;login:

THE MAGAZINE OF USENIX & SAGE

June 2003 • volume 28 • number 3

inside:

THE LAW

Put Your Data Where Your Mouth Is

by Erin Kenneally

USENIX & SAGE

The Advanced Computing Systems Association &
The System Administrators Guild

put your data where your mouth is

Public-Private Partnership Begins with Reporting Cybercrimes

by Erin Kenneally

Erin Kenneally is a Forensic Analyst with the Pacific Institute for Computer Security (PICS), San Diego Supercomputer Center. She is a licensed attorney who holds Juris Doctorate and Master of Forensic Sciences degrees.

erin@sdsc.edu

Society has developed a love-hate relationship with the concept of "sharing" security data. On the one hand, sharing has been a rallying cry for combating cyberterrorism, but it is also bemoaned by corporate financiers to justify a protectionist mentality that sees "sharing" as Big Brother wrapped in sheep's clothing. This article illustrates the ideas of "sharing security data" and "public-private partnership" in hopes of motivating others to move beyond the current holding pattern of cyber-infrastructure needs assessment and into a strategy for securely grounding our structures in response to the dangers of cyberspace.

The San Diego Chapter of the High Technology Crime Investigation Association (HTCIA), a grassroots organization founded to share information relating to investigations and security, has developed "Working with Law Enforcement to Abate Cybercrime." These guidelines are a proactive attempt by law enforcement to communicate elements of policies, incident response plans, and evidence handling procedures that are vital to the effective identification, prosecution, and prevention of cybercrime, as well as infrastructure protection.

THE HTCIA GUIDELINES ARE IN PRINT AND AVAILABLE FROM THE AUTHOR AT *erin@sdsc.edu*. THEY CAN ALSO BE DOWNLOADED FROM *http://www.catchteam.org* OR *http://security.sdsc.edu*

Motivation for Sharing Data Between the Public and Private Sector

The HTCIA Guidelines resulted from a desire to enable the private sector cybercrime victims to communicate clearly with law enforcement. All too often, law enforcement is called onto a cybercrime scene – whether it be a hacker intruding on a company's network, denial of service attack, theft of intellectual property, discovery of child pornography, or insider abuse of privileges – only to find inadequate or nonexistent policies and procedures for handling cybercrime incidents, which prevents investigators from tracking and punishing the digital perpetrator. Corporate victims often wanted to know how to ready the cybercrime scene for optimal law enforcement.

National Strategy to Secure Cyberspace

The recently released "National Strategy to Secure Cyberspace" has been the most popularly recognized call for a public-private partnership and sharing of threat data. However, it has been criticized as not doing enough to hold responsible parties' "feet to the fire" in attempting to secure cyberspace. The Strategy is a framework of suggestions rather than a regulation, so it has few real teeth.

Computer Crime Laws

The need to share data is underscored further by the fact that there are laws in existence that criminalize both unauthorized access to computer systems and exceeding access privileges. There is a misperception that just because most laws targeting the security of computer data congregate around specific business practices within select industries (i.e., HIPPA for the health-care industry and GLBA for banking and finance institutions), there is a dearth of criminal remedies that the private sector can utilize to address cybercrime. On the contrary, the federal Computer Fraud and Abuse Act, as well as its state counterparts, can be a remedy for industry, with one caveat: In order to invoke it, victims of cybercrime must first report the incident to law enforcement. We have been conditioned not to think twice about hailing the cops when someone breaks into our safes or assaults one of our employees at the work site, yet the same knee-jerk reaction to an insider breach of access control or external trespassing on our networks does not occur frequently enough.

The possibility of bad publicity has been used to justify sweeping cybercrime incidents under the rug.

Countering Myths About Sharing Cybercrime Data

Corporate Reputation

The possibility of bad publicity has been used to justify sweeping cybercrime incidents under the rug. Companies can, however, communicate concerns about confidentiality and the desire to minimize publicizing the incident. This will not ensure that this information will never become public if prosecution occurs, but it can lengthen the amount of time until this information is subject to public accessibility and give your organization time to craft a strategy that minimizes potential negative publicity. Additionally, the government recently announced FOIA exemptions for companies wishing to share related cybercrime data.

If public embarrassment and the assumed detrimental effects on business profitability are concerns, consider the bad public relations ramifications of failing to report incidents in the current culture of increasing litigation and the call for disclosure spurred by Enron and security broker scandals. Often, the hint of impropriety or cover-up is enough to send stock plummeting or scare away potential clients and partners.

Some states may choose to follow California's lead in enacting laws that require the disclosure of security breaches that expose customers' personal data. So, whether it is through market or regulatory mechanisms, the costs of not reporting may ultimately be more ominous than what appears on the surface. Furthermore, publicity can sometimes work to your advantage, as companies can distinguish themselves as taking a leadership role by reporting and setting a standard for others to follow.

Notification of cybercrimes to authorities does not obligate victims to participate in the investigation. However, lack of participation may affect successful legal remedies.

Cost of Not Reporting Cybercrime

Another excuse is the notion that reporting cybercrime and pursuing prosecution is cost prohibitive. In other words, it is cheaper to eat the loss and not disrupt the business process. It is prudent to assess the cost of not reporting, too. The mechanisms advocated here should be consistent with the mechanisms that should already be part of your organization's strategy to deal with cybercrime in-house. The Guidelines address the relevant security risks and obligations that you must know to effectively meet your responsibility to your investors, partners, clients, and customers.

Additional costs for evidence-handling and the like should be minimal, since most procedures are similar to what companies should have implemented already. The costs associated with the potential liability (negligence, shareholder suits, regulatory noncompliance) make sharing less ominous. Furthermore, the costs of complying with potential future regulation created by the corporation's lack of reporting will likely equal or exceed the costs of implementing the current recommendations.

High-Tech Crime Fighters

Another misperception used to justify failure to report is that law enforcement is technically ill-equipped to effectively resolve cybercrime. State and federal agencies have teamed up all across the country to establish high-technology task forces whose sole mission is to investigate and prosecute cybercrime. California is a leading example, where the state has six regional teams made up of investigators from local, state, and federal agencies that are specifically trained to handle everything from kiddie porn traders to identity thieves to high-level hackers and corporate espionage. Unless victims call upon their services, funding to support and expand this cadre of skilled investigators will dry up. With a more concerted effort to report cybercrime, we increase the likelihood of laws that place fewer restrictions on cybercrime investigations under the rubric of national security. So, sharing cybercrime incidents may actually facilitate the protection of civil liberties and privacy.

Cyberinsurance and Risk Management

Actuarial data is another motivation for sharing cybercrime incidents. Without reporting, we cannot quantify the incidence of cybercrime. Obtaining actuarial data related to the incidence of cybercrime is relevant to your organization if you are at all concerned with risk management. From a systemic level, the more accurate the data on cybercrime, the more accurate the assessment of risk. Cyberinsurance will almost certainly become as ubiquitous as automobile insurance and is another tool for management of information security.

Without reporting, we cannot quantify the incidence of cybercrime.

Damages and risk factors are difficult to measure and are often exaggerated [CSIS 2000 – Center for Strategic and International Studies, *Cyber Threats and Information Security: Meeting the 21st Century Challenge*]. Actuarial data grounded in reported incidents of cybercrime will enhance the accuracy of probability-of-loss estimates and premium pricing.

HTCIA Public-Private Guidelines

Below is an abbreviated outline of the HTCIA Guidelines:

I. INFORMATION SECURITY POLICIES

A. DEFINITION PHASE

1. Roles and Responsibilities, Personnel Who Deal with Law Enforcement (LE)

    a. Establish two points of contact (POC) – one security/technical and one legal/senior administrative.
    b. Educate and integrate designated POCs into LE and prosecutorial agencies and high-technology associations to establish trust relationships (i.e., HTCIA, Infragard).
    c. Designate chain-of-command regarding authority to control investigation and report to LE.
    d. Define who a "user" is for application of the Acceptable Use Policies.

2. Privacy Expectations

    a. Define scope and coverage in order to inform users of the when, where, why, and what regarding expectations of privacy, enabling companies to deal with violations properly.
    b. Establish organization ownership of computer facilities (hardware, software, data, communication devices).
    c. Establish that use of computer facilities should be work-related and the scope of use should be duty-related.

3. Define Acceptable Use Policies

4. Define What Constitutes an “Incident” for Application of Policies

5. Define and Document Incident Response Plan

    a. Examples of reportable computer crimes
        i. Actual intrusion into system circumventing access controls
        ii. Exploiting vulnerable programs
        iii. Denial-of-service attacks
        iv. Theft of bandwidth
        v. Exceeding authorized access
        vi. Child pornography storage or transmission
        vii. Theft of intellectual property or trade secrets
    b. Examples of incidents better resolved internally or under civil law rather than by LE

6. Define Consequences of Non-Compliance (reserving the right to institute penalties, including criminal prosecution)

B. Documentation Phase

1. Document Policies

    a. Obtain acknowledgment via click-thru forms on the Web that evidence acknowledgment of policies.
    b. Obtain signature evidencing user understanding and pledge to abide.
    c. Include policy language stating that the company reserves the right to change the policy, and the user is obligated to regularly visit a clearly demarcated location where policies are accessible.

2. Document Audit Policy and Audit Logging

3. Document Incident Cost Model

    a. Document policies and procedures for collecting measurable loss data in response to computer security incidents
        i. Replacement of hardware, software, or other property that was damaged or stolen.
        ii. Lost productivity by users who were unable to use systems during relevant time period.
        iii. Time spent by all staff to clean up the damage to systems under your control (e.g., analyzing what has occurred, re-installing the operating system, restoring installed programs and data files, etc.).
        iv. Who worked on responding to or investigating the incident.
        v. Indirect costs: any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service (must have methodology and reasonable justification for calculation).

C. Dissemination Phase

II. IMPLEMENTING AND ENFORCING POLICIES

A. Incident Response Checklist

1. Pre-Incident Planning

2. During Suspected Incident

3. Post-Incident: What Law Enforcement Needs to Investigate (reactive mode)

   a. Preserve all relevant logs on all systems (i.e., Web logs; Intrusion Detection System (IDS); firewall; mail logs).
   b. Obtain name list of all users, new hires, and terminated users within past six months.
   c. Identify all network access points (trusts granted to other networks): Internet gateways, VPNs, LAN/WAN connections.
   d. If dealing with an intrusion from outside the company, and if you have trained in-house security response capabilities, exhaust all methods of intraoffice security investigations in tracing back prior to contacting law enforcement.
   e. Collect copies of complaints sent to organization during timeframe of incident.
   f. Calculate time offset (including time zone) of all affected computers.
   g. Collect copies of badge/entry logs, security cameras, etc. for internal incident.
   h. Identify all correspondence with external organizations/ individuals, especially foreign to the United States.
   i. Preserve forensic image(s) or actual drives from compromised system (law enforcement can supply media and manpower for image). (See D, below, Evidence Recovery and Handling).

4. Notify Law Enforcement

   a. Notification should generally be made immediate on the discovery of a suspected violation. However, you may choose to have skilled and trained staff conduct a forensically sound internal investigation prior to calling in LE. The advantage here is that you may be able to obtain certain evidence more efficiently, yet still within the bounds of the law, than when LE is involved.

NOTE: Notification does not obligate you to participate in the investigation. However, lack of participation may affect successful legal remedies.

5. Questions that LE Will Likely Ask When You Make the Complaint

   a. What evidence do you have that you were victimized?
   b. What is the chronology of the event?
   c. What is the impact to your network?
   d. Are your systems still running?
   e. When did the incident first occur?
   f. When was the incident discovered?
   g. Who discovered the incident?
   h. Is the activity ongoing?
   i. Who do you think is responsible for the incident and why do you suspect them?

j. What is the internal or external IP address for the attacker?
k. Can you provide a complete topology of your network?
l. Who in the organization has been notified?
m.Who outside the organization has been notified?
n. From this point forward, who does law enforcement contact and who can they speak to if they are contacted?
o. What are your estimated damages?

B. Evidence Recovery and Handling Guide

Once the nature of the incident has been defined, the next step is to identify where data relevant to the incident may reside. The steps taken to identify the incident, which may have a forensic impact, need to be completely documented.

Additionally, the decision whether to secure and maintain evidence should be factored into your organization's risk analysis. This is a cost-benefit analysis that should consider the short- and long-term economic consequences of keeping log data, including the effect on potential civil and criminal legal actions. Even if no legal action is taken, organizations may want to consider maintaining logs for a limited amount of time in accordance with document retention policies.

1. Essential Elements to Evidence Recovery and Handling

    a. Identification of relevant data
    b. Isolation of evidentiary data
        i. Considerations – once data is identified, relevant systems should be secured to avoid possible contamination of digital evidence.
        ii. Partial or complete system analysis (copy of relevant logs, logical image of media, physical image of media).
        iii. Real-time backup of data to remote location in accordance with data retention model and policies.
    c. Preservation of evidentiary data
    d. Resources that should be considered

Proper evidence recovery and handling requires specialized forensic tools and training. The resources available may be internal (IT, Security), external (private consultants), and law enforcement.

Conclusion

Our increasing dependence on technology has enhanced business functionality and productivity while simultaneously exposing our organizations to more frequent and severe threats. Securing organizations demands better cooperation with law enforcement, which provides critical and unique information services beyond the capabilities of any one organization.

The HTCIA Guidelines are intended to help victims of cybercrime more effectively interact with law enforcement so that the goals of both entities are better served and to advance public-private cooperation by identifying essential elements of an organization's policies, incident response plans, and electronic evidence-handling procedures that will meet the goals of both your organization and law enforcement. Without more victims working with law enforcement to track down cybercriminals, we cannot expect to abate the frequency and severity of cyber threats.