ICSA White Paper on Computer Crime Statistics

by M. E. Kabay, PhD, CISSP
Director of Education, ICSA

Introduction

ICSA staff members are often asked about computer crime; for example, customers want to know who is attacking which systems how often using what methods. These questions are important because they bear upon the strategies of risk management; in order to estimate the appropriate level of investment in security, it is helpful to have a sound grasp of the probability of damage and the magnitude of damage. Ideally, one would want to compare one's level of risk by evaluating the experiences of other organizations with similar system and business characteristics.

Although we hate to sound negative, it is unfortunately impossible to give reliable answers to such questions. Information security experts understand that there are two fundamental difficulties preventing us from giving accurate statistics of this kind. These difficulties are known as the problem of ascertainment.

The first problem is that an unknown number of crimes of all kinds are undetected. For example, even outside the computer crime field, we don't know how many financial frauds are being perpetrated. We don't know because some of them are not detected. How do we know they're not detected? Because some frauds are discovered long after they have occurred. Similarly, computer crimes may not be detected by their victims. In a landmark series of tests at the Department of Defense, the Defense Information Systems Agency found that very few of the penetrations it engineered against unclassified systems within the DoD seem to have been detected by system managers. A commonly-held view within the information security community is that something like only one-tenth or so of all the crimes committed against and using computer systems are detected.

The second problem is that even if attacks are detected, it seems that few are reported. This belief is based in part on the unquantified experience of information security professionals who have conducted interviews of their clients; it turns out that only about ten percent of the attacks against computer systems revealed in such interviews were ever reported to any kind of authority or to the public. The Department of Defense studies mentioned above were consistent with this belief; of the few penetrations detected, a very small number were reported to appropriate authorities.

Given these problems of ascertainment, computer crime statistics should generally be treated with scepticism. Generalizations in this field are difficult to justify; even if we knew more about types of criminals and the methods they use, it would still be difficult to have the kind of actuarial statistic that is commonplace in the insurance field. It is very difficult to compare the attributes of a mainframe-based network running MVS to the kinds of risks faced by the UNIX-

based intranets.

Under these circumstances, ICSA staff should be very careful not to give customers the impression that we know more than we do. In the following sections, the ICSA Research, Outreach, Strategy and Engineering Group offer our best guesses about what's actually happening in computer crime.

There is hope, however. The ICSA is actively working with ISPs in the United States to develop a database of incident details that will help answer some of the questions we all need to understand. Over the next several months, the ICSA expects to issue interim reports summarizing the findings of this ongoing research project. Look for the first reports by 3Q1998. What kinds of damage do computer systems suffer?

Information systems can be damaged in many ways. For example, an unauthorized person can breach the confidentiality of records stored by information systems. Someone can steal information and by that fact alone reduce our control over what is done with such information. An example of such a breach of control and possession occurs when people make illegal copies of copyrighted software, putting their employers at risk of serious lawsuits and criminal prosecution. The integrity of our information can be damaged; for example when vandals modify the appearance and content of corporate web pages, the victims are suffering a breach of data integrity and may lose credibility in the marketplace. Sometimes intruders use the identity of users on the systems they penetrate; this kind of breach of authenticity can result in serious problems when, for example, the forgers send fraudulent and frequently messages in their victim's names. Sometimes, attackers choose to reduce the availability of computer systems; some denial of service attacks have involved complete saturation of the victims' resources. In one spectacular case in 1996, someone flooded the mailboxes of over a hundred people with thousands of spurious e-mail messages. Another kind of problem caused by a mistake or on purpose is a breach of utility. For example, some disgruntled employees have been known to encrypt valuable documents such as source code before they leave their former employers; in other cases, people just honestly forget their decryption keys. Although the information is still intact, it's not useful until the decryption key is found.

What are the most common methods of attack?

Some deliberate attacks on systems start with non-technical methods. So called "social engineering" techniques take advantage of inadequately trained employees. For example, requests by phone for passwords or new computer accounts are easy for any junior hacker to make but should never be granted. Seduction or bribery of employees to reveal confidential matters or to steal confidential information require no very great technical knowledge but can be made more difficult by adequate employee security-awareness programs.

Successful technical attacks on computers and networks usually seem to use weaknesses that have been well documented and that ought to have been fixed. System managers and network administrators must keep their systems software up to date by installing all appropriate patches issued by their operating-system and security-software vendors.

The Computer Emergency Response Team Coordination Center (CERT-CC) has a number of publications summarizing what has been reported to them; see their Web site at

<http://www.cert.org/pub/reports.html> for free access to these documents.

John D. Howard published a valuable analysis of CERT-CC data from 1989 to 1995 that will interest those who want a broad overview of the kinds of attacks noted by the agency <http://www.cert.org/research/JHThesis/index.html>.

The 1996 Annual Report <http://www.cert.org/pub/annual-reports/cert_rpt_96.html> made the following key points about the most serious problems they encountered:

- Exploitation of weaknesses in the "cgi-bin/phf" program used on Web servers to steal system password files;
- Attacks on systems running the free Linux version of UNIX, including installation of "sniffers" that can steal unencrypted passwords when people log on to the systems
- Denial-of-service attacks were particularly troubling for Internet Service Providers;
- Widely-available hacker kits have permitted even novices to attack systems with known vulnerabilities;
- Poorly-configured anonymous FTP sites were used to exchange illegal copies of proprietary software;
- Abuse of e-mail included mail-bombing, forgeries ("spoofing") and a large increase in the amount of junk e-mail ("spamming");
- Viruses and hoaxes about viruses (especially wild claims about dangerous e-mail) increased in 1996.

What market sectors are most likely to be attacked?

Because of the poor state of reporting of attacks on computer systems and networks, we don't really know much in detail about who gets attacked the most. However, it certainly looks like Web sites of all descriptions are appealing targets for cyber-vandals. At the ICSA, we routinely see dozens of sites attacked every week -- and we are pretty sure this is just the tip of the proverbial iceberg. Another appealing target for cyber-thieves seems to be any organization with lots of credit-card numbers. In general, to be concerned about the safety of any organization whose information has monetary value to others.

What kind of data are being stolen?

In addition to credit card numbers, there have recently been some high-profile cases of industrial espionage, in which valuable proprietary data have been stolen either by competitors or for sale to competitors of the victim.

Who are the perpetrators of the attacks?

Judging from the participants in public hacker meetings, many of the potential criminals are relatively young people; however, some recent computer criminals have been people in their

thirties. Not much is known about the personality profiles, although there have been speculation of articles published over the years about what kinds of personality traits such people might display. Although the level of writing Ian hacker publications such as Phrack and twenty-six hundred seems uniformly immature, there is no way of knowing how representative such authors are of the broader hacker population. There may be differences in the personality profiles of American hackers and European hackers, although there are no definitive studies of this matter; rumor has it that European hackers tend to be more politically motivated than American hackers. An interesting glimpse into the minds of some hackers comes from a video made by Annaliza Savage called Unauthorized Access <http://www.bianca.com/bump/ua/>.

There have been several popular books published recently dealing with the computer underground. Nobody knows whether the people profiled in these books fairly represent the hacker population at large. Nonetheless, the books are interesting and may be helpful for perspective in discussions of computer crime.

For further reading

Fialka, J. J. (1997). *War by Other Means: Economic Espionage in America*. W. W. Norton (New York). ISBN 0-393-04014-3. xiv + 242. Index.

Goodell, J. (1996). *The Cyberthief and the Samurai: The True Story of Kevin Mitnick -- and the Man Who Hunted Him Down*. Dell (New York). ISBN 0-440-22205-2. xix + 328.

Hafner, K. & J. Markoff (1991). *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. Touchstone Books, Simon & Schuster (New York). ISBN 0-671-77879-X. 368. Index.

Kabay, M. E. (1996). *The ICSA Guide to Enterprise Security: Protecting Information Assets*. McGraw-Hill (New York). ISBN 0-07-033147-2. xii + 388 pp. Index.

Kabay, M. E. (1996). *The InfoSec Year in Review 1996.* <http://www.icsa.net/library/isecyir.html>

Kabay, M. E. (1997). *The InfoSec Year in Review 1997*. <http://www.icsa.net/library/iyir.html>

Littman, J. (1996). *The Fugitive Game: Online with Kevin Mitnick--The Inside Story of the Great Cyberchase*. Little, Brown and Company (Boston). ISBN 0-316-5258-7. x + 383.

Shimomura, T. & J. Markoff (1996). *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw--by the Man Who Did It*. Hyperion (New York). ISBN 0-7868-6210-6. xii + 324. Index.

Slatalla, M. & J. Quittner (1995). *Masters of Deception: The Gang that Ruled Cyberspace*. HarperCollins (New York). ISBN 0-06-017030-1. 225 pp.

Smith, G. (1994). *The Virus Creation Labs: A Journey into the Underground*. American Eagle Publications (Tucson, AZ). ISBN 0-929408-09-8. 172 pp.

Sterling, B. (1992). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*.

Bantam Doubleday Dell (New York). ISBN 0-553-08058-X. xiv + 328. Index.

Stoll, C. (1989). *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. Pocket Books (Simon & Schuster, New York). ISBN 0-671-72688-9. viii + 356.

Winkler, I. (1997). *Corporate Espionage: What it is, why it is happening in your company, what you must do about it*. Prima Publishing (Rocklin, CA). ISBN 0-7615-0840-6