *Id.* at 9-10.
14. *Id.*

human threats by creating a separate institution (the military) to resolve threats from "outsiders."[15] Our reliance on the military to deal with external human threats increased as societies evolved into territorially-based nation-states; "territory" became the point of demarcation between external threats and challenges to internal order.[16]

Internal order is achieved by structuring the relationships and activities of those who comprise a society in predictable, productive ways.[17] "Civil" rules structure relationships (ruler-ruled, husband-wife, employer-employee) and allocate essential tasks (farmer, teacher, mayor).[18] They set legitimate social expectations (emancipation, safety, property ownership) and establish a baseline of order by defining the behaviors that are "appropriate."[19] Members of a society tend to abide by its civil rules because they are socialized to believe in the society's civil rules; they also perceive conforming their behavior to the civil rules as the "right" thing to do.[20] They gain approval and avoid disapproval by conforming to the dictates of the civil rules.[21] Civil rules suffice to maintain order in other biological systems, but human beings are highly intelligent, and therefore, have the capacity to deviate; unlike other species and the artificial entities so far created, humans can, and do, deliberately violate the rules that are meant to maintain internal order.[22]

Societies deal with this by implementing an additional set of rules – "criminal" rules – that reinforce the need to obey civil rules.[23] Every society will, for example, have civil rules that define property rights and criminal rules that prohibit violating property rights and prescribe sanctions for doing so.[24] These sanctions include, but are not limited to, societal disapproval; criminal sanctions focus on punishment and include incarceration, death, fines and banishment.[25] Modern societies let individuals sort out disagreements over the application of civil rules (civil litigation), but they maintain exclusive control over their criminal rules because the violation of such a rule is a profound threat to internal order.[26] No society can survive if its members are free to prey upon each other.[27]

---

15. *Id.* at 10.
16. *Id.* at 10-11.
17. *Id.* at 31-45.
18. Brenner, *supra* n. 12, at 35-39
19. *Id.*
20. *Id.* at 41-42.
21. *Id.*
22. *Id.* at 41.
23. *Id.* at 42.
24. Brenner, *supra* n. 12, at 42-43.
25. *Id.* at 42-46.
26. *Id.* at 45-46.
27. *Id.* at 46.

Societies must therefore *enforce* their criminal rules; they must ensure that the rules are being obeyed and maintaining order.[28] Crime is a complex, enduring aspect of human social life; societies accept that they cannot eliminate it and so strive to control it. Historically, these efforts have been based on the assumptions that sanctioning those who violate criminal rules (a) expresses societal condemnation of the violations, (b) exacts punishment for the affront to society, and most importantly for our purposes, (c) controls crime by deterring future violations.[29] This last assumption incorporates two subsidiary assumptions: (i) sanctions deter violations by presenting us with a simple choice—obey rules or suffer the consequences; and (ii) rule violators will be identified, apprehended and sanctioned.[30] The first assumption is based on the premise that inflicting punishment increases the "cost" of violating a criminal rule; when the "cost" becomes high enough, so the logic goes, individuals will refrain from violating the rule.[31] Studies, however, show that the deterrent effect of punishment is a joint function of (i) the severity of the punishment and (ii) the likelihood of being punished.[32]

Therefore, crime control requires that there be some system in place which ensures rule violators are identified, apprehended and sanctioned.[33] There must, in other words, be a credible threat of retaliation for violating criminal rules; absent such a threat, the rules and their attendant sanctions cannot deter crime and maintain internal order.[34] Until recently, societies tended to rely on citizen enforcement to sustain this threat; individuals were required to apprehend criminals or face fines and other punishments.[35] In colonial America, for example, law enforcement was the " . . . duty of every citizen. Citizens were expected to be armed and equipped to chase suspects on foot, on horse, or with wagon . . . ."[36]

While this system may have been adequate for largely rural societies, its effectiveness eroded as urbanization increased with the Industrial Revolution; the attendant rise in urban crime led to various efforts to develop an alternative system, all of which failed.[37] The current model of law enforcement emerged in 1829, when Sir Robert Peel created the London Metropolitan Police.[38] The Metropolitan Police was some-

28. *Id.* at 47-48.
29. *Id.* at 59-60.
30. Brenner, *supra* n. 12, at 59-61.
31. *Id.* at 60-61.
32. *Id.* at 51-52.
33. *Id.* at 61-64.
34. *Id.*
35. *Id.*
36. Roger Roots, *Are Cops Constitutional?*, 11 Seton Hall Const. L.J. 685, 692 (2001).
37. Brenner, *supra* n. 12, at 59-64.
38. *Id.*

thing new: an independent, quasi-military agency staffed by full-time, uniformed professionals whose sole task was to react to crimes and apprehend the perpetrators, who would then be appropriately punished.[39] Peel's model quickly migrated to America and then spread around the world; it has been the dominant approach to crime control for at least a century.[40] As a result, citizens in the twenty-first century assume no responsibility for crime; they regard that as the sole province of professionalized, quasi-military police forces who maintain internal order by reacting to completed crimes.[41]

III. CRIME

The model described above evolved to deal with real-world crime, i.e., crime that occurs in a physical environment.[42] Four characteristics of real-world crime shaped the way this model approaches crime: proximity; scale; physical constraints; and patterns.[43]

In real-world crime, the perpetrator and victim are physically proximate when a crime is committed (or attempted).[44] It is, for instance, not possible to rape, or realistically attempt to rape someone, if the rapist and the victim are fifty miles apart; and in a non-technological world, it is physically impossible to pick someone's pocket, rob them or defraud them out of their property if the thief and victim are in different cities, different states or different countries.[45]

Real-world crime tends to be one-to-one crime; it usually involves one perpetrator and one victim.[46] A crime begins when the victimization of the target is begun and ends when it is concluded; during this event the perpetrator focuses her attention on consummating that crime.[47] When it is complete, she can move onto another crime and another victim.[48] Like proximity, the one-to-one character of real-world crime derives from the constraints physical reality imposes upon human activity: a thief cannot pick more than one pocket at a time; scam artists defraud one person at a time; and prior to firearms, it was very difficult to cause the simultaneous deaths of more than one person. Real-world crime therefore tends to be serial crime.[49]

---

39. *Id.*
40. *Id.*
41. *Id.*
42. *Id.* at 6-11.
43. Brenner, *supra* n. 12, at 49-53.
44. *Id.*
45. *Id.*
46. *Id.*
47. *Id.*
48. *Id.*
49. Brenner, *supra* n. 12, at 49-53.

Physical constraints have other consequences for real-world crime. Like other areas of human endeavor, real-world crimes, even very simple crimes, require some level of preparation, planning and implementation if they are to succeed.[50] One who intends to rob a bank must visit it to learn about its layout, security and routine; this exposes her to scrutiny from witnesses whose observations may later contribute to her being apprehended.[51] As she robs the bank, she leaves trace evidence behind and is again subject to observations (height, weight, accent, skin color, sex) that can result in her being apprehended; the same is true as she flees the scene.[52] She may have obtained a weapon or a disguise before the robbery, and may need help disposing of the money afterward. Each step takes time and effort and thereby augments the exertion required to commit the crime and increases the risks involved in its commission.[53]

Patterns emerge in the real-world crimes committed in a society.[54] Victimization tends to fall into patterns for two reasons. One is that only a small segment of a society will persistently commit crimes; they are likely to be from economically-deprived backgrounds and reside in areas that share demographic characteristics.[55] These offenders will be inclined to concentrate their depredations on people who live in these areas because they are convenient victims; consequently, much of the routine crime in a society will be concentrated in identifiable areas.[56] The other reason is that societies have a repertoire of crimes that range from more to less serious in terms of the "harm" each inflicts.[57] Rape produces nonconsensual sexual intercourse, theft results in a loss of property, murder causes a loss of life and so on. In societies that are maintaining the necessary baseline of internal order, serious crimes will occur much less often than minor crimes.[58]

These characteristics became embedded assumptions about the nature of real-world crime which shaped our current approach to law enforcement.[59] The assumption of proximity added a basic dynamic: victim-perpetrator proximity and victimization; perpetrator efforts to evade apprehension; investigation; identification and apprehension of the perpetrator.[60] This dynamic reflects a time when crime was local, when victims and perpetrators lived in the same neighborhood or vil-

50. *Id.*
51. *Id.*
52. *Id.* at 52.
53. *Id.*
54. *Id.* at 53.
55. Brenner, *supra* n. 12, at 53.
56. *Id.*
57. *Id.* at 54.
58. *Id.*
59. *Id.* at 55.
60. *Id.*

lage.[61] A victim might know the perpetrator by name or by reputation; if she did not know him, there was still a good chance he could be identified by witnesses or by his ties in the community. If the perpetrator was a stranger, this enhanced the likelihood of his being apprehended; he would "stand out" as someone who did not belong. Law enforcement deals effectively with this type of crime because its spatial limitations mean investigations are limited in scope; investigations still focus on the physical scene of the crime.[62]

The model incorporates one-to-one victimization as its default assumption and that, in conjunction with another assumption, yields the proposition that crime is committed on a limited scale.[63] The other assumption is that law-abiding conduct is the norm and crime is unusual.[64] This assumption derives from the operation of the rules discussed earlier: Individuals are socialized to accept civil rules as prescribing the "correct" standards of behavior; criminal rules reinforce this by emphasizing that the behaviors they condemn are outside the norm, extraordinary.[65] The result is that crime becomes a subset, usually a small subset, of the total behaviors in a society; the limited incidence of criminal behavior, coupled with one-to-one victimization as the default crime mode, means law enforcement personnel can focus their efforts on a limited segment of the conduct within a given society.[66] Essentially, it means crime is "manageable."

Finally, the model incorporates the premise that crime falls into patterns.[67] It assumes crime will be limited in incidence and in the types of "harms" it inflicts; it also assumes that an identifiable percentage of crime will occur in geographically and demographically demarcated areas.[68] The combined effects of localized crime, and the differential frequency with which various crimes are committed, gives law enforcement the ability to concentrate its resources in areas where crime is most likely to occur, further enhancing its ability to react to completed crimes.[69]

IV. CYBERCRIME

There is no generally accepted precise definition of "cybercrime." The activity can consist of traditional crimes (fraud, theft, extortion) or

61. Brenner, *supra* n. 12, at 55.
62. *Id.* at 56.
63. *Id.*
64. *Id.*
65. *Id.*
66. *Id.*
67. Brenner, *supra* n. 12, at 58.
68. *Id.*
69. *Id.* at 69-85.

"new" types of criminal activity (denial of service attacks, malware). Cybercrime raises new and difficult challenges for a society's need to maintain internal order; the challenges arise not from the need to adopt new law criminalizing the activity at issue, but from law enforcement's ability to react to it. Cybercrime does not share the characteristics of real-world crime that shaped the current model of law enforcement.[70]

First of all, it does not require physical proximity between victim and perpetrator; they can be in different cities, in different states or in different countries.[71] All the perpetrator needs is a computer linked to the Internet; with this, he can attack a victim's computer, defraud her or obtain information he can use to commit fraud on a grand scale.

One-to-one victimization is not a valid default assumption for cybercrime because it can be automated.[72] A criminal using technology can commit thousands of crimes quickly and with little effort; one-to-many victimization is therefore the correct default assumption for cybercrime.[73] Under the current model of law enforcement, officers react to a crime by investigating and apprehending its perpetrator; the model assumes officers can react to discrete crimes because crime is committed on a limited scale. Cybercrime violates this assumption in two ways: though it is carried out by a small percentage of the population, this relatively small group can commit crimes on a scale far surpassing what they could achieve in the real-world; consequently, the number of cybercrimes will drastically exceed real-world crimes.[74] Further, cybercrime is added to the real-world crime with which law enforcement must continue to deal. These factors combine to create an overload. Law enforcement's ability to react to cybercrime erodes because the resources that were minimally adequate to deal with real-world crime are quite inadequate to deal with cybercrime and with cybercrime-plus-real-world-crime.[75]

Cybercriminals avoid the physical constraints that govern real-world crime; funds can be extracted from a bank and moved into offshore accounts with little effort and less visibility. The reactive strategy is far less effective against online crime because the reaction usually begins well after the crime has been committed; the trail, such as it is, is cold.[76] Another problem is that since much of the conduct involved in committing the crime occurs in an electronic environment, the "physical" evidence, if any, is evanescent and volatile.[77] By the time police react, it

70. *Id.* at 65-75.
71. *Id.*
72. *Id.*
73. Brenner, *supra* n. 12, at 65-75.
74. *Id.*
75. *Id.*
76. *Id.*
77. *Id.*

may have been destroyed. And since perpetrators are seldom present at the crime "scene," assumptions about their being observed while preparing for, committing or fleeing from the crime no longer hold. Indeed, officers may not be able to determine where the perpetrator was located or who he is; cybercriminals, unlike their real-world counterparts, can enjoy perfect anonymity.[78] Even if officers can identify the perpetrator, gathering evidence and apprehending him can be difficult; the country that hosts the perpetrator may decline to extradite him and/or to cooperate in the investigation.[79]

We cannot, as yet, identify offender-offense patterns comparable to those we have for real-world crime, which makes it difficult for law enforcement to allocate its resources to deal with cybercrime. Several factors account for our inability to identify cybercrime patterns: First, it is not well documented; second, agencies often do not break cybercrime out into a separate category so that online fraud, for example, is noted as "fraud;"[80] third, it can be difficult to parse cybercrime into discrete offenses: Is a virus that causes billions of dollars in damage in fifteen countries one crime or thousands of crimes?; and finally, the most important factor is that we do not have accurate cybercrime statistics because many cybercrimes go undetected and many that are detected go unreported.[81] Cybercrime is not detected because security systems cannot detect outside penetrations, or attacks are carried out by trusted insiders who can hide their tracks. It goes unreported because commercial victims, at least, are not inclined to admit they have been attacked by a cybercriminal; they prefer not to reveal their vulnerability to their customers and shareholders.[82]

V. A NEW APPROACH

Our current model of law enforcement is a product of the early nineteenth century, when technology was in its infancy.[83] The model is in many respects an analogue of the military model we use for external threats: both concentrate on organizing personnel and resources to react to activity carried out by individuals at a specific, known physical location.[84] Both use hierarchical organization and chains of command to orchestrate their reactions, which is an appropriate approach to achiev-

78. *Id.*

79. Brenner, *supra* n. 12, at 65-75.

80. *Id.*

81. *Id.*; *see e.g.* Andy Sullivan, *Hacking Attacks Rarely Made Public, Experts Say*, http://www.boston.com/business/technology/articles/2005/02/21/hacking_attacks_rarely_made_public_experts_say/? (Feb. 21, 2005).

82. Brenner, *supra* n. 12, at 70-75.

83. *Id.*

84. *Id.*

ing objectives in the real-world.[85]

Technology eliminates the need, and indeed the ability, to focus on localized activity. Communication technologies, including cyberspace, free us from spatial constraints; we can communicate with anyone anywhere in the world. New technologies generate new types of social organization,[86] and communication technologies have created the network. Networks tend to displace hierarchies because hierarchical organization evolved to deal with real-world activity; as such, it is not an effective means of organizing technologically-mediated activities.[87]

Networks are lateral, fluid systems that decentralize power and authority and empower individuals.[88] Networks can be constructive implements of social change, but, like other forms of social organization, they can also be used for destructive purposes. This has been true of other emerging forms of organization; when hierarchies emerged, they were used for war and military conquest. Often, the "bad guys" are the first to adopt new forms of social organization, primarily because the "good guys" are likely to be locked into the established organizational mode and find it difficult to adapt quickly.[89]

This is precisely what is happening as to cybercrime and other cyber-mediated threats: law enforcement operations are structured by a model that was developed to deal with real-world crime. Cybercrime, in all its variations, does not share the characteristics of real-world crime that shaped this operational model; the model cannot, therefore, deal effectively with cybercrime. This is unacceptable because cybercrime poses a unique threat to the order and stability societies require if they are to survive. Unlike real-world crime, which inflicts "harm" of various types upon discrete victims, cybercrime can inflict both individual "harm" and systemic "harm." Cyberspace and related technologies have become an essential part of national critical infrastructures, and our reliance upon these technologies will only increase.[90] While cybercrime

85. *Id.*

86. *See e.g.* David Ronfeldt, *Tribes, Institutions, Markets, Networks: A Framework about Societal Evolution Pinpoint*, http://www.rand.org/publications/P/P7967/P7967.pdf (1996).

87. *See e.g.* Brian Nichiporuk & Carl H. Builder, *Societal Implications*, in In Athena's Camp: Preparing for Conflict in the Information Age, 298-299, (Rand 1997).

88. *See id.*

89. David Ronfeldt & John Arquilla, *What Next for Networks and Netwars?*, in In Networks and Netwars: The Future of Terror, Crime and Militancy, 313 (Rand 2001).

90. *See e.g.* Office of the President, *The National Strategy to Secure Cyberspace* 5-7, 37-41, http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf (Feb. 2003). Much of the conduct defined as cybercrime can threaten a system's ability to maintain external order, as well as internal order. The distinction is between attacks upon individual citizens of a social system ("crimes") and attacks on the social system itself ("terrorism"). Acts which are encompassed by definitions of terrorism also represent "crimes." Timothy McVeigh, for

harms individual victims, it is not limited to that; as the National Strategy to Secure Cyberspace noted, cybercrime can undermine or even destroy a nation's critical infrastructure. This makes it a far more pressing threat than traditional, real-world crime; in a sense, cybercrime erodes the distinction between internal and external threats.[91] As long as human activity was grounded only in the real-world, societies could divide threats into external and internal and allocate the responsibility for dealing with each to respective social institutions; while society will always need institutions to deal with real-world threats, it no longer lives only in the real-world. We need a strategy to deal with threats that come from the virtual world, and in devising that strategy, we need to decide if we should retain the historical distinction between internal and external threats.

Logically, there are two ways we can go about developing such a strategy: retain the reactive model and improve its ability to react to cybercrime or abandon it in favor of a new approach. If we retain the reactive model, we should continue to differentiate between internal and external threats since the source of an attack can determine what type of response is appropriate. As explained below, reactive responses mediated through cyberspace can be seen as an act of war even though they were intended as a response to cybercriminal activity.

VI. PROPOSALS FOR IMPROVING REACTION

The problems cybercrime poses for the reactive model of law enforcement have been apparent for some time. Some contend that these problems can be addressed by improving the efficacy of the reactive strategy and have offered proposals to this end. The sections below examine the three proposals that have been put forward as ways to improve the reactive model; they also review two other possibilities for achieving the same end.

A. CONVENTION ON CYBERCRIME

In the 1980's, various international groups began working on the problem of cybercrime; they recognized that its transnational character posed new challenges for law enforcement and set about devising solutions for these challenges. The most important of these efforts occurred

example, engaged in a terrorist act and, in so doing, committed murder and large-scale property damage and destruction. The critical difference between cybercrime-as-terrorism and "crimes"-as-terrorism is that "crimes" have to be executed within the physical boundaries of the system, whereas cybercrimes do not. *See generally* Susan W. Brenner & Marc D. Goodman, *In Defense of Cyberterrorism: An Argument for Anticipating Cyber-attacks*, 2002 U. Ill. J.L. Tech. & Policy 1 (Feb. 2003).

91. Brenner, *supra* n. 12, at 74-76.

in Europe: between 1989 and 1997, several entities – including the Organisation for Economic Cooperation and Development, the United Nations, the European Commission and the G8 – issued reports dealing with the legal issues presented by transnational cybercrime.[92] A common theme in these reports was the need for nations to have consistent, adequate laws defining the basic cybercrime offenses and standardizing the procedures governing cybercrime investigations.[93] In 1997, the Council of Europe returned to the problem: its European Committee on Crime Problems created a "Committee of Experts on Crime in Cyberspace" and directed the new Committee to draft "a binding legal instrument" dealing with these issues.[94]

The Committee spent four years working on this assignment. Its Convention on Cybercrime went through twenty-seven drafts before the final version was submitted to the European Committee on Crime Problems at its 50th Plenary Session, June 18-22, 2001.[95] The Convention was approved and opened for signature on November 23, 2001.[96] At the time of this writing, it has been signed by thirty-nine countries—including the United States—and ratified by nine.[97] The Convention becomes binding three months after the date on which a country ratifies it, so it went into effect on July 1, 2004 as to the first five countries to ratify it: Albania, Croatia, Estonia, Hungary and Lithuania.[98] On September 1, 2004, it went into effect in Romania; it will go into effect in Slovenia and the former Yugoslav Republic of Macedonia on January 1, 2005.[99]

The drafters of the Convention recognized that gaps and conflicts in national law impede law enforcement's ability to react to cybercrime.[100] The Convention seeks to remedy this by (i) harmonizing national laws that define cybercrimes, (ii) ensuring that countries have the procedural law needed to facilitate the investigation and prosecution of cybercrimes,

92. *See e.g.* Marc D. Goodman & Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace*, 2002 UCLA J. L. & Tech. 3, 39-45 (2002).

93. *See id.*

94. *See id.*

95. *See* Council of Europe, *Convention on Cybercrime, Explanatory Report* ¶¶ 7-15, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm (accessed Dec. 22, 2005) [hereinafter "Explanatory Report"].

96. *See* Council of Europe, Chart of Signatures and Ratifications, Convention on Cybercrime (CETS No. 185) (Nov. 23, 2001), http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=ENG.

97. Council of Europe, *Convention on Cybercrime, CETS No.: 185*, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=12/07/04&CL=ENG (accessed Dec. 22, 2005) [hereinafter "Convention on Cybercrime"].

98. *See* Council of Europe, *Article 36 – Signature and Entry into Force* ¶¶ 3-4, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm; *see also id.*

99. *See* Convention on Cybercrime, *supra* n. 97.

100. *See* Explanatory Report, *supra* n. 95, at ¶¶ 1-15.

and (iii) creating an international network to facilitate law enforcement cooperation.

The Convention's underlying premise—that harmonizing national laws will improve law enforcement's ability to react across national borders—is unobjectionable. The difficulty lies in its implementation. The Convention has been ratified by nine countries; even if we assume that the remaining, roughly, 180 countries ratify it, that does not end the matter. The Convention contains forty-eight articles, at least thirty-three of which require parties to adopt legislation or take other implementing measures.[101] This will be a less-than-onerous task for countries like the United States, which have cybercrime laws in place; it can be an onerous task for those that do not. The task will be further complicated by differences in local law and culture; the Convention was drafted by Europeans who received substantial input from American lawyers.[102] Consequently, it incorporates notions of substantive and procedural law that may not be routine in other parts of the world. This does not mean countries cannot implement the Convention; it means implementing the Convention will be a complicated process for many countries, one that will take time. Consequently, even if the Convention proves to be a viable means of improving law enforcement's ability to react to transnational cybercrime, we are unlikely to see any marked improvement in the near future.

B. Law Enforcement Strikeback

Professor Reidenberg has proposed letting law enforcement use "electronic sanctions" to react to cybercrime.[103] "Electronic sanctions" include hacking and denial of service attacks, along with disseminating viruses, worms and other types of malware. Officers would use these techniques to shut down or destroy foreign Web sites used to commit crimes in their country.

What he proposes is an official version of an approach that has been discussed for some time: civilian "self-help" or "strikeback" techniques which, as explained below, would supplement law enforcement reactions to cybercrime. Professor Reidenberg's proposal is not an advisable strategy for improving law enforcement's ability to react to cybercrime because (a) it suffers from the problems outlined below, and (b) it adds the official imprimatur of the state to what he concedes are illegal acts. As to

101. *Id.* at ¶¶ 18-19. *See also* Convention on Cybercrime, *supra* n. 97, at Articles 2-22, 24-27 and 29-34.

102. *See* U.S. Dept. of Justice, *Frequently Asked Questions and Answers About the Council of Europe Convention* § QA(3), (Nov. 10, 2003) (available at http://www.cybercrime.gov/COEFAQs.htm#QA3).

103. *See* Joel R. Reidenberg, *States and Internet Enforcement*, 1 U. Ottawa L. & Tech. J. 213, 228 (2004).

the latter, he suggests illegality is not a major concern because the officers' conduct would be encompassed by sovereign immunity.

Invoking sovereign immunity is unlikely to appease a nation whose sovereignty was violated by agents of another state. In 2000, Federal Bureau of Investigation ("FBI") agents lured two Russians, Alexey Ivanov and Vasiliy Gorshkov, to Seattle in a "sting" operation.[104] The agents had identified them as the hackers who had been victimizing United States businesses. They came to Seattle and were arrested after using FBI laptops to demonstrate their skills. FBI agents used data obtained from keystroke loggers on the laptops to download files from Russian computers that Ivanov and Gorshkov used to store files; they did not obtain a search warrant before doing this.

Gorshkov moved to suppress the files, claiming that the agents violated Russian law by hacking into the computers and downloading files. Perhaps relying on sovereign immunity, the court held that Russian law did not apply to the agents. Russian authorities did not agree. The Russian Federal Security Service ("FSB") opened an investigation into the agents' actions and eventually charged one with hacking. United States authorities ignored Russian requests to turn him over for prosecution; this apparently did not surprise FSB officers, who said they brought the case as "a matter of principle," concerned "that the FBI will continue to proceed this way in the future."[105]

The agents did not set out to violate Russian law or sovereignty; they unsuccessfully sought assistance from Russian authorities and then turned to self-help. Anecdotal evidence indicates that their actions adversely affected United States officers' ability to obtain cooperation from abroad. What was perceived as high-handed conduct sparked resentment that has impeded the informal cooperation, which is an essential aspect of any transnational criminal investigation. That is a minor consequence of sanctioning official self-help; as Professor Reidenberg concedes, law enforcement strikeback is "a form of information warfare."[106] As such, it is too high a price to pay for incrementally enhancing law enforcement's ability to react to online crime.

C. Civilian Strikeback

This option would let civilians react when they become the actual or attempted targets of cybercrime, on the assumption that their efforts will

104. *See United States v. Gorshkov*, 2001 WL 1024026 at *1 (W.D. Wash. May 23, 2001).

105. Nicolai Seitz, *Transborder Search* § 2, http://islandia.law.yale.edu/isp/digital%20cops/papers/Seitz_Nicolai.pdf (accessed Dec. 12, 2005).

106. *See* Reidenberg, *supra* n. 103, at 229.

supplement the reactive capabilities of law enforcement officers.[107] In reacting, they would use techniques similar to those which Professor Reidenberg would make available to law enforcement.

Like the law enforcement version, civilian strike-back raises difficult legal questions; aside from anything else, civilians who react would be committing crimes. But it ultimately flounders on the practical risks involved: victims whose computer skills are limited may not be able to trace an attack back to the perpetrator's computer and so may retaliate against the wrong computer system. Their retaliation could shut down a system operated by, say, a hospital, a government agency or a telecommunications company. As one expert noted, the remedy would be "worse than the disease," because the reaction would inflict injury not only upon the computer system that was attacked, but also on those who relied upon it for vital services.[108]

Finally, civilian strike-back is a type of vigilantism;[109] and, as such, it is subject to the objections that have been raised to real-world vigilantism.[110]

D. More Officers

This seems an obvious solution: increase the number of officers who can react. As was explained earlier, cybercrime erodes the effectiveness of the reactive model by increasing the number of crimes to which officers must react; it is "new" crime that is added to the real-world crime with which they must still deal. It seems that increasing the number of officers available to react should offset this effect and restore the efficacy of the reactive model. However, there are two problems with this theory. First, societies already find it difficult to allocate the resources needed to support existing law enforcement agencies; it is highly improbable that they could summon the resources needed to recruit, train and equip enough officers to make the reactive strategy a viable approach to cybercrime. Second, since cybercrime is, and will continue to be, increasingly automated, there is no guarantee that increasing the number of officers will improve the efficacy with which law enforcement agencies can react. It is no longer a matter of fielding officers to track down a perpetrator and apprehend him before he can re-offend; while officers seek the perpe-

107. *See* Curtis E.A. Karnow, *Strike and Counterstrike: The Law on Automated Intrusions and Striking Back* § 2, http://www.blackhat.com/presentations/win-usa-03/bh-win-03-karnow-notes.pdf (accessed Feb. 27, 2003).

108. *See id.*

109. *See e.g.* Bruce Schneier, *Counterattack* Crypto-Gram, http://www.schneier.com/crypto-gram-0212.html (accessed Dec. 15, 2002).

110. *See* Kelly D. Hine, *Vigilantism Revisited: An Economic Analysis of the Law of Extra-Judicial Self-Help or Why Can't Dick Shoot Henry for Stealing Jane's Truck?*, 47 Am. U. L. Rev. 1221, 1227-1228 (1998).

trator of one cybercrime, he can use automated systems to commit hundreds or even thousands of other crimes, to which they will also have to react.

Instead of relying on human officers, we could automate the reaction. We could use automated agents to react to cybercrime or patrol cyberspace to apprehend criminals, just as state troopers patrol interstate highways.[111] While automated cyberpolicing is a logical alternative, its adoption and implementation would be fraught with technical and legal difficulties that make it an unrealistic option, at least for the foreseeable future.[112]

E. Private Sector Participation

What if, instead of hiring more officers, law enforcement recruited the private sector to assist in its battle with cybercrime? This would eliminate the need for additional funding while providing additional personnel and resources, the quality of which would be equal or superior to those that are otherwise available. It would be necessary to decide how and to what extent members of the private sector could be recruited into this effort. As to the latter, would private parties only participate when they had been victimized? Or, would they be part of some greater effort against cybercrime? How would we integrate their participation into the legal framework that currently encompasses criminal investigations?

These questions are beyond the scope of this article, but it is useful to consider the possibility of utilizing private sector resources to improve our reaction to cybercrime. The critical question is one that was not raised above: *How* would the private sector contribute to the effort against cybercrime? Would we recruit members of the private sector into law enforcement's reactive efforts, similar to the posse of old westerns? If so, what would be the scope of their authority? Would it be limited to investigating and identifying perpetrators or would it also extend to apprehending them?

Using the private sector to investigate cybercrimes, at least some cybercrimes, seems an unavoidable reality for the present. When an artificial entity (commercial, governmental or educational) is attacked, its staff will probably be the first to realize there has been an attack; as part of responding to it, they will investigate the nature and source of the attack. So far, such activity is not regarded as part of a law enforcement effort to apprehend the perpetrators, and therefore, is generally not encompassed by the constitutional and statutory restrictions that apply to law enforcement investigations. This is reasonable because the staff's

111. *See e.g.* Kevin Manson, *Robots, Wanderers, Spiders and Avatars*, http://www.search.org/conferences/1997Internet/acjs_search.htm (accessed Nov. 5, 1997).

112. *Id.*

investigatory efforts are, after all, analogous to the conduct of a real-world burglary victim who examines her property to determine what is missing and how the unlawful entry was effected; though she will no doubt communicate what she learns to the officers who investigate the crime, she is not an agent of the state and is not required to abide by the standards governing official investigations.

This is not true when private parties are recruited by law enforcement to assist in their investigation of a crime. Federal and state statutes specifically allow law enforcement to obtain the assistance of private parties in executing search warrants, but when they do this, the private parties become agents of the state.[113] If we let law enforcement officers utilize private resources (personnel and equipment) to investigate cybercrimes, the private actors would become agents of the state and their actions would be subject to the constitutional and statutory restrictions that govern law enforcement. That would create an interesting dichotomy: Private parties would not be subject to these restrictions when they were investigating cybercrimes against themselves, but would be subject to them when assisting in the investigation of cybercrimes against others. This outcome is consistent with current law, but it is not appropriate for a system in which private parties become integral components of the reactive strategy. It is only logical to assume that having become part of this strategy, private parties would pursue the investigation of any cybercrime as state agents; therefore, if we were to adopt this, as yet, hypothetical tactic, we would have to revise our law so that it encompassed "permanent" state agents.

Would we let these "permanent" state agents apprehend cybercriminals? We could approach this as the logical consequence of heading down this path: the purpose of recruiting private parties is, after all, to improve our ability to react to cybercrime; an essential aspect of that reaction is arresting offenders so they can be prosecuted and sanctioned for their crimes. Since law enforcement personnel cannot accomplish this alone, it seems logical to deputize these "permanent" state agents and let them apprehend cybercriminals. This might increase the number of arrests, but it is *not* a good idea. If we let "permanent" state agents make arrests, we would confront the issue considered with regard to civilian strikeback; we would run the risk that civilian enforcement agents would arrest the wrong person. We would also be sanctioning private parties' using some level of physical force to arrest cybercriminals; unless we were to train these "permanent" state agents in the use of force (which would not be cost-effective), we would create an unacceptable risk of injury or death to them and to those whom they sought to apprehend. Our hypothetical venture into using private parties to improve the reac-

113. *See e.g. U.S. v. Ellyson*, 326 F.3d 522, 527 (4th Cir. 2003).

tive model's effectiveness against cybercrime cannot extend to authorizing them to make arrests. Actually, there may be no need to do this: recruiting private parties to assist in *investigating* cybercrime should free up officers who could use their time to pursue cybercriminals. Instead of using private parties as surrogate officers, we could limit them to investigating cybercrime and reallocate officers so they concentrated on apprehending offenders.

The approach outlined above is speculation, but it is already apparent that cybercrime requires a law enforcement/private sector initiative. Since we equate crime control efforts with the reactive strategy, we are inclined to assume such an initiative must involve injecting private sector participation into that strategy. However, doing this raises difficult legal questions by blurring the distinction between "public" and "private" actors. The sections below consider another option: civilian participation in a non-reactive crime control strategy.

VII. A NEW MODEL

If we cannot transform the reactive model into an effective cybercrime control strategy, we must implement a new model. This does not mean we will abandon the reactive model; it has proven a workable approach to real-world crimes and should be retained for that purpose. We can use it to deal with cybercriminals who can be apprehended; if the model outlined below is successful, it will reduce, but not eliminate, the number of cybercrimes. There are valid reasons to pursue and prosecute those who commit these crimes whenever we can: it provides a measure of deterrence, which is important, even though the new model shifts our focus away from reaction; it also emphasizes our condemnation of the conduct at issue.

The new model recognizes that deterrence and prevention require not just *ex post* law enforcement aimed at criminals, but also extensive *ex ante* administrative regulation of the arenas in which cybercrimes are committed – the computers and other information technology products used by victims and dupes, with violations of that regulation punished by criminal sanctions.

As to the alternate model, there are two ways to approach crime control: react to crimes that have been committed or prevent crimes from being committed. The reactive model incorporates prevention insofar as it is seeks to deter offenders, but this is not its primary focus.[114] Prevention is the focus of community policing, which uses police-citizen cooperation to create a climate in which crime is not tolerated.[115] Community

114. *See supra* §§ II & III.

115. *See e.g.* Barry N. Leighton, *Visions of Community Policing: Rhetoric and Reality in Canada*, 33 Canadian J. Criminology 485, 487 (1991); David Thacher, *Equity and Commu-*

policing, as such, is not a viable option for cybercrime: it would require assigning officers to "patrol" cyberspace, and that would require resources which are simply not available.[116] Also, community policing succeeds in the real-world because those who participate want to ensure the safety of the neighborhood in which they live.[117] Cyberspace "communities" are defined by interests, not territory;[118] those who belong to these "communities" are less likely to cooperate with police to discourage cybercrime because they lack the central, binding focus a physical neighborhood provides.

While community policing is itself not an appropriate strategy for cybercrime, we can derive such a strategy from the philosophy behind community policing. It recruits civilians into the law enforcement effort not as officers charged with reacting to crime, but as partners in an effort to prevent crime.[119] This is in a sense reviving the older systems in which citizens assumed responsibility for crime control.[120] It is also a departure from those systems; they relied on reaction as the primary crime control strategy because it is effective against territorially-based crime. Since cybercrime is not territorially-based, we need a new approach: prevention. To the extent we prevent cybercrime, we eliminate the need for a reaction. By preventing a significant quantum of cybercrime, we control it and its capacity to undermine internal order; we also increase the possibility of a successful reaction by law enforcement or by law enforcement-plus-private-enforcement-agents, to at least some of the cybercrimes we are unable to prevent.

A. PREVENTION

Prevention can take many forms. The critical aspect of the new model lies not in prescribing specific preventive measures, but in shifting

---

nity Policing: A New View of Community Partnerships, 20 Crim. Justice Ethics 1, (2003); Gerasimos A. Gianakis & G. John Davis, *Reinventing or Repackaging Public Services? The Case of Community-Oriented Policing*, 58 Pub. Admin. Rev. 1 (1998).

116. Many agencies have officers who are assigned to cybercrime, and many of them "patrol" certain areas of cyberspace. No agency, however, maintains a twenty-four/seven presence in cyberspace and it is exceedingly unlikely any will be able to do so in the foreseeable future. *See e.g.* Gary Nurenberg, *Cracking Down on Online Predators*, TechTV Vault, http://www.g4tv.com/techtvvault/features/28652/Cracking_Down_on_Online_Predators.html (accessed Aug. 22, 2002); Molly Masland, *Stalking Child Molesters on the Net*, http://www.msnbc.com/news/192795.asp (accessed Sept. 4, 1998).

117. *See* Leighton, *supra*. n. 115; *see also* Thacher, *supra* n. 115; *see also* Gianakis, *supra* n. 115.

118. *See* Peter Kollock & Marc A. Smith, *Communities in Cyberspace*, in *Communities in Cyberspace* 3-28 (Marc A. Smith & Peter Kollock eds. 1998).

119. *See* Leighton, *supra*. n. 115; *see also* Thacher, *supra* n. 115; *see also* Gianakis, *supra* n. 115.

120. *See supra* §§ II & III.

the focus from reaction ("Cybercrime is law enforcement's responsibility") to prevention ("It's my responsibility to protect myself"). We must realize that we are the front line of defense against cybercrime; we must understand that our carelessness could facilitate a successful cyber-terrorist or information warfare attack on the critical infrastructures of our society. The next section considers how we inculcate this sense of responsibility. This section is concerned with how citizens can discharge that responsibility.

In considering that issue, it is helpful to divide citizens into three categories: individual users; organizational users; and architects. Individual users utilize computer technologies for professional and/or personal purposes in a non-organizational context, and they are individually responsible for the security of their systems and of their online activities.[121] Organizational users utilize computer technologies in an organizational context; they are the individuals who work in an organization and the organization itself. Architects are the individuals and entities that construct cyberspace and the technologies we use to access it; they provide the software and hardware we use to go online. Architects and organizational users become individual users when they access cyberspace from home, or otherwise outside their organizational context.

1. *Individual users*

For individual users, prevention would involve securing their computers and Internet connections to prevent their being used for unlawful purposes; this would entail measures such as installing a firewall and using anti-virus and other software to frustrate harmful programs. Prevention would not, however, be limited to technical measures; individual users, along with organizational users and architects, would also have to resist social engineering[122] and other ploys used by cybercriminals. We should encourage them to report cybercrimes. The downside of encouraging individual reporting is the large volume of data it would generate;

121. They may also be responsible for securing the activities of others; parents might, for example, be held responsible for securing their children's online activities.

122. Wikipedia, *Social Engineering (Computer Security)*, http://en.wikipedia.org/wiki/Social_engineering_%28computer_security%29 (accessed Dec. 22, 2005) (explaining that Social engineering is essentially the process of manipulating individuals for one's own ends. That is, "[S]ocial engineering is the practice of conning people into revealing sensitive data on a computer system. . . . It is an article of faith amongst experts in the field that 'users are the weak link.' . . . Perhaps the simplest, but still effective attack is tricking a user into thinking one is an administrator and requesting a password for debugging purposes. Users of Internet systems frequently receive messages that request password or credit card information . . . to 'set up their account' or 'reactivate settings' or some other benign operation. . . . [I]n an Infosecurity survey, 90% of office workers gave away their password in exchange for a cheap pen."); *see also* Kevin D. Mitnich & William L. Simon, *The Art of Deception* 3-12 (Wiley, John & Sons, Inc. 2002).

the advantage is that we could use the data to identify patterns in cybercrime and craft appropriate responses.

It is not difficult to outline these responsibilities; it would be difficult to implement them. A section below explains how we can use legal rules to hold individual users (and organizational users and architects) responsible for securing their systems and their activities. The problem lies not in imposing responsibility, but in seeing that it is carried out. Individuals vary widely in terms of their computer expertise; we would be requiring every individual, regardless of his or her level of expertise, to resist efforts launched by those whose expertise is extensive and who have compelling incentives (money, political motivations) to launch successful attacks. If we expect such an effort to succeed, we will have to do more than simply impose obligations and consequences for defaulting on those obligations.

What could we do? We should, as is explained below, require only a reasonable effort to secure one's system and one's self from harm; we cannot expect perfection here, just as we cannot expect perfection in our implementation of the reactive model. We could support individual users' efforts to discharge their responsibilities by encouraging them to use particular software and educating them about new hazards emerging online; we currently do this on an *ad hoc* basis, to little effect, but such efforts might be more productive in a system that holds us responsible for our security defaults. Ultimately though, individual users would remain a notable source of vulnerability; it is highly unlikely that amateurs—online versions of weekend warriors—could compete with sophisticated cyberattackers.

We could address this inevitability by encouraging individual users not to "go it alone." If we conceptualize cyberspace as a "place," our society's "border" with that "place" consists of all the computers citizens use to access that "place." We are open to attack at every point along that "border;" our security depends on protecting every one of those points of access. One can argue that requiring individual users to secure their portions of this "border" is no different than requiring individual citizens to take up arms and apprehend criminals, but they differ in a critical respect. Requiring a citizen to apprehend a criminal may have exposed him to physical danger, but it did not require effort that was quite beyond his abilities; at the time these requirements were in place, male citizens were sufficiently familiar with weapons and their use that it was not unreasonable to expect this of them. They might fail, but they had a good chance of succeeding. The opposite is true for requiring individual users to secure their portions of cyberspace; many will be able to accomplish this successfully, but most will not, as noted above.

Given the specialized, ever-evolving nature of the expertise required, it is not reasonable to expect individual users, as a generic group,

to be able to secure our virtual "border." More precisely, it is not reasonable to expect that all individual users, in isolation, will be able to do this. Instead of insisting they "go it alone" we could offer a collective security option: Those who believe they can protect themselves online could take responsibility for their own security; those who feel this is beyond them could use secure access points.

Making individual users responsible for securing their online activities, and encouraging them to discharge this responsibility by utilizing portals, recognizes that cyberspace is a border we must defend and applies the principle that there is "safety in numbers" to that end. Offering less-than-adept individual users the option of relying on portal services not only enhances the security with which they access cyberspace, but also can prevent cybercrime in other ways. Portals can disseminate warnings about social engineering and other behavioral attacks as they arise; they could also create a climate, a "community," that encourages individual users' to "look out for" others, as well as for themselves. They could also be a useful source of data on successful and unsuccessful cybercrimes; it would be easier for an individual user to report such an event via the portal than to locate the appropriate government agency and submit a report there.

2. *Organizational users*

Prevention for organizational users involves the same basic tasks - securing technical systems, evading social engineering and reporting cybercrimes - we would require of individual users, but they take on added layers of complexity in an institutional context. The process of securing computers and related systems has the same basic goals: preventing unauthorized access and loss from malware and attacks. However, it differs, in varying degrees of magnitude, as to scale and intricacy; organizations will have multiple users (ranging from the single digits to many thousands), each of whose computer system must be protected and secured from harm; this is a daunting task. Unlike individuals, organizations have specialists who are assigned to secure their systems, but it can still be difficult to anticipate where, and how, an attack will eventuate. Here, again, we can require only that organizational users make a reasonable effort to prevent their becoming the target of a successful cyberattack.

Resisting social engineering and related tactics is also far more complex; entities must ensure that their employees understand what social engineering is and, at least, are reasonably able to identify and resist such tactics. This could entail instituting policies governing particular types of interactions with outsiders; it could involve training employees to acquaint them with the type of efforts they are likely to encounter.

However, social engineering is not the only "human" threat organizations encounter; unlike individual users, organizations must deal with internal, as well as external, threats. Internal threats come from trusted insiders, such as: current or former employees, consultants, temporary workers and others who legitimately have, or had, access to the entity's systems and processes.[123] Insiders are in a unique position to exploit an institution's resources or assets.[124] For example, they can use its computers to hack other computer systems for malice or profit, they can exact revenge by damaging the organization's computer systems, deleting or altering data, and they can "harvest" information and sell it to others who will use it for illegal purposes, such as economic espionage or fraud.[125] Dealing with the insider threat requires, among other things, that organizations have procedures in place to screen prospective new hires — including consultants and temporary workers—for criminal convictions or other problematic behaviors. Entities should have measures in place to ensure that those who leave the organization surrender passwords and other information they could use to access its systems.[126] Countering the insider threat also requires monitoring employee activities — again including consultants and temporary workers—to identify suspicious behaviors, such as repeatedly coming into the office at odd hours.[127]

These and other measures, which can counter social engineering and insider threats, consume time and resources that can be devoted to achieving an entity's primary task. So far, organizations are apt to resolve these competing priorities by concentrating on their primary task while making some effort to deal with internal and external threats. Several factors contribute to this: One is that entities accustomed to operating in an environment governed by the reactive model do not see cybercrime as their responsibility; that is not to say they do not make an effort to secure their systems or otherwise protect their operations. They do, but not with the rigor needed for an effective preventive crime control strategy; the rules outlined in the next section are designed to alter this by imposing responsibility upon organizational users.

123. *See generally* Eric D. Shaw, Keven G. Ruby & Jerrold M. Post, *The Insider Threat to Information Systems*, http://www.wasc.noaa.gov/wrso/security_guide/infosys.htm (last updated Nov. 28, 2001).

124. *See e.g.* U.S. Secret Service & CERT Coordination Center, *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector 7-13* (2004), http://www.cert.org/archive/pdf/bankfin040820.pdf (accessed Dec. 20, 2005).

125. *Id.*

126. *See e.g.* Eric Shaw, Jerrold Post and Keven Ruby, *Managing the Threat from Within*, Infosecurity, http://infosecuritymag.techtarget.com/articles/july00/features2.shtml (July 2000) (accessed Dec. 12, 2005).

127. *See e.g.* Richard Bejtlich, *What Is Network Security Monitoring?* http://www.awprofessional.com/articles/article.asp?p=350391&seqNum=5 (accessed Dec. 17, 2004).

Responsibility is not the only problem: Other contributing factors are: (a) civilian organizations typically have little experience in conducting security checks of employees, and (b) employee monitoring can be seen as intrusive and antagonistic.[128] Organizations can (a) by hiring outsiders to do the screening, but this can compound the resource problem noted above and may aggravate (b).

We must resolve these issues if we are to implement a preventive model of cybercrime control. Adopting rules that impose responsibility for preventing cybercrime is of little use if those whom the rules target regard them as unworkable and unreasonable. The solution may lie in initiatives launched in the United States and United Kingdom. In the United States, two federal efforts – the U.S. Secret Service's Electronic Crimes Task Forces and the Federal Bureau of Investigation's Infragard program – bring law enforcement officers together with members of the private sector and academics in a collaborative effort against cybercrime. The United Kingdom's National Hi-Tech Crime Unit does something very similar.[129] All of these initiatives are based on the premise that law enforcement, alone, cannot control cybercrime; they see partnerships between law enforcement, academia, business and other aspects of the private sector as essential to maintain the effectiveness of the reactive model. They put some emphasis on cybercrime prevention, but are solidly rooted in the reactive model, which is not surprising, since it has been the dominant approach for more than a century.

While none of these initiatives has explicitly embraced the notion of an alternate model, the concept is implicit in their recognition that cybercrime cannot be the responsibility of law enforcement alone. We can derive an additional element for our model from this recognition, one that addresses the issues noted above and integrates individual users and architects into the model. The rules outlined in the next section hold civilians responsible for preventing cybercrime, but they do not recruit them into this effort. The model cannot succeed if citizen participation is perfunctory; it requires wholehearted, enthusiastic effort on their part. We can achieve this by extrapolating the philosophy behind the current initiatives to its next level; civilians and law enforcement must become partners in a preventive cybercrime control strategy. As long as law enforcement stands apart and holds itself out as "the" group that handles cybercrime, civilians will regard the obligations imposed upon them as superfluous, burdensome annoyances, which only prove law enforcement is not doing its job. An essential part of moving to a preventive model is breaking down this barrier and creating a real partnership.

---

128. *See* Shaw, *supra* n. 126; *see also* Bejtlich, *supra* n. 127.

129. *See* Owner or Author, *National Hi-Tech Crime Unit Mission Statement*, http://www.nhtcu.org/ (accessed Dec. 22, 2005).

Organizational users would be the linchpin of this partnership. First, organizations have more incentives to prevent cybercrime than individual users or architects: They are a focal point for cybercrimes; cybercrimes that target organizations generally cause more "harm" than those that target individuals; and successful attacks on organizations can erode their operations and even threaten critical infrastructures. Many organizations realize this, which is why they participate in the initiatives outlined above. Another reason is that, as noted above, we have a particular interest in preventing attacks against organizations because of the focused "harm" such attacks can inflict: A virus that cripples the computers used by millions of individual users causes great aggregate "harm;" a virus that shuts down telecommunication systems, air traffic control systems or financial systems causes great aggregate "harm" *and* inflicts systemic harm upon a society. Finally, there are the resources available to organizations; unlike individual users, they can contribute personnel, hardware, software and other resources to a cooperative effort for developing systemic approaches to preventing cybercrime.

Law enforcement and organizational users must therefore establish a collaborative relationship the primary focus of which is preventing cybercrime. Unlike the current initiatives, which are apt to concentrate on larger urban areas and larger organizations, this collaboration would encompass the entire country; ideally, it would include every organization in the country. Like the current initiatives, the collaboration would probably include periodic meetings focusing on networking, information sharing and training; it should emphasize twenty-four/seven online communication (listservs, email) as the primary means for sharing and seeking information about threats and threat responses. Members would be required to execute an agreement when they joined; they would, among other things, commit to participating fully in the group's activities. The agreement might allow for varying levels of membership, based on security clearance or other factors;[130] it should also establish procedures for investigating misconduct by organizational and individual members of the collaboration and for sanctioning them when misconduct was established.[131]

What, precisely, would this collaboration encompass? Information-sharing is critical; the relationship would provide a trusted context, as explained below, in which organizational users could report attacks, identify vulnerabilities and submit other pertinent data. This aspect of the collaboration would be used to overcome entities' current reluctance

130. *See* Infragard Connecticut, *What is InfraGard Connecticut's membership application procedure?*, https://secure.infragard-ct.org/public/about/membership_info.html (accessed Jan. 12, 2004).

131. *See* Federal Bureau of Investigation,: *Bylaws of Infragard National Members Alliance*, http://www.infragard.net/library/pdfs/nat_by_laws_new.pdf (accessed Dec. 17, 2005).

to report cybercrime. Law enforcement would contribute information from governmental sources and should serve as the central collection and dissemination point for information generated by the collaboration.[132] The essential elements of this information would be distributed nationally and internationally; if the preventive strategy is to succeed, it must transcend national boundaries, just as cybercrime transcends national boundaries. As part of the collaboration, law enforcement would work with members from the private sector and from academia to develop new technologies and new procedures for securing systems against cyberattacks and nullifying social engineering tactics. This effort would include the architects, who are discussed below. Organizational users could share information about how they prevent and respond to attacks; they could work together to develop best practices for dealing with external attacks and insider threats. The collaboration might also involve law enforcement assisting organizations with vetting new employees and monitoring the activities of current employees; as noted below, this, and other aspects of the collaboration, would require adopting new legal standards governing public-private endeavors.

Collecting and disseminating the information described above would require the exercise of some discretion; the details of a cybercrime can reveal trade secrets, proprietary information and/or other data that can give competitor organizations an advantage.[133] The law enforcement personnel who staff the central collection and dissemination point for the information should filter and redact it so it can be shared without compromising the interests of the organization that provided it.[134] Guarantees that information will be appropriately filtered and redacted before it is shared should be incorporated into the processes organizational users employ in submitting information; the processes should alert organizations to the need to conduct a risk assessment with regard to the information being provided and should allow them to alert law enforcement as to the sensitive nature of particular information being provided.[135] Organizations might also be allowed to submit information for different purposes or in varying levels of specificity.[136]

---

132. *See* National Hi-Tech Crime Unit, *Working With Business: Confidentiality Charter* [hereinafter "National Hi-Tech Crime Unit"] at 6, 8, http://www.nhtcu.org/media/documents/publications/CON_05.pdf (accessed Dec. 20, 2005).

133. *See e.g. Fighting Cyber Crime - Hearing 1 to 3: Efforts by State and Local Officials: Oversight Hearing Before the House Committee on the Judiciary: Subcommittee on Crime*, 107th Cong. 89-98 (June 2001) (Testimony of Harris N. Miller, President, Information Technology Association of America, *available at* http://www.house.gov/judiciary/miller_061401.htm (accessed Dec. 17, 2005)); *see also* National Hi-Tech Crime Unit, supra n. 132.

134. *Id.* at 6, 8.

135. *Id.*

136. *See id.* (explaining strategic versus tactical information, information submitted as "intelligence only").

We would need new legal standards for such a collaborative effort. Our law assumes public efforts or private efforts; it is not calibrated to deal with public-private efforts. As noted earlier, the statutory and constitutional standards that govern law enforcement do not apply to civilians unless, and until, law enforcement officers recruit a civilian to participate in reacting to a crime. Since these standards are a product of the reactive model, they deal only with the processes of investigating crimes and apprehending perpetrators. A few statutes allow specific segments of the private sector (*e.g.*, Internet Service providers and financial institutions) to share information with law enforcement, but only in the context of reacting to an identified criminal threat.[137] The same is true of statutes and common law that allow private citizens to assist law enforcement in executing a search warrant or apprehending a suspect.[138] Task forces have been operating in the United States for decades, but except for the federal initiatives noted above, they only involve law enforcement agencies.

The effort outlined above would require extensive information-sharing between law enforcement and organizations of all types, as a matter of course; the information would often not concern a specific, known threat. With prevention as its objective, the collaborative effort would collect data concerning identified threats, but it would also attempt to anticipate threats and nullify them. Gathering information pertaining to an identified threat is analogous to the process of investigating a crime. In both instances, a known eventuality sets parameters for the evidence-collection. Anticipating a threat is a less defined endeavor; it would presumably entail a comprehensive approach to information-collection, one that would allow trends and anomalies (and perhaps patterns) to be identified and tracked. How might we go about doing this? Should we eradicate the distinctions between the public and private sectors, so information flows freely between law enforcement, organizational users, architects and even individual users?

Many of us are likely to be uncomfortable with the notion of letting information flow freely between the public and private sectors, perhaps because of the influence of the reactive model. In that model, law enforcement officers gather information which is relevant to a specific event that has already occurred, a "crime;" the purpose is to apprehend the person responsible for the crime. We have therefore never had to think about the advisability of giving law enforcement prospective access to information, i.e., access to information that can be used to anticipate

137. *See* 18 U.S.C. § 2702(b)(7) (2005); *see The USA PATRIOT Act*, Pub. L. No. 107-56, § 314, 115 Stat. 271, 307 (2001).

138. *See* 18 U.S.C. § 3105 (2005) (explaining that citizens may assist with execution of search warrant); *see* Ala. Code § 13A-10-5 (2005) (explaining when citizens are required to assist officers in making arrest).

and prevent crime. Our crime models are based on crimes that have been committed and reported, if not solved. However, internalization of the reactive model is not the only reason we find it difficult to conceptualize collaborative information-sharing between law enforcement and private citizens. For most of human history, "information" was anecdotal and fleeting; we very recently acquired the ability to amass and manipulate data. Further, our ever-increasing use of technology creates vast amounts of information; nearly every transaction and nearly every interaction is documented and preserved for some period of time. Based on past practice under the reactive model, we, as citizens, assume that our transactions and interactions are private. We assume their occurrence and details will not be shared with others, especially law enforcement, absent our consent or formal authorization from a judge who issues a search warrant or subpoena. That, however, is not necessarily true; the Supreme Court has held that individuals have no constitutional right to privacy in records generated and held by third-parties, such as banks and telecommunications companies.[139] Federal statutes currently put restrictions on the dissemination of certain types of records, such as financial, educational and medical records, but since these statutes provide extra-constitutional protection, they could be revised or repealed, if we chose to do so.[140]

If we implement the preventive model outlined above, we will have to decide what, if any, boundaries we want to impose on information-sharing between law enforcement and civilians. In making this decision, we might want to differentiate between various types of information. The information in the hands of organizational users, for example, could be divided into categories. One category would comprise operational information that pertains to an organization's primary and secondary activities. An organization's primary activities are directed at discharging the functions (*e.g.*, education, product manufacture, health care) for which it was created; its secondary activities support the primary activities and include matters such as financial affairs, facilities management and computer security. A second category concerns the organization's employees; it comprises information about their job performance, address, family and benefits. Another category would consist of information about the organization's clients: a business' customers, a hospital's patients and a university's students.

139. *See Smith v. Md.*, 442 U.S. 735, 745-746 (1979); *see U.S. v. Miller*, 425 U.S. 435, 437 (1976); see *Ferguson v. City of Charleston*, 532 U.S. 67, 85-86 (2001) (holding that there is a constitutional expectation that the contents of medical records will not be shared with non-medical personnel).

140. *See* 20 U.S.C. § 1232g (2005); *see* 12 U.S.C. §§ 3401-3422 (2005); *see* 42 U.S.C. § 1320d (2005).

Because operational information is generated by and pertains to an organization, it ""belongs" to that organization; operational information can document activity by organizational employees, but they undertake that activity for the sake of the organization, not for personal reasons. Sharing this information with others, therefore, reveals what Employee A did as an agent acting on behalf of Organization X; it does not reveal information about her personal life. To say operational information "belongs" to an organization is not to suggest that it necessarily qualifies as intellectual property. Some of it may, but much of it will not. We are not concerned here with operational information's status as a legal commodity, but with an organization's ability to control its dissemination. Since this is information *about* the organization that produced it, it is reasonable to let the organization decide with whom it will be shared. The analysis is more complicated for the other two categories: Employee information implicates both the employee's relationship with the organization, and personal data having nothing to do with that relationship; the same is true for the information in the third category. It documents a client's professional relationship with an organization, but the circumstances and details of that relationship can reveal personal information about the client. The conglomerate information in these categories consequently "belongs" neither to the organization, nor to the employee/client; each has an "interest" in the information involved in and resulting from their collaboration, but neither should have the unilateral right to determine whether the information can be disseminated and, if so, with whom it can be shared. Organizations pose the most difficult problems because of the variety and complexity of the information they accumulate, but similar issues will no doubt arise for architects and individual users.

We are back to where we began: Can we implement the preventive model and still retain some limitations, that is, some restrictions on how information is used? The task would be less onerous if it only involved letting civilians share information with law enforcement; we could allow broad disclosure to law enforcement and address privacy concerns by restricting law enforcement's ability to use and to disseminate the information. But if the model is to be effective, information-sharing must be mutual; civilians must be able to share information with law enforcement and with each other. This is particularly true, as explained earlier, with regard to organizational users.

We could forego any restrictions on information-sharing. The primary constitutional guarantee of privacy is the Fourth Amendment, and, as noted earlier, the Supreme Court has held that we have no Fourth Amendment expectation of privacy in information we share with others. Unless, and until, the Court changes its views, there is no constitutional prohibition on information sharing; it might run afoul of state or federal statutes, but statutes can be revised. While this is a logical alternative, it

would be extremely unpopular, at least for the foreseeable future. Notwithstanding the Supreme Court's decisions, individuals for the most part assume that the information they share with others – personal data, transactional details – is "private" and will not be circulated outside the bounds of that interaction. Because of this, the limited information-sharing taking place between law enforcement and some members of the private sector has already generated concerns about an "unholy alliance" that is "bound to threaten human rights."[141]

These concerns are attributable to our internalization of the reactive model; we assume law enforcement seeks and gains access to information for the purpose of pursuing individuals. Given that assumption, it is reasonable to fear what some perceive as an evolving cabal among business and law enforcement; they believe law enforcement will use private sector resources to increase state control and erode our freedom. If we are to move to a preventive model, we must modify our conceptualization of law enforcement. Currently, civilians are likely to see law enforcement officers either as employees ("I pay your salary - find the guy who stole my stereo") or adversaries ("I wasn't speeding - you're picking on me"). Much of our criminal law assumes an adversarial relationship between law enforcement and civilians because it evolved to control law enforcement activity under the reactive model. We must retain that model because crimes, and cybercrimes, will still be committed; the preventive model, like the reactive model, is a crime control, not a crime eradication, strategy. Consequently, if we implement the preventive model, we will have two crime control strategies in effective: reaction and prevention. We would also, presumably, have two sets of legal constraints for law enforcement: (i) the system we have in place governing activity under the reactive model, and (ii) a new system governing activity under the preventive model. As the discussion above illustrates, it is very difficult to determine how we should design this new system of constraints; not only do we have to decide what is, and is not, permissible under the preventive model, we also have to decide how to accommodate activities that move from the preventive model into the reactive model. The Conclusion considers these issues in more detail.

3. *Architects*

Since they provide us with the tools we use to access cyberspace, the architects are in a unique position to help prevent cybercrime. The rules outlined in the next section suggest how we can impose a measure of responsibility for prevention upon the architects, who have so far avoided liability for software vulnerabilities and other defects.

---

141. *See* Michael D. Birnhack and Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment,* 8 Va. J.L. & Tech. 6 (2003).

Architects are essentially a special class of organizational users: Our software and hardware come almost exclusively from organizations. The category "architects" comprises the organizations that supply us with these products and the individuals they employ. Functionally, therefore, the architects' participation in the preventive model will be analogous to that of any other organization. Like the generic organizational users discussed above, they will work with law enforcement to share information and develop products and strategies that can be used to frustrate the efforts of cybercriminals. The primary reason for assigning architects to a distinct category is that we need special rules to recruit them into the preventive model; other issues, however, may arise as the model is implemented. The discussion of organizational users noted that discretion will be needed when organizations share information with law enforcement and with each other to prevent the disclosure of intellectual property or other proprietary information. This concern can be particularly compelling with regard to the contributions of architects.

B. WHY CRIMINAL RESPONSIBILITY?

Under the reactive model, civilians assume no responsibility for crime. Law enforcement is solely responsible for reacting to crime, and citizens are not obliged to prevent crime. Civil law has doctrines — assumption of risk and contributory negligence—that bar an injured party from seeking redress if her conduct contributed to her injury. Criminal law, on the other hand, does not require a blameless victim; a defendant cannot avoid conviction by arguing that the crime was the victim's fault. One's role in causing her victimization is irrelevant because a crime is an affront to the state, which is charged with maintaining order in its territory. Since cybercrime is not territorially-based, it represents a new type of threat to internal social order, and therefore, requires new measures, one of which is civilian responsibility for preventing cybercrime.

This discussion explores the possibility of using criminal laws to implement cybercrime prevention. Civil liability could be used for this purpose, but its effectiveness would be limited. To understand why this is true, it is helpful to consider an example: V, a home user, becomes the victim of a cybercrime because he did not take appropriate preventive measures. If we were to rely upon civil liability, we would have to devise principles that imposed a "cost" upon V, and other V's, for their security default. How could we do this? Civil liability requires a plaintiff, an injured party, who brings a civil suit for redress (usually damages) against the defendant, the offending party in the suit. Who would sue V and for what? V has been reckless or negligent, and thereby caused injury to himself in the form of compromised files or lost credit card and other information. If the cybercrime compromised V's files, the only injury is

to V; we lack an injured party who would be willing to pursue a civil suit against V to seek redress for injuries caused by V's conduct. We could let the government bring civil suits to seek punitive damages against scofflaws like V, the theory being that punitive damages are assessed as a sanction, not as redress for the infliction of specific injury.

There are two objections to this tactic. First, V may be judgment proof: He may not have assets with which to satisfy an award of punitive damages, which erodes the efficacy of the proceeding. V would be sanctioned in form but not in substance. Second, punitive damage suits brought by the government are a diluted criminal prosecution; they are brought to sanction conduct, not to remedy injury. If we decide sanctions imposed on behalf of the government are needed to institute a culture of cybercrime prevention, the preferable approach is to use criminal liability. This approach avoids the futility of seeking compensatory damages from one without the means to satisfy such an award; it also eliminates the possibility that citizens would perceive the government as hounding those who do not have the resources to defend a civil suit. Such a perception would undermine the efficacy of using civil suits to sanction those who default on their obligation to prevent cybercrime. We are accustomed to the government's prosecuting and imposing sanctions – fines and incarceration – on those who violate criminal law. We regard this conduct as appropriate, for reasons noted earlier. We are not accustomed to having it seek large damage awards from those with few, if any, resources and are apt to find the tactic unpleasant. For these and other reasons, this discussion will focus on using criminal liability to implement cybercrime prevention.

Implementing civilian responsibility for preventing cybercrime requires altering deeply embedded assumptions ("crime is the police's job, not mine") and creating new norms. We can make this voluntary or impose an obligation. A voluntary approach relies on education and encouragement in order to evolve norms that could eventually result in cybercrime prevention being regarded as the "right" thing to do. Ideally, this is the best option, since internalized standards of conduct are the most likely to be effective. However, there are at least two problems with using a voluntary approach. First, we have to un-do deeply embedded norms about crime being the exclusive province of law enforcement; second, the norm we would seek to create involves conduct in cyberspace, which is an alien environment to most people. While a voluntary approach could work, it would take a very long time to establish a norm of prevention. Given the threats cybercrime poses, it is not advisable to take this approach.

The obligatory approach requires us to act or to not-act. Laws requiring action are not suitable for instituting cybercrime prevention. To understand why, we need only consider state seat-belt laws, which re-

quire those in a vehicle to wear seat belts when it is in operation and impose fines for not doing so. They have been effective in implementing seat belt use in the United States, but our experience with them cannot be extrapolated to cybercrime prevention. For decades, the federal government has required that vehicles be equipped with seat-belts, so the obligation they impose is to use a simple, available device in public, where one's failure to comply can be observed by the police. Cybercrime prevention laws would require citizens to (i) identify and obtain the often complex tools needed to prevent cybercrime; (ii) install the tools, update them and replace them as necessary; and (iii) use them in an effective manner. These are highly demanding tasks, given that technology and the threats in cyberspace are constantly evolving. One differentiating factor, therefore, is the complexity of the duty imposed. Another is the likelihood of being caught; studies show that sanctions' effectiveness in controlling behavior is a function of the perceived risk of being caught. Cybercrime prevention targets conduct that takes place in private, for the most part; absent remote monitoring (which raises constitutional issues), it would be difficult for those charged with enforcing these laws to determine whether they were being obeyed, at least until someone became a victim of cybercrime. Another problem is that laws of this type would be inconsistent with how we approach criminal liability; we would be holding citizens criminally liable for failing to prevent crimes that never happened.

The better approach, as explained below, is to require citizens not-to-act, i.e., to create disincentives for not preventing cybercrime, and thereby develop a norm of prevention.

C. INDIVIDUAL AND ORGANIZATIONAL USERS

We can use two complementary principles to impose "costs" on those who fail to prevent cybercrime. The first principle is assumption of risk, a civil law doctrine we would modify for use in this context; the second is complicity, a criminal law doctrine we would also modify for use in this context.[142]

The civil doctrine of assumed risk bars recovery by one who knowingly exposed herself to injury. Importing this principle into criminal law would confer immunity from prosecution on those whose victims could be deemed to have assumed the risk of their victimization, and create incentives to prey on those least able to protect themselves. It would encourage cybercrime, not prevent it. A modified version of assumed risk could, however, be used to create incentives for preventing cybercrime.

142. *See* Brenner, *supra* n.12, at 94-105.

The modified, "criminal" version has two components: (1) One who uses cyberspace to engage in activity without having taken all reasonable measures to protect herself from being victimized by criminals during the course of, and with regard to, that activity, assumes the risk of any victimization resulting from it; and (2) The fact that one assumed the risk of victimization pursuant to paragraph (1) cannot be used as an affirmative defense in a prosecution for conduct involved in that victimization. The goal is to negate civilians' expectations of a law enforcement response to victimization, while retaining the ability to implement such a response. Citizens must understand that they have to protect themselves online and cannot expect an official reaction to their loss if they fail to do so. The risk of failure is on them. Once they realize this, they will begin to protect themselves by taking steps to prevent cybercrime.

Assumed risk creates a disincentive by negating the expectation that law enforcement will redress one's victimization by apprehending and sanctioning the perpetrator. The second principle creates such a disincentive by imposing criminal liability on those who fail to prevent cybercrime. One who aids and abets a crime is liable for it as if he committed it. Complicitous liability is usually based on an affirmative act, but it also applies when one has a legal duty to prevent a crime and fails to do so.[143] Currently, accomplice liability requires purposeful or knowing conduct and cannot be based on recklessness or negligence.[144] Requiring purpose or knowledge reflects two concerns: First, "lawful activities would be made perilous";[145] if negligence sufficed, I could be held liable if the car I sold was used to commit a crime. The other concern is the belief that I should not be held liable for the act of one whom I exercise no control over.[146]

Assumption of risk negates an expectation of redress for my own victimization, but what if by becoming a victim I contribute to another's victimization? Should I be liable for facilitating this consequent victimization? This is not acceptable under existing law because it (a) imposes liability in the absence of a duty to act; and (b) contravenes the concerns noted above. A modified complicity-by-omission liability can, however, be used for this purpose.

We can overcome the first hurdle by imposing a duty to avoid becoming the victim of a cybercrime.[147] The duty is to prevent my own victimization. If I protect my computer, I prevent its being used against others;

143. *See e.g.* Model Penal Code § 2.06(3)(a)(iii) (ALI 1962).

144. *See e.g.* Wayne R. LaFave, *Substantive Criminal Law* §§ 13.2(d)-(e) (West 2003).

145. Sanford H. Kadish, *Criminal Law: Reckless Complicity*, 87 J. Crim. L. & Criminology 369, 382 (1997).

146. *Id.* at 391.

147. Another option is declaring the failure to prevent a cybercrime is in itself enough to establish complicity. *See* Model Penal Code § 2.06(3)(b).

if I do not protect my computer, I create the possibility it can be used against others. If a cybercriminal exploits that possibility, it is reasonable to hold me liable for the resulting cybercrimes. We would use a negligence standard to decide if I discharged the duty; I would be liable if I did not take the precautions a reasonable person would have known were necessary to protect the system(s) at issue.[148] We would not use strict liability because it would undermine the incentive to take precautions—I would be liable for consequent victimization regardless of my efforts to avoid being victimized.[149]

This brings us to the second hurdle: We require purpose or knowledge to avoid holding individuals liable for the acts of those whom they have no control over. The liability postulated here, however, does not pose that risk. Assume X victimizes V and uses his victimization of V to victimize B. It may seem unreasonable to hold V liable for X's attacks on B. If we assume the most challenging scenario, in which V does not know X, has no control over X and was merely negligent in not preventing X's gaining access to his computer, it seems we are holding V liable for nothing more than not preventing a stranger from attacking another stranger. This may seem as unreasonable as holding a liquor store clerk liable as an accomplice if a customer to whom she sold a bottle of whiskey uses it to incapacitate a young woman whom he rapes.

The scenarios actually differ in an important respect: In the real-world scenario, the clerk is liable for the volitional and consequently unforeseeable acts of her customer based on her having sold him a product; her conduct was lawful and she has neither the right, nor the ability to control what he does after he leaves the store. In the cybercrime scenario, V is liable, not for failing to control X (which is impossible given that V does not know X and has no ability to control X's actions), but for failing to prevent equipment and processes that are within V's control from being attacked and compromised to the detriment of others. We cannot hold V liable for what X does on the theory that V should have prevented X from attacking others, but we can hold V liable for giving X access to the tools he needs to victimize others by defaulting on his legal duty to prevent his computer system from being compromised. This is consistent with traditional accomplice liability: V is held liable for contributing to the criminal venture.

If we decide this outcome is still too harsh, we can implement another modification. Rather than holding V liable as an accomplice to X's cybercrime, V could be liable for facilitating it. In some states, one who provides another with the means or opportunity to commit a crime is a

148. *See* Model Penal Code § 2.02(2)(d) (ALI 1962).

149. *See e.g.* LaFave, *supra* n. 144, at 5.5(c).

"facilitator" of that crime.[150] Facilitators are not liable for the crimes they promoted; instead, they are guilty of facilitation, a relatively minor offense.[151] Facilitation could be used for those who negligently contribute to consequent victimization; accomplice liability would be reserved for those who purposefully or knowingly further the commission of cybercrimes.

D. ARCHITECTS

When they act as individuals or as members of an organization, architects would be encompassed by the individual user and organizational user rules set out above. The question is whether they should be subject to additional rules based on their unique abilities to contribute to preventing cybercrime. Architects provide the tools users rely on to access cyberspace.; Users' ability to avoid cybercrime is a function of the reliability of the tools they have.

Cybercriminals exploit software and other vulnerabilities, so improving the tools is an essential aspect of the preventive strategy. Neither the modified assumption of risk, nor the complicity principles, would create incentives for architects to improve the products they provide. The risk of becoming a victim of cybercrime is assumed by those who use the products, not by those who provide them. Further, the complexity of software would make it impossible to hold architects liable as an accomplice to cybercrimes that exploited defects in the software they provided. In the standard outlined above, liability is based on failing to take the precautions a reasonable person would have known were necessary. This standard assumes a level of predictability in the risks and precautions to be taken; predictability, in turn, assumes experience with the product and its use. An architect facing the prospect of being held liable for a cybercriminal's exploitation of defects in software he provided could argue, quite reasonably, that he was not negligent because the defects in the software did not become apparent until it was released and used; if he was faced with liability for not remedying defects in software that had been in circulation for some time, he might argue that the failure to do so was not "negligent" because no reasonable person (no reasonable architect) could have remedied the defects given the complexity of the program and its interactions with the user and with other programs.

Instead of trying to use these principles, we should focus on the real issue: the quality of the tools being provided. We use the civil doctrine of product liability to ensure other products are of satisfactory quality, but software producers have avoided civil product liability by arguing that software is too complex to be a "product;" that is, it is misused by users

150. *See e.g.* N.Y. Penal Law §§ 115.00, 115.01, 115.05, 115.08 (2005).
151. LaFave, *supra* n. 144, at § 13.2(d).

and that applying the doctrine would chill innovation by exposing them to thousands of private lawsuits involving conflicting standards from varying jurisdictions.[152] These arguments all deal with civil product liability. What about using criminal product liability to improve our ability to prevent cybercrime?

Criminal product liability is not part of American law, presumably because we find civil suits sufficient to ensure the safety of the products we use. Software and related technologies differ from the other products we civilians use in an important respect; because of the role they play in creating and sustaining our participation in cyberspace, these technologies have become essential components of our national infrastructure. They have, in effect, ceased to be "civil" products and become something more – implements we use to maintain order and protect ourselves from external threats. This does not mean we should "nationalize" computer technologies; it means that their heightened significance for our internal and external security can justify invoking criminal liability to ensure that they meet some threshold level of adequacy.

The most reasonable way to implement criminal product liability is to define a regulatory offense based on strict liability. Strict liability is appropriate here, as it is for other regulatory offenses, because it puts the risk of failure on the architects whose conduct we want to channel in certain directions.[153] We are not addressing traditional crime, in which the State seeks redress for injury willfully inflicted upon a citizen. The premise for holding architects criminally liable is that they have inflicted systemic injury upon society by defaulting on a duty "not to act in such a way as to endanger the . . . general public."[154] The rationale for imposing criminal product liability upon architects is the same as the rationale we use for other regulatory offenses. The goal is to use criminal liability to reinforce the duty to ensure that the products one supplies do not harm the public directly or, in this instance, indirectly, by eroding the security of cyberspace.[155]

Criminal product liability responds to one of the architects' concerns by reducing the number of actions that would be brought; civil suits can be filed by any motivated plaintiff who has the filing fee, regardless of the merits of the suit. Prosecutions are brought by professionals and

152. *See e.g.* Steve Lohr, *Product Liability Suits Are New Threat to Microsoft*, N.Y. Times C2 (Oct. 6, 2003).

153. *See e.g.* LaFave, *supra* n. 144, at § 15.5(b).

154. *Id.* at § 13.5 (explaining that if an architect intentionally incorporated a defect into software so it could be exploited by cybercriminals, we could use traditional principles of criminal law – complicity, conspiracy and substantive crimes—to hold him liable for the "harm" he caused).

155. Since criminal liability is being utilized for a regulatory purpose, the penalties should be minor, probably only fines. *See e.g. id.*

must be based on probable cause to believe a crime has been committed.[156] The number of prosecutions could be further reduced by utilizing an enforcement strategy comparable to that used for environmental crimes. The Environmental Protection Agency and the Department of Justice cooperate in enforcing the criminal provisions of most federal environmental statutes.[157] The EPA investigates potential violations and can request prosecution in appropriate cases; its policy is to seek criminal sanctions only if "both significant environmental harm and culpable conduct are present."[158] The goal is to encourage self-policing and voluntary compliance.

A similar approach could be used for criminal product liability. Combining the selective use of criminal liability and an emphasis on self-policing (a) resolves the "litigation overload" objections to civil product liability; (b) resolves similar objections that would no doubt be raised to an unfiltered criminal product liability; and (c) fills the vacuum that results from relying on market forces to improve software. Prosecution authority, at the federal level, would reside with the Department of Justice. The authority to initiate prosecutions could be given to the Criminal Division or to a special unit analogous to the Antitrust or Environmental and Natural Resources Divisions.[159] Given the technical complexity of the issues, the need to use liability judiciously and for consistency in prosecutions, it would be advisable to reserve prosecution for the Criminal Division or for a special enforcement unit created for this purpose.

VIII. ADMINISTRATIVE REGULATION

Computer users who fail to adopt efficient security measures are like businesses and consumers who do not adopt basic waste disposal practices. Both fail to implement reasonable precautions against foreseeable harm and thereby contribute to harms that impose costs on others. In other words, inadequate security results in what the economists call externalities – the costs incurred by the computer user do not reflect the costs incurred by victims, other computer users and law enforcement to compensate for cybercrimes committed with that computer. If computer users had to internalize (incur) the costs reasonably necessary to prevent those crimes, computer use would be more expensive and computer us-

156. *See* American Bar Association Standards for Criminal Justice: Prosecution Function Standards 3-3.9(a).

157. *See* Rachel Glickman et al., *Environmental Crimes*, 40 Am. Crim. L. Rev. 413, 416 (2003).

158. *Id.* at 427-428.

159. *See generally* U.S. Dept. of Justice, United States Attorneys' Manual Titles 5, 7 and 9, http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title5/title5.htm, http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title7/title7.htm and http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/title9.htm (*respectively*).

age would decline. In other words, an economist would conclude that the existence of these externalities means that computer, and especially Internet, use is under-priced.

As an example, consider the internalization of the costs of crime at a brick and mortar retailer, compared to its online counterpart. One can expect a brick and mortar store to factor into its prices the costs of stock theft, employee embezzlement and other crimes, as well as the costs and recoveries of any insurance against those risks. To the extent that the store may contribute to crimes against customers or others (for example, by failing to light or patrol a parking lot), it would include in its pricing the costs of liability insurance and any tort judgments arising from such acts or omissions. The store will also indirectly incorporate the costs of the traditional law enforcement by factoring its property taxes into its pricing.

The situation will be different for a dot-com merchant selling the same items. Certainly, the dot-com will take into account in its pricing the costs of credit card fraud, transaction repudiations and theft, just as will its brick and mortar counterpart. Its prices should also include: data restoration costs from unauthorized intrusions, response costs to incidents such as denial of service attacks, and insurance premiums and liabilities to third parties from security lapses. However, given the current state of civil law, a dot-com merchant is unlikely to take into account costs to third parties resulting from unauthorized intrusions by hackers and crackers that result in identity thefts or other wrongs to customers because he or she is not likely to be liable for such losses. Nor will a rational dot-com merchant take into account the transaction and lost opportunity costs suffered by third parties, as a result of denial of service attacks, phishing and so on.

In short, a rational dot-com merchant would not factor into its prices all the effects of cybercrime. As a result, economic theory tells us that the prices charged by the merchant will not reflect the marginal cost of all resources used, there will be more purchases from the dot-com merchant than there should be and our system will be "inefficient." The same analysis would apply to individual users who do not adopt basic security precautions. They do not reflect in their purchasing and use decisions the costs incurred as a result of the abuse of their machines by criminals. Therefore, they use their computers and the Internet more than is economically efficient. To put it more bluntly, victims of cybercrimes pay expenses (their losses) that computer users should have paid.

To remedy the inefficiencies caused by these externalities, economic theory would dictate that government should impose a "tax" on persons who do not adopt efficient security measures, so that their computer use reflects the overall costs of that usage to society. "Tax", in this context, does not require a monetary assessment. (Indeed, it would appear im-

practicable to allocate the proceeds of such a tax.) Rather, the tax should take the form of other burdens that will provide an incentive to computer users to adopt efficient security measures.

The appeal of this economic analysis is undercut by the reality of any appeal to economic theory. The theory itself depends on assumptions that are not satisfied in the real world. For example, the theory assumes that all market participants have access to perfect information at no cost. The notorious insufficiency of accurate information about the frequency, nature and cost of cybercrime, therefore, indicates that neither government, nor market participants, would have the information necessary to make the precise adjustments required to eliminate externalities without the risk of over-reaction and resulting under-use of cyberspace and information technology.[160] Indeed, the "Theory of the Second Best" demonstrates that any imprecise regulatory measure may actually produce counterproductive results.[161]

Nevertheless, these academic concerns should not constrain government or the private sector to a do-nothing policy, especially because in the present context we can be confident that our information is dramatically skewed in the direction of underreporting and that the trends show that cybercrime, and its costs, are continually accelerating. These factors reduce the risk of over-regulation that would exist if the missing information could support contrary conclusions, as would be the case with the reporting of experiential data that could err in either direction.[162] We conclude, then, that an economic analysis is helpful, but neither necessary, nor sufficient, in determining an approach to distributed security. The key point, as recognized by others,[163] is that incentives are needed to push computer users and participants in Internet, and other information technology markets, to allocate additional resources to prevent third party losses from cybercrime.

---

160. This is an issue not only of the availability of raw data but also of methodologies that can be used to analyze the data. *See* Congressional Research Service, *The Economic Impact of Cyber Attacks* (Apr. 2004).

161. *See* Thomas S. Ulen, *Courts, Legislatures, and the General Theory of the Second Best In Law an Economics*, 73 Chi.-Kent L. Rev. 189 (1998) (providing a general discussion of the "Theory of the Second Best" and the competence of government institutions to make decisions regarding allocations of resources).

162. A classic example of risks of over and under reporting would be reports on UFO sightings, in light of the fact that to some, every moving light in the sky is an alien spacecraft, whereas skeptics would explain even a Martian invasion as an hallucination.

163. *Cybersecurity for the Homeland*, Report of the Activities and Findings by the Chairman and Ranking Member of the Subcommittee on Cybersecurity, Science and Research & Development of the U.S. House of Representatives Select Committee on Homeland Security, at 9, http://cryptome.org/cybersec-home.htm (Dec. 2004) (citing Aberdeen Group, *June 2003 Report on the Economic Impact of ID Theft*) [hereinafter "Cybersecurity for the Homeland"].

Once it is agreed that "taxation" in the form of government incentives is an appropriate response to cybercrime, the question arises as to the appropriate level of government that should implement such a system. In our view, adoption of an administrative system of such "taxation" complements well the adoption of a system of distributed security enforced by criminal sanctions. The system must be administrative because computer security is too nuanced and too ephemeral to allow effective legislative regulation. Instead, government should employ an approach similar to that adopted for other common externalities, most notably environmental pollution. That model enhances basic criminal sanctions with permitting/licensing and reporting requirements, that are enforced by state and federal agencies with appropriate expertise. Because computer security so directly affects interstate commerce, the appropriate level for administrative regulation is the federal government.

Even with the shorter response time of administrative agencies, compliance with the rulemaking procedures mandated by the Administrative Procedures Act will preclude the agency from responding on a timely basis to the continued and accelerated changes to technology and to cyber-criminal methods and techniques. Therefore, government must use more blunt tools to address the externalities of inadequate security. The sections below outline some tools that could be used for this purpose.

A. INDIVIDUALS AND SMALL ORGANIZATIONS

Excluding certain crimes related to infringement of intellectual property rights,[164] the cybercrime externalities created by individual users and small organizations primarily arise from their access to the Internet. Government cannot expect individuals, small businesses, nonprofit organizations and similar users to monitor developments in computer security, or to maintain the precautions reasonably necessary to deter and detect cybercrime, because the transaction costs of doing so far outweigh the direct benefits of doing so and even, under present tort law, the risk of liability to third parties. Those transaction costs are subject to economies of scale, however, so that the externalities might be efficiently redressed by denying consumers and small organizations access to the Internet, except through licensed Internet service providers ("ISP"s) that are required to provide such protection to the consumers. Stated differently, government could require, by legislation, that it is unlawful for any intermediary to offer its services to the public unless it has obtained governmental authority to do so. Because those intermediaries

164. The most notorious criminal violations of intellectual property laws may be downloading of bootlegged music, videos and software. Nevertheless, violations of such laws also occur through the copying of protected materials and the transfer by means not using the Internet, for example, by copying of compact discs.

can take advantage of scale economies in identifying and remedying security risks, the externalities can be eliminated at a lower overall cost.

Intermediaries could offer varying levels of security; some could provide merely a secure gateway into cyberspace, while others might offer a controlled online environment with filtered content and other protections. Intermediary functions could be provided by various entities: commercial, organizational or governmental. I could subscribe to a "mere" ISP that provides only access, to America Online ("AOL") or other access-content providers, or I might use portal services provided by my employer as an employee benefit. Governments could provide portal services, but their doing so would to some extent defeat the purpose of the preventive model, which is to reallocate much of the responsibility for securing cyberspace to citizens. The better approach would be for government to encourage the development of private sector portals as an alternative to individual user responsibility.

Licensing of ISPs and limiting consumer access except through such licensed gateways may seem like an unprecedented and drastic step. Licensing, however, is hardly an unprecedented means of addressing externalities. Instead, it is a relatively low cost method of reducing externalities in industries as basic as banking and insurance and as marginal as massage parlors and tattoo artists. Nor is licensing an overly Draconian method of regulation that would inappropriately restrict consumer freedom. While licensing does increase the costs of entry and operation, we have learned to live with limited consumer choice in many basic industries without disastrous affects on consumer satisfaction. One need only point to the histories of the automobile and airline industries, where increases in concentration have not prevented vigorous competition or innovation. Even if the number of ISPs drastically decreases, it will only reflect the fact that external costs of under-security are being eliminated. Individual users and organizations of less than a certain size would still have a choice: To paraphrase Henry Ford, "You can get on the Internet any way you want, as long as it is through a licensed intermediary."

The primary benefit of limiting the gateway to the arena where cybercrime flourishes is that government will reduce its enforcement burden by many magnitudes. Limited access will also permit government to set more precise standards than would be possible in legislating/regulating for individual and unsophisticated organizational users. Additionally, collaborative approaches are more feasible when government is dealing with a smaller number of sophisticated licensees. Finally, reducing the enforcement burden and shifting security conformance to sophisticated entities will permit more timely responses to new criminal methods.

Of course, shifting the burden for security to ISPs is neither free nor simple. The "not free" part should not be an issue as long as the costs associated with the regime do not exceed the current losses and wasted resources resulting from inadequate security at the user level. As discussed above, we seem to be a long way from that limit. For example, according to some sources, by June 2003 over $222 billion in losses were sustained by the global economy.[165] Even if such an estimate is grossly over-inflated, the total possible costs of cybercrime readily justify the expenditures contemplated here.

As to the "not simple" part, there are several responses. First, ISPs are already providing security services to their subscribers, such as spam and virus filters and personal firewalls.[166] Second, it would not be necessary or advisable for the regulator to dictate a single means of compliance, especially since accepted industry standard security measures do not exist at the present time.[167] Instead, the practical difficulties of implementing such a proposal could be addressed through different structures. One might be to require the ISP to automatically download to its subscribers' computers appropriate security programs in the same way that Microsoft Windows and other popular software programs "push" patches and updates by allowing the consumer to choose to have updates automatically downloaded. Another structure might be similar to that of a typical corporate network, with the ISP taking on the role of the network administrator and individual subscribers in the position of individual workstations in the network. In this structure, the ISP would be responsible for establishing firewalls, unauthorized detection programs, spam filters and other security systems between the subscriber and the Internet. The ISP would also be responsible for limiting and controlling access from the subscriber's computer to other IP addresses, just as corporate administrators regulate external connections and attempted downloads. Individual subscribers might be allowed to override those restrictions, but only by discrete selection and perhaps by paying a higher subscription rate or demonstrating proof of liability insurance, as discussed below. For the vast majority of consumer users, these measures would not restrict their Internet access at all. For those whose use is restricted, it would simply be a matter of paying for the privilege of uses that increase the risk of cybercrime.

---

165. *See* Cybersecurity for the Homeland, *supra* n. 163, at 8.

166. America On-Line has adopted an aggressive marketing campaign on that basis to differentiate itself from smaller ISPs that apparently cannot afford or do not have the technical capacity to provide such services. *See e.g.* AOL, Inc., *Safety & Security*, http://discover.aol.com/optimized/safetyandsecurity.adp (accessed Dec. 17, 2005).

167. *See* National Cyber Security Partnership, *Technical Standards and Common Criteria Task Force, Recommendations Report*, A-4, A-5, A-6, http://www.cyberpartnership.org/TF4TechReport.pdf (Apr. 2004).

It is likely that a substantial portion of the ISP community would object to such licensing as an anti-competitive measure and as an unfair burden. Licensing will create barriers to entry that will increase concentration in the intermediary market(s), thereby artificially increasing the costs of Internet access and usage beyond that needed to eliminate the cybercrime externality.[168] Also, any licensing scheme requires additional capital and expertise, even if it does not include specific capitalization requirements. However, the situation here would not seem to differ materially from that involved in regulation of financial services or other commonly licensed industries. Indeed, such concentration can be viewed as a positive outcome because the resulting profits can be used for research and development, industry collaboration and other socially responsible activities.[169]

Similarly, although licensing regulation would impose a burden on ISPs, it is not unfair because it is universally applied and is intended to be passed on to the consumer. Indeed, the statute authorizing the license could even require ISPs to include "access fee" that would be used by the ISP to meet licensing requirements. Under such a system, ISPs could be provided with an incentive to meet licensing requirements at the lowest possible cost, thereby enabling them to retain the unexpended access fees. In this regard, the regulation is similar to the sales tax, which, although it depresses demand for the taxed goods, is not perceived as unfair to sellers because it is universally applied and required to be passed on.

In addition to the objections of potentially regulated intermediaries, there are likely to be two primary public policy objections to the notion of intermediary licensing.[170] The first objection is that concentration will chill innovation, including innovation in security measures, thereby potentially providing criminals with the upper hand in technological developments. There is some truth in this criticism. We can, however, look again to the heavily regulated financial services industry to determine that licensing does not materially chill innovation. There (or "In that industry"), we see a healthy industry of consultants and vendors who develop products for sale or licensing to the licensed entities. The reduction in innovation should not exceed acceptable levels as long as (i) sufficient competition remains in the intermediary market, or (ii) regulators

168. *See* U.S. Department of Justice, Bureau of Justice Statistics Technical Report, *Cybercrime Against Businesses*, at 2, http://www.ojp.usdoj.gov/bjs/pub/pdf/cb.pdf (Mar. 2004) (explaining there were 9,511 ISPs in the United States in 2001).

169. *See generally* John Kenneth Galbraith, *The New Industrial State* (3d ed., Houghton Mifflin Company 1978).

170. We do not consider here objections based on the refusal to recognize that inadequate security is an externality such that taxation is not appropriate.

retain the authority and expertise to require licensees to adopt new technologies and products.

The second objection, and potentially the most troublesome to the public, will be the perception that restrictions on use or access will constitute invasions of privacy. For example, if an ISP limits access to certain pornographic sites based on information that the sites are used to recruit robots for cybercrimes, subscribers who nevertheless desire access, might have to request and pay for such access. We see this restriction as no more troublesome than the risk of being seen parking in front of an adult video store – eliminating a capability that has existed for less than a decade is not a matter of interfering with a fundamental right. Even if it were, we believe that the gain to protection of inherently private information, as a result of a system of distributed security, far outweighs any loss of privacy as a result of indirect limitations on Internet access and surfing.

B. Larger organizations

Another potential tool to distribute responsibility for cybercrime prevention, and thereby eliminate the current externalities, would be to more stringently regulate organizations that operate enough computers connected to the Internet or that maintain sufficient collections of data to present a significantly greater risk to other Internet users and to the infrastructure. Such regulation would establish minimal standard security measures, to which these larger "institutional" organizations would have to conform. It would not be necessary, however, to require certificates of authority, or otherwise license such institutional organizations in the manner common for utilities, barbers and trucking companies. Rather, it would be sufficient, at least as an initial step, to merely require the organization to certify its compliance with *basic* standards set by the government and to report on unauthorized intrusions, denial of service attacks and other significant events.

There is ample precedent for this approach. A common method of enforcement of statutory and administrative requirements is to require those subject to the requirements to file reports showing compliance and/or providing data necessary to permit the enforcement agency to determine compliance. Some examples include an employer reporting on withholding of employee taxes, bank call reports, and various Department of Commerce reporting requirements on economic activity. It is also common to subject such reporting to audit or inspection. Occupational Safety and Health Administration ("OSHA") regulation and labor and employment information are obvious examples. In short, many models exist on which to base regulation that would require institutional organizations to certify that they have installed and maintain firewalls

and detection systems with certain characteristics, and to report on the number and nature of unauthorized intrusions. These are, of course, just examples of the many types of standards and reporting requirements that could be imposed.

Adoption of security requirements need not await development of a consensus as to universal industry standards or detailed cyber-security specifications. Undue precision would both delay implementation and chill innovation. Instead, what will be needed is strong leadership in both government and private sectors to develop standards that incorporate substantial room for flexibility and innovation. Perhaps, more importantly, administrative enforcement must incorporate substantial prosecutorial discretion based on technical competence.

For example, any system of standards adopted by the government must provide for distinctions based on size and exposure so that compliance and reporting requirements are reasonably tailored to the nature and magnitude of the risk presented. For example, government could impose a higher set of standards on Web sites that receive over a million hits per month, or that operate databases with data on more than 1,000 people. Distinctions could also be made on the basis of the type of information processed, so that Web sites dealing in sensitive medical or financial information would be subject to more stringent standards than those dealing in cosmetics or baseball cards.

Compliance with basic security standards is not enough, however. Because corporate managers now have a disincentive to report cybercrime either internally or externally,[171] it is important that any regulatory regime demand accurate and timely reporting of cybercrime incidences and its severity. One approach would be to follow the Sarbanes-Oxley Act that created particular requirements for publicly held companies. The regulator could require chief executive officers and outside auditors to certify that due investigation had been made as to the existence, amount and cause of losses from cybercrimes, and that such facts had been timely and completely reported to executive management and all applicable law enforcement agencies and disclosed on financial statements.[172] Only by imposing such a duty to disclose on management and external auditors, can we ever hope to obtain the data necessary to prevent cybercrime effectively. Again, the argument can be made that the mandated disclosure requirement is not universal, limited as it is to publicly held companies. From the perspective of deterrence of cyber-

171. *See* Cybersecurity for the Homeland, *supra* n. 163, at 9.

172. Imposing a reporting requirement on auditors is especially important in light of anecdotal evidence that companies have made extortion payments and written off theft and fraud losses without specifically tying those events to cybercrimes.

crime, however, the distinction is immaterial because the vast majority of assets at risk are held or controlled by publicly traded companies.

Of course, Web sites are not the only prey of cybercriminals. Large and small networks are also a popular venue for cybercrime. Thus, a system of distributed security regulation could also require certification and reporting by organizations pertaining to security measures protecting their corporate networks and stand-alone computers that are connected to the world outside. Regulation of this aspect of security can be refined to the same extent as Web site security. This is not to deny the unique issues that must be addressed; rather we move on solely for the sake of brevity.

C. IT Products

Regulation of users and intermediaries will not be efficient if they do not have the tools to accomplish the tasks given them. Therefore, it will also be necessary to provide incentives to architects to make hardware and software more security friendly. This is treacherous territory for regulators since the impact on product development and technological innovation from ill-advised regulation could be disastrous, not only from the viewpoint of the economy as a whole, but also from the viewpoint of cybercrime deterrence. Instead, what is needed here is not substantive regulation, but transparency. For example, product makers should be required to disclose, in marketing materials and in product documentation, appropriate information regarding security recommendations, configuration checklists, and best practices. Additional initiatives could address the need for better product analysis and standardization procedures.

D. Mandatory insurance

Another possible means of enforcing a system of distributed security, and of providing restitution to persons harmed by cybercrime, would be to require Web site owners and owners of computer networks exceeding a minimum size (say ten computers), to maintain insurance against the risk that the Web site or network would be victimized by a cybercrime. It may strike the reader as nonsensical that a computer owner should be required to purchase insurance against the risk that he will be victimized by a cybercriminal. However, it is the use of the computer that enhances the risk of the cybercrime, and the crime harms not merely the computer owner, but also those who have entrusted data to the owner and those who are injured by the cybercriminal's ability to control the computer. Thus, this is not a situation of making the victim pay for the crime, but rather is a method of increasing the likelihood that all those

hurt by the crime are protected from the negligence of one whose property is used as a means of committing the crime.

Requiring insurance for specified risks is a common feature of regulatory regimes in this country. Requirements that regulated entities maintain liability insurance are found in regulatory systems affecting businesses as diverse as insurance agencies, taxicabs, telecommunications, trucking and banking. There are two distinct purposes of these insurance requirements. The first is to provide a fund to satisfy claims from persons injured by the regulated entity, and the second is to reduce the frequency and severity of injuries by using the independent underwriting and risk management expertise of the insurers to cause the regulated/insured entity to adopt prudent risk management policies and procedures. For example, property and casualty insurers frequently inspect their insureds' premises and use underwriting policies and premium pricing to influence their insureds, to adopt better risk management techniques. Such byplay between insurers and insureds has a major impact on compliance with fire codes, OSHA regulations and similar guidelines.

This second aspect of mandatory insurance is of primary significance in a system of distributed responsibility for computer security. We do not suggest that government delegate to private insurers either the authority to set standards, or the power to enforce those standards. However, the combination of government standards and insurer self-interest could provide an acceptable surrogate to direct government enforcement of standards, at a fraction of the cost. This approach has now been widely accepted with respect to mandatory automobile liability insurance. Obviously, there are key distinctions between the risks presented by uninsured motorists and uninsured computer users, but those distinctions relate to the nature and severity of the risk, not to the existence of the risk or nexus between the activity and the risk.

One issue that must be addressed before an insurance requirement is imposed, however, is the amount of insurance that should be required. It is not necessary or desirable that the required limits be sufficient to compensate all possible victims of crimes committed using that computer.[173] A hacker who creates a robot network that attacks Web sites or networks may cause damages in the millions of dollars for data restoration costs, lost revenues and harm for disclosure of confidential information. It would neither be just, nor efficient, to impose a system of even

173. Indeed, at the present time, limits of liability under policies offered by even the largest insurance companies are much less than potential exposures. For example, AIG eBusiness Risk Solutions, a subsidiary of the largest insurer in the world, typically limits its exposure to $25 million. *See* The AIG eBusiness Risk Solutions, *The AIG netAdvantage Suite, Coverage Highlights*, http://www.aignetadvantage.com/content/netad/Coverage.pdf (accessed Dec. 17, 2005).

proportionate liability, much less joint and several liability, on the owners of those captured robots. Moreover, the purpose of our proposed criminal/administrative approach to computer security is primarily prevention, not restitution. Thus, the limits should be enough to pay just the criminal fines that might be imposed. The need for higher limits to protect the interests of those with contract or tort claims is beyond the scope of this article. We leave those very different issues to those concerned with compensating victims of cybercrime.

Perhaps the strongest practical objection to this proposal would be that the insurance markets for information technology coverage are thin and immature. This criticism is accurate,[174] but the adoption of this proposal would help solve that problem. Interestingly, segments of the insurance industry have attempted to market information technology security policies since the late 1990s. Sales, however, have been hampered by a lack of perceived need, and underwriting (and therefore pricing) has been perhaps unduly conservative because of the lack of readily available information related to risk. A program of distributed security would provide both the information, and the impetus, to satisfy stewards of organizational resources that insurance is as prudent for information security as it is for fire and theft risks, and it would enable insurers to evaluate risk more accurately and competitively.

It must be admitted, however, that more information will not eliminate the shortage of insurance markets. What should be considered, therefore, is a government reinsurance risk pool that would provide the temporary liquidity to cover losses beyond the retentions of individual insurers, with the government pool recouping those losses out of assessments on future premiums. A detailed explanation of this topic is beyond the scope of this article, but we can find precedents in federal deposit insurance and the Terrorism Risk Insurance Act. The deposit insurance model is an appropriate remedy since for many years, premiums were assessed without regard to risk, and even now, the risk adjusted premiums do not purport to be actuarily accurate assessments. Instead, the government's role as an insurer of last resort has been based on the notion that it is required by the importance of the banking and payments systems to the economy and the nation's interest. Certainly, cybercrime presents a comparable risk.

On a related front, proof of adequate insurance could justify lesser regulation of ISPs as gateways to the Internet for organizational users that have adopted extensive security measures due to independent regu-

174. There are less than two dozen insurers that now write coverage expressly addressing cyber risks. *See* Richard S. Betterley, *Cyberrisk Market Survey 2004: Continuing Innovation, and Growth Opportunities Galore* at 1, www.betterley.com/adobe/CyberRisk04_nt.pdf (June 2004) (stating that ten carriers represent the "core of the Cyberrisk market").

lation of their networks. Just as we have more lenient regulation of "wholesale" banks who deal only with sophisticated customers, and of securities issuers who sell only to accredited investors, we could have a less regulated class of ISPs who deal only with customers who certify that they meet specific security standards and who have insurance to back up that certification. In other words, a "wholesale" ISP would be relieved of the full panoply of security devices required of a consumer-level ISP, as long as all its customers certified their compliance with the standards required of the ISP. This approach might offer the additional benefit of providing for market differentiation, so that organizations with leading edge security performance could avoid the costs of unnecessary regulation.

IX. CONCLUSION

The notion of preventing cybercrime is not new: In February of 2003 the White House released *The National Strategy to Secure Cyberspace.*[175] The *National Strategy* called for civilian participation in (i) preventing cybercrime, (ii) reducing our vulnerability to cybercrime and (iii) minimizing the damage from successful cybercrimes.[176] It relied upon a purely voluntary approach; citizens were "encouraged," but not required, to participate in this effort.[177] Many were critical of this approach from the outset; one report, for example, criticized the *National Strategy* because it "relies on private sector willingness to take certain security measures and bear their costs, and chooses not to use government's power to legislate, regulate or otherwise require certain actions."[178] James Lewis, director of the CSIS Council on Technology and Public Policy agreed, noting that "[c]ybersecurity is too tough a problem for a solely voluntary approach to fix. . . . Companies will only change their behavior when there are . . . market forces and legislation that cover security failures."[179]

---

175. *See generally The National Strategy to Secure Cyberspace*, *supra* n. 90, at 13-15.

176. *See id.* at 1-10.

177. *See id.* at 13.

178. Dan Verton, *Gilmore Commission Critical of Bush Cybersecurity Plan* ComputerWorld ¶ 2-3, http://www.Computerworld.com/securitytopics/security/story/0,10801, 76827,00.html (Dec. 17, 2002); (quoting report issued by the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, which commented on a draft of the later-released *National Strategy*); *see also id.* at ¶ 7 (stating "'The government . . . has failed to exercise any of its powers other than persuasion . . . . As a result, there has been no change in the significant market disincentives to the adoption of cybersecurity measures necessary for ensuring the viability of critical functions performed by the information infrastructure . . .'").

179. Robert Lemos, *Government Unveils Cybersecurity Plan* CNET News, http://news.com.com/2100-1023-956353.html (Sept. 18, 2002).

It has been, at this writing, two years since the *National Strategy* was released. It has had absolutely no effect on the behavior of individual or organizational users of cyberspace; it has done nothing to prevent cybercrime.[180]

We believe that preventing cybercrime, with some degree of efficacy, *is* an achievable goal. We believe the flaw in the *National Strategy to Secure Cyberspace* was, as noted above, its failure to use the power of government to create incentives to secure systems, and otherwise prevent cybercrime. We believe a purely voluntary system is doomed to fail for the foreseeable future because achieving cybercrime prevention requires altering our basic assumptions about who bears responsibility for "crime," in all its forms. In the twenty-first century, citizens assume law enforcement deals with "crime;" we do not see it as our responsibility. The only way we, as a society, can alter this assumption and achieve an effective cybercrime prevention strategy, is to utilize the power of government; and as we explain above, the judicious use of criminal sanctions and administrative regulation is an effective way to impose and enforce a responsibility to prevent cybercrime.

---

180. *See e.g.* The Mercury News, *American Cyberspace: Waiting for Its Sept. 11,* San Jose Mercury News Editorial 8B (Dec. 9, 2004) *available at* 2004 WL 102142795 (stating: "[T]he Bush administration's cybersecurity plan was never terribly ambitious. The National Strategy to Secure Cyberspace was a watered-down document, the product of endless compromise. It . . . relied on voluntary measures and good will, rather than modest and sensible regulation . . . . [N]early two years after it was unveiled, the plan has amounted to pretty much nothing"); *see also* Bob Keefe, *More than Ever, Internet's an Unsafe Place,* Austin American-Statesman Business (Dec. 5, 2004) *available at* 2004 WL 57669711 (noting that little, if anything, has been done to implement the *National Strategy,* and that it has, therefore, had no effect).