

Brief of article “Private Intrusion Response,” by Stevan D. Mitchell and Elizabeth A. Banker, *Harvard Journal of Law & Technology*, Summer 1998.

1. Private Intrusion Response

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 authority. 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.

The federal government has begun to equip itself to address an expected increase in the volume of computer intrusions, raising basic questions about the ability of federal law enforcement to effectively and efficiently resolve large numbers of incidents, but even if adequate resources are available – a questionable assumption – not all cases will be investigated, and not all will be prosecuted (an example is the “Rome Labs” case, where the U.S. government’s investigation was deemed inadequate by the United Kingdom courts, who refused to prosecute the suspect.) The response typically pursued by law enforcement is geared toward identifying, apprehending, and prosecuting the intruder, which this is not necessarily consistent with the objectives of a corporation that has been the victim of a serious incident.

Businesses have a primary need to repair the 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.

Statutory civil remedies are in place at the state and federal levels, though they are seldom pursued. Contract and tort remedies have been proposed as potential vehicles for settling disputes between private parties for unauthorized use of systems. However all of these alternatives are dependant on identifying the source of the intrusion – identification that must be sought through an investigative 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.

2. Convergent Trends, Diverging Responsibilities

a. Potential Growth of Computer-Related Misconduct

There has been little or no discussion about contributions that could be made through the formalization of the resources that are already trained and equipped to work within the private sector.

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

A. Difficulties in Detection

Less than one in ten successful computer intrusions are detected.

B. Limited Reporting

About 11% to 17% of intrusions are reported to law enforcement. Victims may fear media attention, loss of control over resources dedicated to an investigation, or they may wish to retain control over the remedies sought.

C. Jurisdictional Complexities

In an increasingly networked world, it is increasingly likely that an intruder would enter at least one foreign system, perhaps even without knowing it. This situation usually demands some level of involvement by federal law enforcement in the investigation.

The legal measures being contemplated to ease the jurisdictional impediments 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.

D. Resource Constraints

Whereas a typical (non-“high tech”) state or local law enforcement officer may carry between forty and fifty cases, a high-tech investigator has a full-time job handling three or four cases a month. Compare this with the figures of 1 in 10 intrusions being detected, and roughly one tenth of those being reported, and the implications

of building an effective response proportional to the problem is apparent.

c. State of the Law

The Computer Fraud and Abuse Act (“CFAA”) prohibits a range of activities involving unauthorized access to protected computers. 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. Prohibitions of the Electronic Communications Privacy Act (“ECPA”) may similarly restrict private intrusion response while placing carefully circumscribed conditions on law enforcement access to protected forms of communication. 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. 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 laws 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 and in 1994 the CFAA was amended to include a federal civil remedy.

d. Law Enforcement Capabilities

Law enforcement techniques and capabilities appear to be improving at the state, local, and federal level, however these capabilities come at considerable cost and are inherently limited in their ability to provide confidentiality.

e. Private Sector Capabilities

At the same time as law enforcement capabilities are increasing, the private sector response is growing very rapidly. Businesses who provide intrusion response services range in size, and go from local to nation-wide in their scope. Some maintain procedures to insure trustworthiness and accountability, while others primarily emphasize results. Some appear acutely aware of the limitations placed on their activities by current law – civil and criminal – and conduct their business accordingly, while others are likely unaware of the potential implications of certain legal provisions, while yet others may even use their willingness to disregard current law to their competitive advantage. (In instances where private investigative practices 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.)

3. A Call for a Balanced Public/Private Approach

a. What the Industry Would Need from an Oversight Mechanism

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 and many other states protect client information from disclosure by law.

It is not uncommon for clients to conduct 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. Civil remedies are available through federal and state law, for example.

b. Oversight Options

A. Licensing

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. It is generally quite clear to those obliged 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.

A licensing body, however, has the corresponding disadvantage of requiring a fairly elaborate bureaucracy.

More than forty states currently have mandatory licensing schemes for private investigators. 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. 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.

B. Certification

To receive certification, an applicant may be required to take a prescribed set of courses, or even to pass an exam.

4. Fertile Ground for Compromise

a. What the Industry Could Get from an Oversight Mechanism

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 from a clarification of the substantive laws, such as the CFAA and ECPA. 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.

Standard, defined liability, and education and training criteria would all contribute to the trust placed in a computer security expert.

b. What the Government Could Get from an Oversight Mechanism

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.

We merely suggest that 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.

They can (and do currently) loan valuable technical expertise to law enforcement in complex computer 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.

c. What the Public Could Get from an Oversight Mechanism

Security specialists 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.

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.

d. Long Term Benefits of a Cooperative Environment

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 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. 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 national emergencies 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. Nowhere is there a complete picture of the true size, scope, and severity of a problem that could significantly impact national and economic security. 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.

5. Unanswered Questions

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. 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. (E.g., Private bodies are not as well positioned as government to impose a mandatory licensing scheme; Purely professional groups offer only certifications or similarly limited forms of approval of qualifications; A wholly private entity may not be able to support the necessary functions attendant with licensing; A private oversight mechanism may be reluctant, for liability or other reasons, to participate in many of the collaborative activities which would benefit law enforcement and government responses.)

In many traditionally licensed professions, oversight functions are conducted under 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.

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. The limitations of these state-by-state licensing approaches have already been shown. State licensing schemes for medical doctors, for example, appear to be limiting the growth of "telemedicine," because a doctor is often not permitted to render a diagnosis on a patient located in a jurisdiction where the doctor is not licensed to practice.

Because these jurisdictional complications apply with equal force to state-licensed professionals, they militate strongly against a state-level oversight mechanism for private security experts. Thus, in this respect, a centralized oversight mechanism is desirable.

The federal government does not have as long and well developed a history of licensing professions, but federal licensing is not without precedent (e.g, the Nuclear Regulatory Commission licenses operators of nuclear power plants, and the Food and Drug Administration licenses food inspectors.)

a. Who Should be Covered by the Oversight Mechanism?

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. 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 services only for their employer.

b. Should Oversight be Mandatory or Permissive?

Most current licensing schemes are mandatory. They set a very high level of qualifications to meet the requirements of obtaining and keeping a license and do not allow those without a license to practice. Some even provide criminal or civil penalties for those who practice without a license or whose activities exceed its scope.

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.

Although licensing offers a way to achieve a higher level of compliance with set standard of behavior, it also has the potential to drive what is already something of an “underground” practice even further below the surface. 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.

c. Required Changes in the Law

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

The oversight function, if performed by the government, may need to be limited to ensure that the licensees will not be considered to be “agents” of the government and thus subject to the Fourth Amendment.

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.

A robust private investigative response undoubtedly will contribute to the effectiveness of civil adjudicative functions, and vice versa. Both will serve the interests of enhancing deterrence.

d. International Implications

We certainly would not want to see the activities of law enforcement or private parties interpreted by foreign powers as hostile acts. 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. (An example of this is the Rome Labs case, where intruders used an Air Force system as a vehicle by which to access a system at the “Korean Atomic Research Institute.” The intruders copied material back to Rome Labs. 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 not apparent intrusion by a U.S. Air Force computer to be considered an attack on the North Koreans.)

6. Conclusion

We believe that a coordinated effort to clarify the roles of the public and private sectors with respect to investigations 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.