Harvard Journal of Law & Technology
Volume 11, Number 3 Summer 1998

PRIVATE INTRUSION RESPONSE

Stevan D. Mitchell[*]
Elizabeth A. Banker[**]

TABLE OF CONTENTS

---

* Trial Attorney, U.S. Department of Justice, Computer Crime and Intellectual Property Section; Former Member, President's Commission on Critical Infrastructure Protection. J.D., 1989, Florida State University College of Law.

** Associate, Steptoe & Johnson LLP, Washington, D.C.; Former Assistant General Counsel, President's Commission on Critical Infrastructure Protection. J.D., 1996, summa cum laude, Catholic University of America, Columbus School of Law; M.A., 1996, Catholic University of America, School of Philosophy.

The views expressed here are those of the authors and do not necessarily reflect those of the President's Commission on Critical Infrastructure Protection or the U.S. Department of Justice.

I. INTRODUCTION

Law enforcement is improving its ability to respond to and deter computer-based intrusions. A private response is developing on a parallel track, in ways that may be more responsive than current government efforts to the private sector's need for confidentiality and control over sensitive investigations. The private response is taking shape in an environment where liability and standards of conduct are largely undefined. The simultaneous growth of divergent governmental and private responses hinders the nation's ability to estimate the size and scope of the threat of computer intrusions, share information about vulnerabilities, and lay a foundation for an effective threat warning capability. A professional licensing scheme for certain classes of computer security specialists may provide a basis for compromise, cooperation, and enhanced deterrence.

Misuse of computer systems appears to be the modus operandi of an increasingly broad spectrum of actors, including those without authorization to enter a system and those who exceed their valid authorization. They range from recreational hackers seeking a challenge, to disgruntled employees out for revenge, to those pursuing financial gain through theft of trade secrets and proprietary data, and even terrorists or nation-states seeking to further foreign policy or

military objectives. Protecting vulnerable systems is increasingly vital given our increasing dependence on them for information, communication, and commerce. As a result, we are beginning to see dramatic changes within the computer security industry and in the mechanisms put in place by governments to provide responses to computer misconduct. But as both the frequency and reporting of incidents increase, the resources made available to prevent, investigate,[1] and respond to the consequences of incidents — particularly those incursions that appear to originate from external sources — will become increasingly taxed.

The most visible responsive resources currently reside within the federal law enforcement community. A federal governmental response has developed for a number of reasons. Geographic dispersal of networks and the need to investigate incidents that cross state boundaries implicate federal jurisdiction. The expense of training, equipment, and conducting computer investigations often price computer crime expertise out of the range of state and local police resources.[2]

The federal government has begun to equip itself to address an expected increase in the volume of computer intrusions,[3] raising basic

---

1. This paper explores ways to supplement investigative capabilities. Private investigators may be both an alternative and a supplement to traditional law enforcement responses to computer crime. In some cases, companies may opt to use a private method to resolve an intrusion problem instead of pursuing criminal remedies. In other instances, a criminal remedy may be unavailable for practical reasons, requiring a private response capability to supplement law enforcement. In still others, private services may be used at the preliminary stages of an investigation to gather evidence for subsequent legal action. We recognize, of course, that enhanced investigative capabilities ideally should be coupled with enhanced opportunities for prosecution, either through the civil or criminal law.

2. *See Security in Cyberspace: Hearings Before the Senate Comm. on Governmental Affairs, Permanent Subcomm. on Investigations*, 104th Cong. 73-74 (1996) [hereinafter *Security in Cyberspace Hearings*] (statement of Minority Staff discussing the reluctance of local law enforcement to develop computer-related expertise, due at least in part to the required technical expertise and need for special training and equipment, and noting the dependence on federal law enforcement created by the lack of a local response capability).

3. Reliable statistics remain elusive owing to definitional ambiguities, methodological inconsistencies, and limited reporting. Investigators have conveyed anecdotally their sense that the volume of potentially criminal incidents is increasing. See, e.g., Sharon Walsh & Robert O'Harrow Jr., Trying to Keep a Lock on Company Secrets, WASH. POST, Feb. 17, 1998, at D1 (comments of FBI Section Chief William Perez). Attorney General Janet Reno recently requested $64 million in increased funding to "expand efforts to protect the nation's critical infrastructures from cyber-attacks and to combat cybercrime." *Hearings Before the Subcomm. on Commerce, Justice, and State of the House Comm. on Appropriations*, 105th Cong. 16 (1998)

questions about the ability of federal law enforcement to effectively and efficiently resolve large numbers of incidents. Even assuming the availability of adequate resources — an assumption we question — not all cases brought to the attention of law enforcement will be investigated.[4] Still others may not be prosecuted.[5] In addition, the response typically pursued by law enforcement is geared toward identifying, apprehending, and prosecuting the intruder. Such a response is clearly a critical element in deterring such activity, but is not necessarily consistent with the business objectives of a corporation that has been the victim of a serious incident.

Businesses have a primary need to repair damage and restore service to customers, a process often complicated by an ongoing criminal investigation. While some businesses may also be interested in pursuing criminal prosecution, other business considerations, such as the need to control costs and maintain customer confidence in the reliability of service and in the security and confidentiality of transactions and records, may militate against initiating a public response. The result to date has been a low rate of reporting intrusion incidents to law enforcement.[6]

(statement of Attorney General Janet Reno). Most of the funding is intended to support 75 new FBI agents and 24 new federal prosecutors to track down and prosecute computer criminals. *See id.*

4. For example, some violations of the Computer Fraud and Abuse Act are misdemeanors, and law enforcement officers overwhelmingly prefer to dedicate resources to the investigation of more serious felonies. *See* 18 U.S.C.A. § 1030(c)(2)(A) (West Supp. 1998) (enumerating punishment under §§ 1030(a)(2), (a)(3), (a)(5)(C), and (a)(6) as a fine or imprisonment for not more than one year, or both).

5. On November 21, 1997, Mathew Bevan, a.k.a. "Kuji," one of two then teen-aged hackers responsible for the celebrated Rome Labs intrusion incident, was freed after London prosecutors declined to go forward with the prosecution. The decision not to go forward appeared to be based on the cost of trying the case and the uncertainty of prevailing due to evidentiary problems. See Duncan Campbell, More Naked Gun Than Top Gun, GUARDIAN, Nov. 27, 1997; Stephen Farrell, Hacker Who Broke into NASA Walks Free, TIMES (London), Nov. 22, 1997.

6. Predominant reasons given by security experts and survey respondents for non-reporting consistently include fear of negative publicity, fear of competitors using information to their advantage, and loss of productivity. *See, e.g.*, Computer Security Institute, 1997 CSI/FBI Computer Crime and Security Survey (1997) (unpublished report on file with *Harvard Journal of Law & Technology*); see also Computer Security Institute, Annual Cost of Computer Crime Rises Alarmingly: Organizations Report $136 Million in Losses (Mar. 4, 1998) (press release on file with *Harvard Journal of Law & Technology*);WarRoom Research, LLC, 1996 Information Systems Security Survey (1996), *available at* <http://www.warroomresearch.com/wrr/SurveysStudies/1996ISS_Survey_SummaryResults.htm>. Such fears may not be unjustified. After Citibank received publicity for the 1995 intrusion into its system, six of its competiors

Whether viewed as alternatives to the traditional criminal law enforcement response or as supplements to such a response, there is are several existing and emerging avenues for responding to intrusion activity. Statutory civil remedies are in place at the state and federal levels, though they are seldom pursued.[7] Contract and tort remedies have been proposed as potential vehicles for settling disputes between private parties for unauthorized use of systems.[8] However, all of these alternatives are dependent on identifying the source of the intrusion — identification that must be sought through an investigatory process. Identifying the source of an unauthorized intrusion can be costly and time-consuming, causing businesses carefully to weigh the respective benefits of initiating a public response, a private response, or no response at all.

Due to the sensitive nature of the work performed by security firms and their customers' desire for confidentiality, there are few published discussions of the services related to tracking the sources of intrusions. Many of our insights were gained through confidential interviews with members of the security community. Many similar conclusions were drawn as an outcome of the 1996 Security in Cyberspace Hearings.[9] In addition, our observations receive anecdotal support from advertisements for computer security services available on the Internet.

Richer options are becoming available. Some computer security experts have begun to provide services to clients that can ensure

---

targeted the bank's top 20 customers, claiming their systems were more secure than Citibank's. *See Security in Cyberspace Hearings* (statement of Minority Staff), *supra* note 2, at 34–35.

7. *See infra* notes 28–29 and accompanying text.

8. *See, e.g.*, Anne W. Branscomb, *Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime*, 16 RUTGERS COMPUTER & TECH. L.J. 1, 57 (1990) (considering as alternatives strict liability for service and software providers, compulsory insurance coverage, and establishment of higher ethical values); Michael P. Dierks, *Computer Network Abuse*, 6 HARV. J.L. & TECH. 307, 337–39 (1993) (proposing greater emphasis on prevention through regulation or tax incentives for greater computer security); Robert L. Dunne, *Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace Through a Contract Law Paradigm*, 35 JURIMETRICS J. 1 (1994) (examining the advantages of using contract law to address unauthorized access to computers); David L. Gripman, Comment, The Doors Are Locked but the Thieves and Vandals Are Still Getting in: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem, 16 J. MARSHALL J. COMPUTER & INFO. L. 167, 172 (1997) (proposing that courts should impose on corporations a duty to have adequate computer network security to prevent intrusions that can damage the corporation or third parties).

9. *See generally, Security in Cyberspace Hearings* (statement of Minority Staff), *supra* note 2.

confidentiality and control over their systems, while providing the necessary security measures and intrusion detection and response capabilities. Given the sensitive nature of the work involved in provision of computer security services, and the legal complexities of conducting private investigations into intrusion incidents, the potential benefits of creating an oversight mechanism for computer security experts engaged in such activities seem compelling. In addition, a licensing scheme could be administered in such a way as to provide mutual benefits to private security experts, government, and owners of compromised systems.

Computer security practitioners could benefit from working within the parameters of a more clearly defined legal and liability climate and from the marketing advantages that a license may afford, including enhanced public trust. The government could benefit from receiving limited information about incidents that are currently investigated and resolved without its knowledge. System owners could benefit by having available a broader array of intrusion response options. The public could benefit from having more of these sensitive operations performed by licensed professionals. Several security practitioners agree that merely raising the prospect of such an approach would contribute in important ways to awareness of the problem and would begin an important public policy dialogue.

Given current uncertainty over the size and scope of the future threat,[10] and of the ability of technological solutions and existing

---

10. Several sources offer statistics on the current scope and projections of the future growth of the computer misconduct problem. However, the divergence of the results of these surveys and the methodological pitfalls associated with them limit their utility. See, M.E. Kabay, ISCA White Paper on Computer Crime Statistics (visited Apr. 8, 1998) <http://www.ncsa.com/knowledge/research/comp_crime.htm> ("Given these problems of ascertainment, computer crime statistics should generally be treated with scepticism."). One obvious problem with statistics that attempt to measure the frequency and costs of computer intrusions is that many — though no one can really know how many — go undetected. We have used, for purposes of discussion, the assumption that roughly 1 in 10 successful intrusions is detected, and of those, roughly 1 in 10 is reported to law enforcement. At least one published source agrees with this estimate, although some security professionals have referred to it as optimistic. *See id.*

Losses from individual intrusion incidents also vary considerably depending on the nature of the intrusion and the intention of the intruder. Most figures place the average loss in the neighborhood of $40,000 per successful external intrusion, but the consequential damages associated with such an attack have gone as high as $10 million. *See* WarRoom Research, *supra* note 6; David Bernstein, *Industry Survey*, INFOSECURITY NEWS, May 1997, at 20; Reuters, *Sabotage Suspect Charged*, CNET NEWS.COM (Feb. 18, 1998)<http://www.news.com/News/Item/0,4,19245,00.html>; *see generally Security in Cyberspace Hearings*, *supra* note 2.

government structures to provide an adequate response, further consideration of the idea seems warranted. Vehicles to provide effective forms of public and private response are becoming increasingly entrenched and institutionalized. It may now be an opportune time to consider the extent to which limited and carefully defined cooperation may be mutually beneficial. We have produced this article to provide a perspective on the disadvantages of increasingly uncoordinated and potentially inadequate means of response, and to encourage further exploration of the range of available and emerging options.

II. CONVERGENT TRENDS, DIVERGING RESPONSES

It is unclear to what extent routine computer-based intrusions will proliferate. It is similarly unclear to what extent traditional forms of governmental response will be adequate to address and deter this behavior. It is not necessary, however, to project accurately huge growth in these areas in order to begin thinking about next steps. Technology will continue to provide more effective ways of not only preventing, but also detecting unauthorized intrusions and unauthorized use. Reluctance to report anomalous activity may decrease as events become more commonplace. These trends will place a progressively greater burden on a growing federal law enforcement response. While alternative and effective forms of response are developing within the private sector, developments are taking place under conditions that make it difficult for the government adequately to assess the scope of the problem or to develop a predictive threat-warning capability. Perhaps there is a way for private experts to function in a way that also advances important societal and governmental interests.

As long as firm data on the numbers of intrusion incidents that occur are unavailable, it will be almost impossible to determine accurately the scope and magnitude of the computer misconduct problem. This will hamper not only law enforcement efforts to build an adequate response capability, but also the development of national policies to protect our information infrastructure. *See Security in Cyberspace Hearings* (statement of Minority Staff), *supra* note 2, at 37.

A. Potential Growth of Computer-Related Misconduct

Not much is known about the future size and scope of computer-related misconduct.[11] Statistics and surveys compiled to date are of limited utility, but do reflect trends that would support qualified assumptions. It is reasonable to expect steady increases in the number of people with the technical capability to commit computer-related misconduct, and the continued widespread availability of increasingly harmful and easy-to-use "hacker" tools. It is also reasonable to assume public and private institutions' growing dependence on information technology, and growing interdependence on the information and processes that are generated by and shared among them. Taken together, these trends could mean an increase in the number of unauthorized intrusion incidents, and an increase in the severity of the potential effects of any single intrusion incident.

Congress has begun to ask difficult questions about the ability of law enforcement and the defense community, as currently configured, to serve adequately national interests in this area.[12] There has been little or no discussion, though, about contributions that could be made through the formalization of the resources that are already trained and equipped to work within the private sector. Because it makes good administrative sense to consider extant resources before building anew, these potentially powerful capabilities should also be included within the framework for discussion.

We may be at a stage where the proliferation of personal computers and computer networks resembles the birth and expansion of automobile transportation, although at an accelerated pace. We hold out high hopes for security measures, but if they do not fulfill their promise, the next few years could see unlawful instances of computer-related misconduct — if unchecked or undeterred — become as common as traffic infractions. Traffic infractions, however, are not all handled through conventional "criminal" channels. Consider the overlapping and decentralized criminal and administrative enforcement mechanisms that

---

11. The term "computer-related misconduct" is used in a broad sense to refer not only to unauthorized intrusions, but also to unauthorized interceptions of communications, routine instances of trespass that may result from exceeding authorized access, or incursions into privacy caused by, for example, e-mail "snooping."

12. See, e.g., *Hearings Before the Subcomm. on Terrorism, Tech. and Governmental Info. of the Senate Comm. on the Judiciary*, 105th Cong. (Mar. 17, 1998) (statement of Sen. Kyl) (on file with the *Harvard Journal of Law & Technology*); *id.* (statement of Jamie S. Gorelick & Sam Nunn) (on file with the *Harvard Journal of Law & Technology*).

developed in response to the growth of automobile transportation. Similarities are apparent:[13] Respective rights of way are pervasive across our borders. Jurisdiction is often shared. Different rules govern bodies in motion (electronic interceptions and "moving violations") and at rest (stored electronic communications and parking infractions). Before the problem becomes this large, we need to assess existing divisions of response authority.

Because we do not know very much about the future scope of the problem, we cannot now know very much about the effectiveness of any particular set of solutions. Technology may lead to promising ways of preventing minor intrusions and detecting major ones, thus making enforcement truly manageable. Law enforcement resources and capabilities will continue to grow, perhaps obviating the need to consider alternatives. Civil enforcement regimes are likely to assume a more prominent role as well. But certain trends create cause for concern: Computer crimes are more difficult to detect than other forms of crime. A large percentage appear to go undetected, with others detected only long after having been committed. Even when detected, equities often militate in favor of not reporting incidents. And many of the same factors that make detection so difficult also make responding to an incident an inordinately time and resource-intensive undertaking. All of this has contributed to the rapid growth of a private-sector response capability. But this capability is one that arose to prevent and respond to discrete incidents, and is thus highly decentralized, creating accompanying concerns.

It may now be the best time to begin a public dialogue about possible ways of supplementing existing response capabilities. Perhaps a coordinated effort to clarify the roles of the public and private sectors with respect to investigation and responsive legal action is warranted, and could be done in a manner that is mutually beneficial to public and private interests.

B. Computer Crime is Different from Conventional Crime

Computer crime is different from conventional crime. It is grossly under-detected and under-reported. It is extraordinarily difficult and expensive to investigate owing to jurisdictional complexities, among other things. The laws in the area are complicated, and are evolving at a different rate from the underlying technology. As a result, responding

13. The analogy is imperfect, as it fails to account for issues relating to enforcement of computer-related misconduct across international boundaries.

to computer crime can severely tax even rapidly developing law enforcement response capabilities.

1. Difficulties in Detection

Roughly speaking, less than one in ten successful computer intrusions is detected.[14] There are many reasons why this may be.[15] Detection tools are still in the early stages of development. Existing security measures are, like their physical analogues, often slow and cumbersome, and as a result are only partially implemented or are implemented in ineffective ways. This leaves the difficult and often burdensome task of monitoring networks to systems personnel, who may also be overwhelmed with providing other forms of computer support. Even with monitoring, small anomalies may not be apparent. Those who use the systems may not attribute the anomalies to intrusions or other forms of unauthorized behavior. To increase intrusion detection capabilities, technological and educational solutions are required.

2. Limited Reporting

Even if intrusions are detected, victims tend not to report intrusions, particularly to law enforcement. Frequently-quoted sources place figures for reporting intrusions to law enforcement at somewhere between eleven percent and seventeen percent.[16] There are many documented reasons behind the reluctance of private businesses to report

---

14. *See* KaBay, *supra* note 10. It is difficult to estimate the percentage of intrusion incidents that are actually detected. For example, in a 1996 General Accounting Office report, the Defense Information Systems Agency (DISA) estimated that during vulnerability assessments of Department of Defense systems only 4% of attacks were detected. *See* GENERAL ACCOUNTING OFFICE, INFORMATION SECURITY: COMPUTER ATTACKS AT DEPARTMENT OF DEFENSE POSE INCREASING RISKS, GAO/AIMD-96-84 (1996).

15. See Dierks, *supra* note 8, at 332–33, for discussion of difficulties of detecting computer crimes.

16. The Computer Security Institute reports 17% of detected intrusions are reported. Previous FBI estimates have been at 11%. Estimates of the rates of reporting for the Department of Defense are even more disparate. The range is from between 1 in 8 (12%) and 1 in 140 (0.7%). See generally, the discussion of DISA and Air Force Information Warfare Center statistics in John D. Howard, An Analysis of Security Incidents on the Internet:1989–1995, 174–77 (1997) (unpublished Ph.D. dissertation, Carnegie Mellon University, on file with *Harvard Journal of Law & Technology*).

intrusions. [17] As news of a computer vulnerability could be devastating to business, companies often demand a degree of confidentiality that law enforcement rarely can promise. Businesses may also be reluctant to relinquish control over the resources they dedicate to an investigation. Because they can be extraordinarily resource-intensive, companies often prefer to remain in control of the resulting investigation — to preserve the option of terminating it before it becomes too costly. They also prefer to remain in control of their remedies, i.e., whether to take the case to civil court, criminal court, or to resolve it internally.[18] These needs — for confidentiality and control over resources and remedies — appear to be some of the principal drivers behind the development of private response alternatives.

3. Jurisdictional Complexities

Computer crimes are geographically complex, often crossing state or international boundaries. As a result, they are jurisdictionally complex, usually necessitating involvement by more than one authority, and often hindering state authorities' ability to pursue complete investigations.[19] Even novices are usually clever enough to disguise their actual location by looping through several systems before reaching their final destination. In fact, the desire to use free long-distance service for hacking activities may necessitate a certain amount of this evasiveness. The chances of an intruder remaining within one state's jurisdiction become more remote with every additional system he or she enters. And in an increasingly networked world, it is increasingly likely that an intruder would enter at least one foreign system, perhaps even without

---

17. *See, e.g.*, Branscomb, *supra* note 8, at 55–56; Scott Charney & Kent Alexander, *Computer Crime*, 45 EMORY L.J. 931, 938 (1996); Dierks, *supra* note 8, at 335 (financial disincentives to reporting); see also James A. Fagin, Computer Crime: A Technology Gap, 15 INT'L J. COMP. & APPLIED CRIM. JUSTICE 285 (1991); B.J. George, Contemporary Legislation Governing Computer Crimes, 21 CRIM. L. BULL. 389 (1985).

18. We understand it is not uncommon for companies to hire private investigative specialists to track and identify sources of intrusions or other anomalies. Often, as a cost-effective alternative to law enforcement, investigators will issue intruders a warning, which often provides satisfactory resolution of the problem for that victim. Similar methods were noted during discussion with computer security experts in conjunction with the Security in Cyberspace Hearings. *See Security in Cuberspace Hearings* (statement of Minority Staff), *supra* note 2, at 48–49.

19. *See generally*, Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 EMORY L.J. 911 (1996) (discussing the inadequacy of traditional, territory-based regulatory regimes for governing activities in cyberspace).

knowledge of having done so. This situation usually demands some level of involvement by federal law enforcement in the investigation.

Legal measures to ease these jurisdictional impediments are not unattainable, but are likely to place an even greater burden on a centralized federal response. For example, the U.S. government is currently working in international fora to enhance the ability of cooperating law enforcement officials to investigate computer crimes that cross international boundaries. The measures being contemplated include creating networks of law enforcement and communications carriers who can work together on investigations, and improving the legal agreements by which cooperation can be extended in time-sensitive situations.[20]

4. Resource Constraints

The burden imposed by jurisdictional complexities is aggravated by the highly resource-intensive nature of computer crime investigations. Staffing a response capability involves the cost of procuring and frequently updating hardware and software, and training and retaining qualified personnel. Perhaps most significantly, these investigations are extraordinarily time-intensive. Whereas a typical (non-"high-tech") state or local law enforcement officer may carry between forty and fifty cases at a time, a high-tech investigator has a full-time job handling three or four cases a month.[21] Considering that approximately only one tenth of all intrusions are detected and roughly one tenth of those are currently reported, the implications for building an effective response proportional to the problem — given its potential rate of growth — should be apparent.[22]

---

20. *See, e.g.*, Communique of the Meeting of Justice and Interior Ministers of The Eight (Dec. 10, 1997), *available at* <http://www.qlinks.net/comdocs/washcomm.htm> (communication from meeting to discuss enhancing the abilities of the participant nations to investigate and prosecute high-tech crimes).

21. *See* Ingrid Becker, *Cybercrime: Cops Can't Keep Up with Technobandits*, CAL. LAW., June 1995, at 47, 91 (quoting Bill Spernow of the System for Electronic Analysis and Retrieval of Criminal Histories ("SEARCH") Group).

22. Assuming that existing law enforcement capabilities were sufficient to be perfectly responsive to all incidents currently reported, these figures suggest that a 10% increase in either the number of incidents detected *or* the number reported would effectively double the resources required to investigate. A 10% increase in detection *and* reporting would require a quadrupling of existing resources. Considering that computer crime specialists only appear to be able to manage roughly one tenth of the number of cases handled by non-high-tech investigators, the number of investigators required to fully staff a response capability — one that would keep pace with anticipated

C. State of the Law

Through the 1980s, lawmakers and enforcement officials were learning how to address computer-related crime. It was seen largely as a shared responsibility between local, state, and federal government. More recently, the explosive growth of international data networks and the Internet has shifted a greater degree of enforcement responsibility and authority to the federal government.[23]

The Computer Fraud and Abuse Act ("CFAA") prohibits a range of activities involving unauthorized access to protected computers.[24] Insofar as private security experts may lack authorization to enter third-party systems, even for investigative purposes, some of the law's prohibitions may impact attempts by private parties to trace and identify unauthorized intruders.[25] Prohibitions of the Electronic Communications

---

improvements in intrusion detection technologies — would be staggering.

23. By the late 1980s, 49 states had computer crime laws on the books, and Congress had passed (in 1984) and amended (in 1986) the Computer Fraud and Abuse Act ("CFAA"). 18 U.S.C.A. § 1030 (West Supp. 1998). Early iterations of the CFAA recognized the shared responsibilities of local, state, and federal law enforcement. Congress, reluctant to preempt state computer crime enforcement, drew the law to protect only a relatively narrow class of "Federal interest computers." The term applied roughly to government computers, banking computers, and computers involved in offenses that crossed state lines. *See* 18 U.S.C.A. § 1030(e)(2) (West Supp. 1998). Successive amendments to the CFAA in 1994 and 1996 have now expanded federal jurisdiction over government computers, banking computers, and computers "used in interstate or foreign commerce or communication." 18 U.S.C.A. § 1030(e)(2)(B) (West Supp. 1998).

24. *See* 18 U.S.C.A. § 1030 (West Supp. 1998).

25. The CFAA, in its most general sense, prohibits *unauthorized* intrusions into computers protected by the statute. But if an intruder, through her own act of unauthorized intrusion, were to implicitly consent to reciprocal actions by the victim, then the intruder would be hard-pressed to argue that these reciprocal actions were not authorized. "Banner" warnings posted on computer systems currently serve a similar purpose with respect to consensual monitoring of unauthorized intruder activity. Note, however, that such consent, even if upheld as valid, would not necessarily constitute consent to pass through third-party systems to identify the source of an intrusion.

The fact remains that the full implications of the CFAA on the activities of computer security professionals have not been adequately spelled out. Legal experts can reasonably disagree on the interpretation of key provisions, and few technology professionals are fully aware of the scope and implications of alternative interpretations. For example, a major telecommunications company recently announced its intent to release free software that can track down "hackers" by following paths back through several servers to locate the source of the attack. *See* MCI, Information on DoSTracker, (Oct. 9, 1997) (press release), *available at* <http://www.security.mci.net/dostracker/prelease.html>. Some applications of this software might be construed by the Department of Justice to constitute a criminal violation of applicable computer crime

Privacy Act ("ECPA") may similarly restrict private intrusion response while placing carefully circumscribed conditions on law enforcement access to protected forms of communication.[26] Prohibitions in the federal wiretap statute make it unlawful to intercept real-time computer-based communications just as it is unlawful to intercept voice communications.[27] It bears noting, however, that the wiretap statute was originally drawn to pertain to telephonic voice communications and was subsequently extended to pertain to electronic (and hence computer-based) communications. The wiretap statute can, as a result, be interpreted to apply to networked computer environments in broad, unpredictable, and occasionally even counterintuitive ways.

The civil law has lagged considerably behind the criminal law in this area, leaving victims an insufficient number of middle-ground options between pursuing criminal remedies and essentially doing nothing. But effective civil remedies are beginning to appear in state codes,[28] and in 1994 the CFAA was amended to include a federal civil remedy.[29]

D. Law Enforcement Capabilities

Law enforcement techniques and capabilities appear to be improving at the state, local, and federal level. Investigators are receiving more and better training, and are hiring professional staff with relevant skills. Over time, investigators have become more acutely aware of the sensitivities of private sector victims, and are learning to conduct investigations in ways more respectful of their need for confidentiality and control over resources and outcomes. As indicated above, however,

---

laws.

26. *See* 18 U.S.C.A. §§ 2701–2711 (West 1970 & Supp. 1998).

27. *See* 18 U.S.C.A. §§ 2510–2522 (West 1970 & Supp. 1998). Thus, some applications of commonly-used "packet sniffer" devices, without proper consent, may be construed as violations of the federal wiretap statute.

28. Representative state civil remedies include CAL. PENAL CODE § 502(e) (West 1988) (permitting recovery of compensatory damages); CONN. GEN. STAT. § 52-570b (1997) (allowing civil recovery independent of criminal actions for acts done recklessly); GA. CODE ANN. § 16-9-93(g) (1996) (allowing victim to recover damages, including lost profits).

29. *See* 18 U.S.C.A. § 1030(g) (West Supp. 1998). To date, we have located one attempt to invoke the federal civil remedy, albeit unsuccessfully and in an unreported case. *See* Letscher v. Swiss Bank Corp., No. 94 CIV. 8277 LBS, 1997 WL 304895 (S.D.N.Y. June 5, 1997).

these capabilities come at considerable costs[30] and are inherently limited in their ability to provide confidentiality.[31]

At some point, it may be incumbent on law enforcement to plot the relevant growth trends, and to arrive at a realistic estimate of the resources required to continue to address these incidents. It may be, for example, that there are practical limits imposed for budgetary or policy reasons that would be placed on its ability to expand proportionately.[32]

E. Private Sector Capabilities

At the same time as law enforcement capabilities are increasing, the private sector response is growing very rapidly.[33] A series of recent mergers and consolidations in the computer security industry signals its coming of age and tremendous potential for profitability.[34] Practitioners estimate that there are over 600 firms currently offering some form of computer security services, including firewall installation, intrusion response, incident recovery, and backup restoration. Some but not all of these businesses offer actual incident investigation.[35] Though dictated,

---

30. *See supra* Part II.B.

31. Law enforcement may be willing to modify its current investigative procedures to allow for greater confidentiality and control by victimized companies. There are, however, legal and, more importantly, constitutional limitations on the extent to which such procedures can be modified. For example, while the private sector may crave confidentiality, the Constitution and laws of Congress quite properly require a large degree of transparency and openness. *See, e.g.*, Darryl C. Wilson, *Viewing Computer Crime: Where Does the Systems Error Really Exist?*, 11 COMPUTER/L.J. 265, 284 (1991).

32. *See* discussion of growth of incidents *supra* notes 14 & 22.

33. As early as 1994, estimates of the annual growth rate for the information security industry were as high as 70% to 100%. *See Infosec Growth to Continue — Internet Security Hot*, SECURITY TECH. NEWS, Oct. 21, 1994, *available in* 1994 WL 8715532.

34. *See, e.g.*, Malcolm Maclachlan, *Security Market is Maturing, but Needs Standards*, TECHWEB NEWS (Mar. 9, 1998) <http://www.techweb.com/wire/story/0398iwld/TWB19980309S0015>; Todd Spangler, *Rapid Consolidation in Security Market*, WEBWEEK (Dec. 8, 1997) <http://www.internetworld.com/print/1997/12/08/news/19971208-rapid.html>; Wylie Wong, *Security Software Companies Continue Consolidation*, TECHWEB NEWS (Feb. 24, 1998) <http://www.techweb.com/wire/story/TWB19980224S0011>.

35. It is unclear, however, what percentage of computer security firms might make available response capabilities, or even how a useful conceptual distinction might be expressed to separate those who provide more conventional computer security services from thos who offer investigative service. Some firms attempt to maintain a hard distinction between "intrusion response" and "incident investigation." "Intrusion response" may refer to responsive and restorative actions taken by security specialists

of course, by the client, the focus of these companies' efforts is not always consistent with the focus of law enforcement. The companies offer services to protect against, respond to, and mitigate the effects of harmful intrusions. Finding their source is a secondary concern.

These businesses range in size from the largest nationwide security firms to individual practitioners who, with technique, tools, and talent, are striking out on their own with increasing frequency.[36] Qualifications and standards of practice appear to vary accordingly. Some businesses maintain procedures to insure trustworthiness and accountability. Others primarily emphasize results.[37] Some businesses appear to be acutely aware of the limitations placed upon their activities by current law — civil and criminal — and conduct their businesses accordingly. Others are likely unaware of the potential implications of certain legal provisions. Still others, we fear, may even use their willingness to disregard current law to their competitive advantage.[38]

III. A CALL FOR A BALANCED PUBLIC/PRIVATE APPROACH

It may indeed be desirable to improve oversight and increase the professionalism of investigative segments of the computer security profession. But there are also certain features demanded by clients that should remain undisturbed — key features that originally fueled the rise of the profession and that remain integral to its continued growth and success. To get a sense of some of these factors and the equities underlying them, we have spoken with a number of private security

---

within systems that belong to their clients. "Incident investigation" may refer to actions taken outside a client's system, in an attempt to track and identify sources of disruption. Given the close interdependence of many systems, potential shared vulnerabilities, and muddled conceptions of system ownership, we question whether this can always be a serviceable distinction.

36. A search of the Internet reveals that an increasing number of members of the private investigations field are branching out into computer-related areas. *See, e.g.*, In fact, the National Association of Investigative Specialists "Investigator of the Year" for 1996 specializes in computer-related cases. *See* Ralph D. Thomas, *The Nation's Cutting Edge Cyber Detective–A New Kind of Private Eye* (visited Apr. 9, 1998) <http://www.pimall.com/nais/n.seanor.html>.

37. This tension is exemplified by the debate within the computer security field over whether or not to hire hackers as consultants. Some find the practice irresponsible and fear liability; others stand behind the practice as an important way to secure needed expertise. For further discussion, see RICHARD POWER, CURRENT AND FUTURE DANGER: A CSI PRIMER ON COMPUTER CRIME & INFORMATION WARFARE 12–13 (2d ed. 1996).

38. In instances where private investigative practices may run afoul of current criminal law, law enforcement resources would be doubly taxed by having to investigate the conduct of the intruder *and* the investigator.

practitioners, some of whose activities would likely fall within the purview of the measures contemplated here.

A. What the Industry Would Need from an Oversight Mechanism

We learned, not surprisingly, that confidentiality is the cornerstone of the computer security business. Clients insist on confidentiality above all because, for many, public confidence is their most valued asset. This includes, for example, public confidence in the ability of businesses to deliver service reliably, and to maintain with confidentiality and integrity the information they receive from clients and customers. In businesses such as these, public knowledge of an actual or apparent vulnerability, or of an event that appeared to exploit or actually exploited a vulnerability, could cause significantly more harm than the vulnerability or the event itself. Accordingly, the experts we spoke to made clear that for their services to remain valued and effective, any oversight mechanism would have to allow for services to be rendered confidentially.

Currently, confidentiality is dictated largely by the client, and is controlled through individual non-disclosure agreements often drawn by the client. A more formal type of confidentiality is not without precedent within professional licensing schemes. The doctor/patient, lawyer/client, and priest/penitent privileges are all well known and accepted. A similar type of privilege is beginning to be recognized in an area more clearly analogous to the security-service-provider/client relationship; at least one state currently recognizes a privilege for the private investigator-client relationship[39] and many other states protect client information from disclosure by law.[40]

Confidentiality would assist in the fulfillment of another condition demanded by clients — control over the outcome of the incident. It is not uncommon for clients to conduct a preliminary, internal assessment of a problem and weigh its likely causes and effects before considering additional action. When additional action is desired, customers are then able to choose among a range of available remedies, including informal resolution through private channels.[41] In such instances, the option to seek criminal investigation and prosecution still exists and in many cases

---

39. *See* MICH. COMP. LAWS § 338.840 (1997) (stipulating investigator/client privilege).

40. *See* ARIZ. REV. STAT. ANN. § 32-2455 (West 1996); CONN. GEN. STAT. § 29-156q (1996); HAW. REV. STAT. § 463-15 (1996); 225 ILL. COMP. STAT. 446/195 (West 1996).

41. *See supra* note 18.

may offer the only real satisfaction for the victim. There are, however, other options a client may consider. Civil remedies are available through federal and state law, for example.[42] A client may even decide that it is not worth the expenditure of resources required to identify the source of the intrusion, and may simply ask the security expert to "plug the hole."

B. Oversight Options

We noted above that certain trends and factors may make it desirable to improve oversight and increase professionalism of the computer security profession, or at least certain segments of it. But whose responsibility should it be? Is it a governmental responsibility, or should the profession police itself? How strictly should adherence to rules and norms be enforced? These are some of the fundamental policy questions that differentiate licensing schemes from less imposing, but also less effective, means of oversight.

1. Licensing

Although licensing may mean different things depending on the profession, it does have certain fairly uniform characteristics. Licensing schemes, such as those that apply to lawyers, doctors, and even most state-licensed private investigators, involve a degree of governmental involvement. The government may issue licenses directly, or establish boards of practitioners to oversee the licensing function.[43] Licensing authorities may set minimum educational and training requirements, impose professional conduct standards, and provide a mechanism for continued oversight to review the status and performance of licensees.

Licensing frameworks carry advantages. They offer robust and identifiable mechanisms to provide services related to the license. Often, licensing bodies set requirements governing receipt of the license; administer the necessary tests, background investigations, continuing education requirements, and professional conduct standards; and develop a disciplinary framework. These organizations are largely overseen by

---

42. *See supra* notes 28–29.

43. For example, the Nuclear Regulatory Commission ("NRC") sets out the terms and conditions for licensing and issues licenses directly to operators of nuclear facilities. *See* 10 C.F.R. § 55 (1997). In the professions typically licensed at the state level there is often an additional layer between the licensee and the state. This is often a board of professionals that assists the state in setting educational and other qualification standards and reviewing character and other disciplinary matters. *See, e.g.*, N.Y. EDUC. LAW §§ 6521–6529 (McKinney 1997) (licensing for medical doctors).

peers of the licensees — those who best understand the nature of the profession. Licensing bodies can be responsive to an ever-changing environment, as they often have considerable direct or indirect influence over licensing requirements. Licensing bodies are effective enforcers. It is generally quite clear to those obligated to keep a current license that they remain accountable to the issuing authority. A breach can substantially harm a practitioner's professional reputation and lead to monetary fines, suspension, or even revocation of the license.

Whatever advantages may accrue from its ability to achieve close oversight and compliance, a licensing body has the corresponding disadvantage of requiring a fairly elaborate bureaucracy. While many bureaucratic costs can be recovered through licensing fees,[44] the mere existence of a bureaucratic framework may discourage candidates from obtaining a license or from participating in the profession.

State licensing of traditional investigators may provide both a model for and some potential obstacles to the growth of the investigative aspects of the private profession. More than forty states currently have mandatory licensing schemes for private investigators.[45] The schemes not only set forth licensing prerequisites, but make it unlawful to engage in certain specified activities without a license. Many of the licensing schemes are quite robust, and include rigorous qualifications to obtain a license, continuing education, stringent professional conduct requirements, and appropriate oversight to enforce the licensing standards.[46] Despite all of these requirements, which would seemingly ensure a high caliber of professional conduct among private investigators, abuses are not uncommon and some who are harmed by a private investigator's conduct decline to report violations to the licensing board for fear of having sensitive information publicized.[47]

State licensing schemes actually may create additional challenges, owing to an overlap between traditional private investigative services and emerging computer investigative services. Computer security experts could find themselves subject to state licensing schemes for private investigators if they are not cognizant of the law and careful to limit the services they provide. This could be problematic for a computer security expert not only because the skills and education

---

44. California's private investigator licensing framework is at least partially funded through licensing fees. *See* CAL. BUS. & PROF. CODE § 7520 (West 1997).

45. *See, e.g.*, MASS. GEN. LAWS ch. 147 § 23 (1994); N.J. STAT. ANN. § 45:19-10 (West 1995).

46. *See, e.g.*, 225 ILL. COMP. STAT. 446/1-299 (1997).

47. *See* Michael A. Braun & David J. Lee, *Private Police Forces: Legal Powers and Limitations*, 38 U. CHI. L. REV. 555, 559–60 (1971).

required to be a private investigator may not be similar to his computer security skills,[48] but also because he may have to satisfy the requirements of each jurisdiction in which he conducts investigations.[49]

2. Certification

Other professions are not subject to licensing requirements, but rather require a certification or other official "seal of approval." Much like licensing, certification schemes can ensure that those practicing are properly trained and educated. To receive certification, an applicant may be required to take a prescribed set of courses, or even to pass an exam. Once the initial qualifications are met, however, few certification programs provide additional or continuing oversight. They may provide nominal professional conduct standards, but generally lack effective discipline mechanisms. They generally do not require certified professionals to stay current with new developments in order to keep their certification active.

There is a number of emerging private certification authorities in information technology. Some even address computer security services.[50] In our view, they will only accomplish part of the job. Private certification authorities may raise educational requirements, and perhaps even impose minimal liability insurance requirements and procedural guidelines to aid the private sector in obtaining trustworthy services. But without substantial incentives and/or disincentives, the government and the public are less likely to benefit. Without enforceable standards of conduct and a strong enforcement mechanism, there is little deterrence of overly intrusive investigation practices,

---

48. The flip side of this is that some who are currently offering computer intrusion investigative services are in fact state-licensed private investigators. It is unlikely that the skill sets of computer security experts and private investigators are similar. In fact, the danger posed by those who may be "licensed" computer investigators already, but who are not experts in computer technology, may be one of the most powerful arguments in favor of requiring a unique license to conduct this specialized type of investigation. *See supra* Part II.B.

49. States, in general, do not recognize any kind of reciprocity for private investigator licensing. In fact, some states even allow local jurisdictions to add requirements on top of the state requirements. *See, e.g.*, OHIO REV. CODE ANN. § 4749.09 (Anderson 1997). This jurisdictional complexity is one of the more vexing issues complicating state investigations of computer misconduct that crosses state lines.

50. *See, e.g.*, International Information Systems Security Certification Consortium (visited Mar. 14, 1998) <http://www.isc2.org>. The International Information Systems Security Certification Consortium ("ISC^2") certification framework is based on an exam, and requires either continuing education over a three-year period, or passing the exam again, to maintain certification. The ISC^2 also has a code of ethics.

particularly in areas where procedural shortcuts can save considerable time and resources. And without a standing body to oversee and facilitate limited information sharing, the government would likely be left in no better position to assess threats and vulnerabilities from a national perspective. It bears noting, however, that licensing and certification schemes need not be mutually exclusive. They can even coexist insofar as certain certifications may serve as necessary prerequisites to obtaining a license.

IV. FERTILE GROUND FOR COMPROMISE

Achieving the delicate balance between public and private investigative authority involves the weighing of the needs for accountability and deterrence. We have noted the limits of a traditional law enforcement response to maximize deterrence, the inherent limits on victim confidentiality, and potential for growth of the problem. But allowing unfettered expansion of a powerful private sector response, under conditions that could jeopardize accountability, is not a satisfactory solution. Fertile ground for compromise lies somewhere in between.

A. What the Industry Could Get from an Oversight Mechanism

An oversight mechanism, such as a licensing scheme, could carry substantial benefits for those currently offering computer investigative services. Benefits include competitive advantages, a more predictable legal and liability climate, more well-defined standards of practice, and enhanced trustworthiness of those engaged in the profession.

A licensed investigator may benefit from operating in a more clearly defined legal environment. The terms of the licensing scheme might, for example, exempt a computer investigator from state licensing requirements that might otherwise apply, reducing the potential for incurring penalties for operating without a license in certain jurisdictions and reducing duplicative licensing requirements. The computer investigator may benefit not only from clarification of the administration requirements governing his activities, but also from a clarification of the substantive laws, such as the CFAA and the ECPA, that govern activities relating to computer networks. The formal recognition of the profession and its function — investigation of computer intrusions and tracking of intruders — may facilitate needed reexamination and clarification of many of the laws implicated by activities such as system monitoring, tracking of the source of an intrusion, and other attempts to identify

intruders.[51] Even if clarification or modification of controlling law is slow to occur, the licensing oversight body would be available to provide guidance to investigators on the application of these laws to their practice. This guidance likely would remove much of the prevailing doubt and fear about exposure to criminal and civil penalties for violations of relevant statutes.

Consider, in addition, the potential liability that private security practitioners can currently face owing to the sensitive nature of their duties and the value of the systems and information placed in their care. The nature and extent of their duties, the conditions that might constitute a breach, and their resulting liability exposure are currently undefined in the industry. Practitioners and clients address these issues in contracts, but these contracts cannot fully address third-party liability. With increasing interconnectedness and interoperability of systems, third-party vulnerabilities, liabilities, damage, and related issues will inevitably be addressed in law — but only over time and probably only after much conflicting precedent.

Enhanced oversight may provide the quickest means of achieving a more adequately defined liability climate and to accelerating the availability of needed insurance products. An oversight mechanism could, for example, require practitioners to carry a certain level of liability coverage adequate to meet the needs of potential plaintiffs. This requirement could be scaled or structured to reflect the character of the services that were made available. This insures that those whose systems might be damaged or whose data might be compromised could recover. As importantly, and in the interest of fostering growth of the profession, an oversight scheme could bound the level of liability for the practitioner and make insurance a more estimable and predictable cost of doing business (one that could be distributed uniformly across the practitioner's client base).

Though oversight may help define the liability climate in direct ways, requiring computer security experts who track the source of an intrusion to meet certain educational criteria and to follow professional standards may ultimately, albeit indirectly, reduce the need for or reduce the cost of liability coverage. Practitioners who are educated not only about the legal limits of their ability to trace intruders, but who are also technically aware of the potential dangers and pitfalls, are more apt to stay within appropriate ranges of activity. In addition, knowing that a serious mistake, whether or not technically illegal, could have serious

51. *See supra* note 25 and accompanying text.

consequences for one's ability to practice will ensure adherence to a more rigorous standard of care.[52]

One of the more tangible benefits for all concerned that would emerge from an oversight mechanism would be the development of standard practices within the industry. Standards, defined liability, and education and training criteria would all contribute to the trust placed in a computer security expert. Thus, the license itself would likely accrue value as a marketing feature. Customers would likely opt to use a licensed investigator over an unlicenced investigator, secure in the belief that services provided will meet certain quality standards. Investigators would likely pay reasonable licensing fees if confident of the liability and marketing advantages, and the licensing fees could be used to make the governing body self-sufficient.

B. What Government Could Get from an Oversight Mechanism

Improving intrusion response should be a primary concern of both the private and public sectors. Without an adequate and effective response and the attendant benefits of stout deterrence, unlawful events may proliferate and interfere with reliable and safe operation of systems and networks. Likewise, the proliferation of even relatively "minor" events threatens to "raise the noise level" — as minor intrusion attempts may make gravely harmful events all the more difficult to detect.[53]

Law enforcement is likely to express concern that a private response will not complement, but rather thwart its current law enforcement efforts. Such an argument is misdirected because it fails to recognize that a potent private sector response exists today, and that it appears to be growing at a rate at least commensurate with that of law enforcement. The question is not whether a private response should be permitted to exist — it does. In recognizing the inevitability of these private response mechanisms, law enforcement and government should instead consider

---

52. We can imagine that if there were substantial and enforceable consequences for breach of or damage to third-party systems in the course of an investigation, it would provide an additional incentive for private investigators to contract with or obtain consent from those parties. Obtaining consent in this way could also serve the interest of comporting with the dictates of the criminal law. *See* 18 U.S.C.A. § 2511(2)(d) (West 1970 & Supp. 1998) (consent exception to wiretap statute); 18 U.S.C.A. § 2702(b) (West 1970 & Supp. 1998) (consent exceptions to ECPA).

53. *See* Trent D. McNeeley, *Hackers, Crackers & Trackers*, THE AMERICAN LEGION MAGAZINE, Feb. 1997, at 34 (quoting FBI agent that those who pose real threats "tend to hide among the noise—the everyday, 'OK' hackers who just enjoy penetrating and exploring systems"), *available at* <http://www.legion.org/pubs/1997/hackers.htm>.

the degree to which they should nurture the growth of the profession to serve the best interests of society.

That said, we do not agree that recognition or even fortification of a private investigative response will invariably interfere with law enforcement efforts. First, the mere availability of private professionals will not interfere with law enforcement's ability to investigate any incidents that continue to come to or are brought to its attention. Rather, with private professionals available to provide a supplemental response, law enforcement could be freed from the weight of preliminary work associated with distinguishing between nuisance intrusions and more serious threats to our national or economic security, such as dangerous intrusions into federal government systems and incidents involving economic espionage. Law enforcement could focus resources on investigations that, for the time being, appear to require governmental intervention, such as intrusions originating from foreign countries. Second, it is possible that law enforcement reporting might actually increase, as practitioners who are reluctant to exceed their legal authority and risk sanction or loss of license would be inclined to recommend that their clients make referrals to law enforcement when available private response options have been exhausted.

As private response capabilities grow, it is likely that an increasing number of incidents will be handled without the government's knowledge or involvement. This cannot bode well for the government's ability to obtain an accurate appreciation for the scope and nature of the threat, extant vulnerabilities, or for the development of an effective threat warning capability. The computer security industry would continue to conduct its business outside of the view of law enforcement, and the government would derive little benefit from the information, insights, or collective expertise and experience of those working within the industry. Instead, we merely suggest that the government first recognize the services being performed by computer security experts and private investigators, and second, consider aiding in the "professionalization" of the investigative portion of those services. These steps would create opportunities for increased cooperation between the industry and law enforcement.

This cooperation may involve little more than opening lines of communication between private computer specialists and the government. Increased communication, even if in the form of sanitized and generic reporting on incidents and vulnerabilities, could contribute significantly to the effort of government and law enforcement to estimate the size of the problem, to develop responsive policy, and to allocate sufficient resources to the problem area.

But cooperation likely would achieve additional benefits. Evidence collected by private computer security experts operating in an investigative capacity would be available for use in civil and criminal proceedings. Security experts may be important sources of expertise and evidence, even in cases initiated by law enforcement or cases later referred to law enforcement by the victimized system owner. They can (and do currently) loan valuable technical expertise to law enforcement in complex criminal cases. Depending on the resources available to law enforcement investigators in the future, having additional support to gather preliminary information, or to turn over to law enforcement "ready-made" cases, could be an important component of effective criminal deterrence of computer crime. [54]

C. What the Public Could Get from an Oversight Mechanism

Investigations into computer intrusion incidents are delicate undertakings. Their effectiveness is dependent on the practitioner's having a working knowledge of the latest technology, and their legality is dependent on the practitioner's having a detailed knowledge of the current state of the law. The position of investigator is not unlike that of a doctor or lawyer, who is expected to be maximally effective through their knowledge of the most recent developments in her field, but who is held strictly to the bounds of safe, ethical, and professional conduct.

Potential breaches of safe and ethical conduct can create similarly serious consequences. In the same way that the doctor protects a patient's life, and the attorney a client's liberty and property, the security specialist deals in an environment that places at risk a business' most valued commodities — its communications and information. They do their work in an environment that can be easily abused, in which abuses are extremely difficult to detect. Unlike doctors and lawyers, but more like police officers, they are in a position to place third parties in jeopardy by infringing on third-party systems and communications.

---

54. In a growing number of areas, particularly those involving economic crime, private investigators — many of them former law enforcement officers — are employed by companies and trade associations to continue to pursue their chosen profession, albeit from the private side. This is common practice, for example, in the insurance and intellectual-property-based industries. In such instances, industry investigators conduct preliminary investigations and compile evidence of incidents that might otherwise escape the attention of law enforcement. They may present to law enforcement evidence so gathered, and often continue to provide assistance to law enforcement after cases are referred.

Investigations should be undertaken in ways that minimize these dangers.

Mitigating risks to third-party systems comes through care, equipment, and experience. It requires in-depth knowledge of the systems that are placed at risk, access to the latest technology or to a proper testing environment, and experience to guide selection of tools and techniques. Mitigating risks to personal privacy requires knowledge and appreciation of the prevailing laws, current company policies and procedures, and adherence to principled investigative practices.

Although it is certainly possible to find practitioners who meet these lofty standards, it can be made more likely through adherence to an oversight structure. Clients and customers would likely be more confident in their expectations about the safety and quality of the services provided. Third parties would likely be more confident that such services would be rendered in ways that did not impinge on their interests. In either case, the public and the profession would benefit.

D. Long-Term Benefits of a Cooperative Environment

There are still other longer-term benefits that may be realized. Facilitating the growth of a responsible investigative profession undoubtedly would expand the market for better tools to detect and identify the source of unauthorized intrusions. Increased private-sector market demand can, in turn, be expected to stimulate research and development in a way that the government market alone cannot.

It is precisely because the private sector is so adept at developing and using current technology that law enforcement currently uses private computer security experts as advisors, technical consultants, and even contract support on investigations.[55] A licensed group of computer security experts trained and experienced in conducting investigations would provide even more outsourcing opportunities for government. In addition, this cadre of trained experts could be mobilized in the event of

55. George Vinson, Supervisory Special Agent of the FBI's computer crime squad, was quoted in an Internet newsletter as saying that his unit outsources most of the technical work on their investigations to computer security experts. *See* Joel Deane, *Digital Dragnet: The Hacking Crackdown*, at The Hacking Crackdown (visited Apr. 26, 1998) <http://www.zdnet.com/zdtv/thesite/0597w3/life/life550_051297>.

national emergencies[56] under specific arrangements defined by the oversight body.

The greatest benefit of such a supplement to current law enforcement capabilities may be the rich source of information that ultimately could help the government perform its responsibilities more efficiently and the private sector better manage its risk. Government investigators are learning more about intrusion incidents, particularly those that succeed in compromising government systems. Private computer security experts have a more intimate knowledge about the numbers and severity of intrusions into corporate computers — the vulnerabilities exploited, the tools and techniques of intruders, and the damage caused by intrusion incidents. This information is currently unaggregated. Nowhere is there a complete picture of the true size, scope, and severity of a problem that could significantly impact national and economic security. With a limited system of reporting, one that respected complete client confidentiality, a more accurate picture of this problem could be developed. This information could be used operationally, by government or the private sector, as the basis for vulnerability advisories. It could provide the insurance industry with the actuarial data it needs to develop and refine currently scarce insurance protection. At the policy level, a more complete picture of threats and vulnerabilities would allow the government properly to manage its response, to consider appropriate changes to support criminal deterrence, and to facilitate investigations and prosecutions. It would create an avenue for policy development that truly is tied to the size and nature of the problem.

---

56. Although the Report of the President's Commission on Critical Infrastructure Protection found no current, imminent threat of a successful nation-state or terrorist attack sufficient to affect large portions of the United States or U.S. infrastructure, it nonetheless recommended initiation of a series of measures to promote the development of a protective environment. *See* THE PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE, CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURE (1997). In response, President Clinton issued Presidential Decision Directive 63, on May 22, 1998. *See* The White House, Office of the Press Secretary, *Fact Sheet: Summary of Presidential Decision Directives 62 and 63* (May 22, 1998) <http://http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1998/5/22/6.text.1>

V. UNANSWERED QUESTIONS

There are additional determinations likely to bear on the desirability or effectiveness of an oversight mechanism or authority. They involve, among other things, clarifying the scope and nature of the oversight mechanism and how participation or compliance might be enforced.

A. Who Should Be the Oversight Authority?

The principal unanswered question appears to be "who should do the licensing?" Is it a private sector or a governmental responsibility? If governmental, is it more appropriately performed at the state or federal level? Each of these options has advantages and disadvantages that can be examined effectively against the objectives of the oversight mechanism.

The private sector may offer advantages as a home for an oversight body, particularly for a profession so closely linked with sensitive private sector concerns. The ability of the private sector to influence and manage the oversight of investigative professionals may increase confidence, at least within the private sector, in those professionals' competence, qualifications, and sensitivity to concerns such as confidentiality and control of investigations.

In addition, a private board would avoid many of the bureaucratic pitfalls that may be encountered with government oversight at the state or federal level. However, a private oversight mechanism will have inherent limitations. Private bodies are not as well positioned as government to impose a mandatory licensing scheme. Most purely private professional groups offer only certifications or similarly limited forms of approval of qualifications for a profession. It is also not clear that a wholly private entity would be able to support the necessary functions attendant with licensing. Additionally, a private oversight mechanism may be reluctant (for liability-related or other reasons) to participate in many of the collaborative activities which would benefit law enforcement and government responses to the computer intrusion problem.

This is not to say that the private sector should not have a role in an oversight mechanism. In many traditionally licensed professions, oversight functions are conducted under the auspices of a state licensing board created and funded by the state government, but the board's participants are often members of the profession who also sit on a review panel. Clearly, peer review is an important aspect of any oversight scheme and could be incorporated at the state or federal level.

State governments have a long and distinguished history of licensing professionals to practice within their jurisdictions. States license doctors, lawyers, accountants, private investigators, and other professionals. While there is history of professional state licensing, problems are beginning to emerge. Many time-tested state licensing schemes are now strained, because many state licenses are effective only within the state in which they are granted. For example, to practice medicine or law within a state, a professional must either be licensed in the state, subject to a reciprocal agreement between their state of licensure and the state where he wishes to practice, or fit within narrowly circumscribed exceptions.[57] The limitations of these state-by-state licensing approaches are already being shown in professions not as intimately connected with the Internet (and other networked environments) as the computer security profession. State licensing schemes for medical doctors, for example, appear to be limiting the growth of "telemedicine," because a doctor often is not permitted to render a diagnosis on a patient located in a jurisdiction where the doctor is not licensed to practice. While technology may allow doctors, lawyers, or other professionals to practice in nearly every jurisdiction in the world, often at a reduced expense to clients, licensing requirements predicated on physical boundaries may prevent or severely restrict multi-jurisdictional practice.

Jurisdictional limitations also hamper state law enforcement officers in the investigation of computer crime. Intrusions are almost always multi-jurisdictional, even if the intruder and the victim are located next door to one another. Networks used to obtain access to a system usually cross physical and thus legal jurisdictions.[58] Because these jurisdictional complications apply with equal force to state-licensed professionals, they militate strongly against a state-level oversight mechanism for private computer security experts. Thus, in this respect, a centralized oversight mechanism is desirable.

While the federal government does not have as long and well-developed a history of licensing professions, federal licensing is not without precedent.[59] The Nuclear Regulatory Commission licenses

---

57. Such as when lawyers try a case *pro hac vice*.

58. These jurisdictional complications have placed much of the responsibility for investigating incidents on the federal government, which is currently struggling with jurisdictional issues relating to national boundaries. *See* discussion of international implications *infra* Part V.E.

59. In fact, new technologies may require some new thinking. A recent bill on the use of digital signatures proposed a certification scheme very similar to state licensing schemes, but to be implemented at a national level. *See* H.R. 2937, 105th Cong. (1997).

operators at nuclear power plants. The Food and Drug Administration licenses food inspectors. There are federal licenses for everything from nuclear-material transporters and security officers to pilots.[60]

B. Who Should Be Covered by the Oversight Mechanism?

The appropriate scope of an oversight mechanism will likely be dependent on its structure. The higher the bar to obtain a licence to perform intrusion investigations, the more appropriate a limited scope may be. There are many ways to define coverage. The oversight mechanism could apply to all computer security specialists, only to computer security specialists who respond to intrusion incidents by employing defensive mechanisms, or only to those who respond "offensively" to intrusion incidents by tracing and identifying intruders. It would be neither prudent nor necessary to create an oversight mechanism so broad as to cover large numbers of employees engaged in routine system security, system design, or system maintenance. Given that security specialists often work in teams, a determination must be made as to whether the license would attach to an individual, a company, or some subset of qualified employees. A determination must also be made as to whether the oversight mechanism applies only to those who perform such services for hire or also to those who perform such services only for their employer. The oversight mechanism's scope may also depend on its requirements, such as the amount of liability coverage required.

C. Should Oversight Be Mandatory or Permissive?

Another important determination that must be made with respect to an oversight mechanism is whether it should be permissive, allowing those who wish to take advantage of its features to opt in, or mandatory, applying to all those who fall within its determined scope. Most current licensing schemes are mandatory. They set a very high level of qualifications to meet the requirements for obtaining and keeping the professional license and do not allow those without the license to practice. Some even provide criminal or civil penalties for those who practice without a license or whose activities exceed its scope. This is true for doctors, lawyers and private investigators.

---

60. *See, e.g.*, 7 C.F.R. § 868 (1997) (food inspectors); 10 C.F.R. § 55 (1997) (NRC operator licenses); 10 C.F.R. § 71 (1997) (packaging and transportation of radioactive material); 10 C.F.R. § 95 (1997) (nuclear-facility security officer licenses); 14 C.F.R. § 61 (1997) (pilot licenses); 46 C.F.R. § 10 (1997) (licensing of maritime personnel).

By contrast, some professions make use of certification schemes that are permissive in nature. While employers may generally prefer to hire an employee with a certification, and while doing so may provide incidental liability or insurance incentives, they may accept a certain amount of education or experience as a suitable substitute. Whether a permissive or mandatory scheme is preferable may ultimately depend on the types of incentives offered licensed practitioners. Guarantees of confidentiality through privilege and limitations on liability would surely attract interested practitioners even if licensing were not made mandatory. But strict criminal prohibitions on practicing without a license could also achieve a similar result.

Although licensing offers a way to achieve a higher level of compliance with set standards of behavior, it also has the potential to drive what is already something of an "underground" practice even further below the surface. And given the difficulties already inherent in investigating criminal violations of computer crime laws, it may prove unwise to attempt to graft on top of the existing enforcement regime additional requirements to investigate and enforce mandatory licensing conditions.[61] The benefits that will flow to all parties — service providers, their customers, and government — will require participation and thus openness. A robust, open, and voluntary federal licensing scheme may be the best way to assure the availability of qualified and responsible professionals, while simultaneously encouraging them to abide by established procedures and standards of conduct.

D. Required Changes in the Law

Permitting private computer security experts to investigate intrusion incidents raises red flags for some people. Allowing the government to sanction such activity raises them for others. Is this legal? Our short answer is "yes." Many aspects of the concept detailed in this paper are based on long-standing practical and legal precedent. We may be accused of applying these precedents in new ways, but we do not believe they stretch past our understanding of current law.

Private investigations have been licensed activities for approximately fifty years and practiced for well longer. In the past, licensing was done at the state level. This paper raises as a policy option the propriety of a federal licensing scheme — one fully justified by the interstate nature of computer intrusions. These types of federal licensing schemes are not without precedent. Government agencies have adopted

---

61. *See supra* note 38 and accompanying text.

federal licensing techniques in several settings, including security and law enforcement, by agencies such as the Nuclear Regulatory Commission and by the Department of Agriculture.

Certain legal issues would have to be resolved in designing an oversight mechanism. The oversight function, if performed by the government, may need to be limited to ensure that the licensees will not be construed to be "agents" of the government and thus subject to the Fourth Amendment.[62]

Without the ability to go to a court and obtain a search warrant or intercept order, private response is more limited in what it is able to legally accomplish. In other respects, available civil mechanisms may provide latitude not available to the government. The question is then whether private computer security experts can do enough within the bounds of the law to make their services of use to their clients. The first and most obvious answer might come from observing the rapid growth of the profession today. Desirable services are being offered at levels that are sufficiently affordable such that demand for these services is still on the rise. Is it all being done illegally? We think not.[63]

---

62. Though private individuals are not subject to the Fourth Amendment and other laws restricting law enforcement activities, this does not mean that they are free to break into and search homes, offices, or computer systems. Rather than being subject to the procedural restrictions on law enforcement, private individuals are subjected to criminal and/or civil liability for breaking and entering, theft, assault, kidnaping or false imprisonment, battery, and other actions that are outside legal boundaries. Under some state licensing schemes for private investigators, committing such acts may be grounds for losing one's license or other disciplinary action. *See, e.g.*, IND. CODE § 25-30-1-18 (1993); NEV. REV. STAT. § 648.150 (1997); N.C. GEN. STAT. § 74c-10 to -12 (1989); OKLA. STAT. tit. 59, § 1750.7 (1989); S.C. CODE ANN. § 40-17-140 (Law. Co-op. Supp. 1997).

63. First, it bears noting that successful investigation of even high-tech crimes is often dependent on sound conventional investigative practices. Second, under existing law, there is still room for a private investigator to operate, although she is required to proceed cautiously, and frequently only with the consent of the parties involved.

We do not intend to suggest that there is no room for improvement in the current legal structure that governs networked environments. The laws that currently apply to computer networks are laws that were originally intended to apply only to telephone conversations. Over time they have been expanded in the breadth of their coverage to include computer networks, but the statutes themselves have not been substantially revised to account for differences in public expectations when communicating in networked environments. The evolution of this legal framework has not yet taken a turn to address more adequately and contend with the unique aspects of the Internet and other computer networks. This does lend a degree of ambiguity to the determination of what is legal in such an environment and what is not. This should not be seen as a barrier to erecting an oversight structure for computer security experts, but rather, such an oversight structure should be seen as an opportunity to create a context and an impetus

Finally, additional prosecutorial options may contribute to additional deterrence of computer intrusions. This may require expanding the availability of civil remedies to those who suffer intrusions. A robust private investigative response undoubtedly will contribute to the effectiveness of civil adjudicative functions, and vice versa. Both will serve the interest of enhancing deterrence.

E. International Implications

We have not studied in detail the comparative legal barriers that face public and private investigators operating through networks linked to foreign countries. But given that private parties, including private investigators, currently enjoy unfettered access to international networks and systems — access which, if performed by law enforcement for investigative purposes, may raise issues of international law — this area should be considered more thoroughly. We certainly would not want to see the activities of law enforcement or private parties interpreted by foreign powers as hostile acts.[64] These concerns — the need to exercise particular caution in investigations implicating computers in foreign nations — may provide yet another compelling reason to impose additional oversight and standards on the investigative portions of the computer security profession.

VI. CONCLUSION

As FBI Director Louis Freeh recently noted, the future of effective computer crime enforcement lies in the creation of workable partnerships.[65] We agree that a coordinated effort to clarify the roles of

---

for the reexamination of the laws in light of their new applications and possible outcomes.

64. For example, in the often-cited "Rome Labs" case, intruders into Air Force computers at Rome Labs in New York used the Air Force system as a vehicle by which to access a system called the "Korean Atomic Research Institute." The intruders copied material back to the Rome Labs system. U.S. officials had considerable cause for concern; they were not sure whether the Atomic Research Institute belonged to North or South Korea and did want the apparent intrusion by a U.S. Air Force computer to be considered an attack on the North Koreans. *See Air Force Investigative Office Deemed Incompetent During Rome Labs "Info-War" Break In*, CRYPT NEWSL., Jan. 1998 <http://sun.soci.niu.edu/~crypt/other/crpt46.htm>.

65. "Clearly these problems and issues cannot be solved unilaterally by law enforcement, no more than they could be solved unilaterally by the private sector. If we are to identify and respond to these various problems, we've got to unite the efforts of industry and law enforcement on an international scale." Louis J. Freeh, Director of the

the public and private sectors with respect to investigation and responsive legal action is warranted. We believe such a clarification could be done in a manner that is mutually beneficial to public and private interests. Professional licensing offers a novel venue for cooperation and compromise. And the debate that would accompany such a proposal will, regardless of the result, undoubtedly raise the level of awareness and depth of understanding of the gravity and complexity of the computer intrusion problem we face.

FBI, Speech at the 1997 International Computer Crime Conference (Mar. 4, 1997), *available at* <http://www.fbi.gov/dirspch/compcrim.htm>.