Cybersecurity Unit
Computer Crime & Intellectual Property Section
Criminal Division
U.S. Department of Justice

1301 New York Avenue, N.W., 6th Floor, Washington, D.C. 20530 - CYBERSECURITY.CCIPS@USDOJ.GOV - (202)514-1026

Best Practices for Victim Response and Reporting of Cyber Incidents

Version 1.0 (April 2015)

Any Internet-connected organization can fall prey to a disruptive network intrusion or costly cyber attack. A quick, effective response to cyber incidents can prove critical to minimizing the resulting harm and expediting recovery. The best time to plan such a response is now, *before* an incident occurs.

This "best practices" document was drafted by the Cybersecurity Unit to assist organizations in preparing a cyber incident response plan and, more generally, in preparing to respond to a cyber incident. It reflects lessons learned by federal prosecutors while handling cyber investigations and prosecutions, including information about how cyber criminals' tactics and tradecraft can thwart recovery. It also incorporates input from private sector companies that have managed cyber incidents. It was drafted with smaller, less well-resourced organizations in mind; however, even larger organizations with more experience in handling cyber incidents may benefit from it.

I. Steps to Take *Before* a Cyber Intrusion or Attack Occurs

Having well-established plans and procedures in place for managing and responding to a cyber intrusion or attack is a critical first step toward preparing an organization to weather a cyber incident. Such pre-planning can help victim organizations limit damage to their computer networks, minimize work stoppages, and maximize the ability of law enforcement to locate and apprehend perpetrators. Organizations should take the precautions outlined below before learning of a cyber incident affecting their networks.

A. Identify Your "Crown Jewels"

Different organizations have different mission critical needs. For some organizations, even a short-term disruption in their ability to send or receive email will have a devastating impact on their operations; others are able to rely on other means of communication to transact

business, but they may suffer significant harm if certain intellectual property is stolen. For others still, the ability to guarantee the integrity and security of the data they store and process, such as customer information, is vital to their continued operation.

The expense and resources required to protect a whole enterprise may force an organization to prioritize its efforts and may shape its incident response planning. Before formulating a cyber incident response plan, an organization should first determine which of their data, assets, and services warrants the most protection. Ensuring that protection of an organization's "crown jewels" is appropriately prioritized is an important first step to preventing a cyber intrusion or attack from causing catastrophic harm. The Cybersecurity Framework produced by the National Institute of Standards and Technology (NIST) provides excellent guidance on risk management planning and policies and merits consideration.[1]

B. Have an Actionable Plan in Place Before an Intrusion Occurs

Organizations should have a plan in place for handling computer intrusions before an intrusion occurs. During an intrusion, an organization's management and personnel should be focused on containing the intrusion, mitigating the harm, and collecting and preserving vital information that will help them assess the nature and scope of the damage and the potential source of the threat. A cyber incident is not the time to be creating emergency procedures or considering for the first time how best to respond.

The plan should be "actionable." It should provide specific, concrete procedures to follow in the event of a cyber incident. At a minimum, the procedures should address:

- Who has lead responsibility for different elements of an organization's cyber incident response, from decisions about public communications, to information technology access, to implementation of security measures, to resolving legal questions;
- How to contact critical personnel at any time, day or night;
- How to proceed if critical personnel is unreachable and who will serve as back-up;
- What mission critical data, networks, or services should be prioritized for the greatest protection;
- How to preserve data related to the intrusion in a forensically sound manner;
- What criteria will be used to ascertain whether data owners, customers, or partner companies should be notified if their data or data affecting their networks is stolen; and
- Procedures for notifying law enforcement and/or computer incident-reporting organization.

[1] The NIST Cybersecurity Framework is available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

All personnel who have computer security responsibilities should have access to and familiarity with the plan, particularly anyone who will play a role in making technical, operational, or managerial decisions during an incident. It is important for an organization to institute rules that will ensure its personnel have and maintain familiarity with its incident response plan. For instance, the procedures for responding to a cyber incident under an incident response plan can be integrated into regular personnel training. The plan may also be ingrained through regularly conducted exercises to ensure that it is up-to-date. Such exercises should be designed to verify that necessary lines of communication exist, that decision-making roles and responsibilities are well understood, and that any technology that may be needed during an actual incident is available and likely to be effective. Deficiencies and gaps identified during an exercise should be noted for speedy resolution.

Incident response plans may differ depending upon an organization's size, structure, and nature of its business. Similarly, decision-making under a particular incident response plan may differ depending upon the nature of a cyber incident. In any event, institutionalized familiarity with the organization's framework for addressing a cyber incident will expedite response time and save critical minutes during an incident.

C. Have Appropriate Technology and Services in Place Before An Intrusion Occurs

Organizations should already have in place or have ready access to the technology and services that they will need to respond to a cyber incident. Such equipment may include off-site data back-up, intrusion detection capabilities, data loss prevention technologies, and devices for traffic filtering or scrubbing. An organization's computer servers should also be configured to conduct the logging necessary to identify a network security incident and to perform routine back-ups of important information. The requisite technology should already be installed, tested, and ready to deploy. Any required supporting services should either be acquired beforehand or be identified and ready for acquisition.

D. Have Appropriate Authorization in Place to Permit Network Monitoring

Real-time monitoring of an organization's *own* network is typically lawful if prior consent for such monitoring is obtained from network users. For this reason, before an incident takes place, an organization should adopt the mechanisms necessary for obtaining user consent to monitoring users' communications so it can detect and respond to a cyber incident. One means of accomplishing this is through network warnings or "banners" that greet users who log onto a network and inform them of how the organization will collect, store, and use their communications. A banner can also be installed on the ports through which an intruder is likely to access the organization's system.

Also available as part of the eCourse
Hooked on CLE: February 2018

First appeared as part of the conference materials for the
2017 Essential Cybersecurity Law session
"Cybersecurity Regulation and Enforcement"