FINAL

BEST PRACTICES FOR LAW ENFORCEMENT INTERACTION WITH VICTIM-COMPANIES DURING A CYBERCRIME INVESTIGATION

Prepared by the G8's Subgroup on High-Tech Crime
June 17, 2005

This Best Practices document was developed by the G8's Subgroup on High-tech Crime to help guide prosecutors and investigators in their interactions with victim-companies during an investigation of a computer incident.

While cybercrimes such as the destruction or theft of data, interruption of network services, or compromise of network integrity often harm individuals, the effects of such unlawful activities on companies is particularly pernicious. Computer information systems are essential to the everyday operation of businesses, and the disruption of services provided by those systems can seriously hamper a company's performance. Furthermore, since the majority of the information systems targeted by cybercrime are owned by private companies, businesses disproportionately bear the brunt of cybercrime.

When conducting a cybercrime investigation involving a victim-company, law enforcement should consider the measures outlined below, while being mindful that victim-companies may themselves be involved in related criminality. These procedures are intended to:

- Improve the likelihood of conducting a successful investigation by helping to establish a trusted relationship with victim-companies, thereby improving the quality of cooperation provided by victim-companies;

- Help investigators to better safeguard victim-companies by reducing the likelihood that an investigation will exacerbate the damage already suffered by victim-companies; and

- Help law enforcement establish procedures for obtaining efficient and timely assistance from victim-companies.

1. Minimize the disruption to a victim-company's normal business operations.

Law enforcement should weigh countervailing considerations as it plans to implement investigative measures that may disrupt business operations. Where there is a choice between disruptive investigative measures and equally effective, less disruptive measures, law enforcement should always opt for the latter. Law enforcement should make every effort to use investigative measures that minimize computer downtime and

displacement of a victim-company's employees. While some investigative measures that may inconvenience a victim-company are unavoidable, some less important measures may needlessly aggravate or prolong the damage already suffered by a victim-company. For example, rather than seizing compromised computers and depriving a victim-company of their use, law enforcement should consider creating a "mirror image" of the system or part of the system and leaving the original computers in place.

2. Coordinate the release of any information to the news media about the investigation. Investigations and prosecutions of cybercrime cases may entail the voluntary release of information to the news media by law enforcement (e.g., in a press release or at a press conference). Where possible, public statements to the news media should be coordinated with victim-companies where information that is potentially harmful to that victim-company may be released. Of course, law enforcement and justice officials should take all possible measures to prevent unauthorized releases of information about a pending investigation and to seek sanctions against those who make unauthorized disclosures.

3. Work closely with victim-companies on issues that will have an impact on sentencing. In many instances, it will be important to quantify the damage suffered by the victim-company as a result of a cybercrime. An accurate assessment of damages may be needed to satisfy the legal elements of an offense or to ensure that the punishment meted out at sentencing adequately reflects the damage suffered by the victim-company. It will be difficult to obtain a realistic assessment of the damage caused to a business and its productivity and to quantify the company's costs of remediating the damage without receiving significant assistance from the victim-company.

4. To the extent possible, regularly update the victim-company on the progress of the investigation. After the initial onsite investigation is conducted, law enforcement may have little direct contact with a victim-company. To the extent possible (and without jeopardizing any aspect of the investigation), law enforcement should inform victim-companies of the general progress of the investigation. If an arrest is made that results in court proceedings, notify the victim-company of all significant court dates, so it has the opportunity to attend.

5. Consult with the victim-company's information technology staff about network architecture before implementing investigative measures on the network. It is difficult to implement some investigative measures on a victim-company's network without first consulting with individuals in the company who are knowledgeable about the architecture of the company's network. It is usually advantageous to work closely with the information technology staff at a victim-company to obtain critical information about network topology, the type and version of software being run on the network, and any vagaries of the network, in order to minimize disruption of or damage to the

company's network. Be mindful, however, that victim-companies can themselves be involved in the criminality under investigation; before government officials coordinate investigative activities with a victim-company, they should have confidence that the company is not a culpable party.

6. Be aware that you may need to consult with a victim-company's senior management before undertaking intrusive investigative measures on the company's network. It is not always apparent who within a company has the authority to make binding commitments to law enforcement or to consent on behalf of the company to investigative measures that will affect the operation of the company's network. Law enforcement will often deal directly with a company's system administrator following a report of a cybercrime incident. However, system administrators may lack the authority to give the company's consent to law enforcement activity on the company's network that will affect business operations. Be aware that some decisions may require the authorization of a company's senior management and be prepared to consult with the appropriate persons at the appropriate level within the company's management structure.

7. Encourage ongoing relationships with businesses before an incident occurs. While a strong working relationship can be built between a victim-company and investigators during the course of a cybercrime investigation, it is preferable to have already established a relationship with a company before it is the victim of a cybercrime. Many companies are reluctant to report cybercrime incidents to law enforcement because they are fearful that law enforcement will conduct an investigation in a manner harmful to their business interests or because they have misconceptions about how law enforcement will conduct an investigation. Such fears and misconceptions can more easily be dispelled if law enforcement has a pre-existing relationship with a victim-company. For example, conducting presentations for trade associations on investigative procedures or forming liaison groups comprised of law enforcement and private industry representatives can help bridge the gap of mistrust or unfamiliarity and increase cybercrime reporting by private industry.