U.S. International Trade Commission

Audit of Incident Management

OIG-AR-11-16

September 29, 2011

Office of Inspector General

The U.S. International Trade Commission is an independent, nonpartisan, quasi-judicial federal agency that provides trade expertise to both the legislative and executive branches of government, determines the impact of imports on U.S. industries, and directs actions against certain unfair trade practices, such as patent, trademark, and copyright infringement. USITC analysts and economists investigate and publish reports on U.S. industries and the global trends that affect them. The agency also maintains and publishes the Harmonized Tariff Schedule of the United States.

Commissioners

Deanna Tanner Okun, Chairman
Irving A. Williamson, Vice Chairman
Charlotte R. Lane
Daniel R. Pearson
Shara L. Aranoff
Dean A. Pinkert

UNITED STATES INTERNATIONAL TRADE COMMISSION

OFFICE OF INSPECTOR GENERAL

WASHINGTON, DC 20436

VIA ELECTRONIC TRANSMISSION

September 29, 2011 OIG-JJ-018

Chairman Okun:

This memorandum transmits the Office of Inspector General's final report Audit of Incident Management, OIG-AR-11-16. In finalizing the report, we analyzed management's comments on our draft report and have included those comments in their entirety in Appendix A.

This report contains eight recommendations for corrective action. In the next 30 days, please provide me with your management decisions describing the specific actions that you will take to implement each recommendation.

Thank you for the courtesies extended to my staff during this audit.

Sincerely,

Philip M. Heneghan
Inspector General

Table of Contents

Results of Audit **1**

Problem Areas **1**

Problem Area 1: The Commission does not have an incident response plan. 1

Problem Area 2: The Commission does not have an incident detection program. 4

Management Comments and Our Analysis **5**

Scope and Methodology **6**

Appendix A: Management Comments on Draft Report ..... **A**

Results of Audit

Does the USITC's incident management program provide senior management with detailed, actionable information regarding security incidents?

No. USITC's incident management program does not provide senior management with detailed, actionable information regarding security incidents.

The Commission's incident response plan lacks the specifics required to enable staff to successfully respond to incidents. Incidents are being handled on an ad-hoc basis, and the Commission does not have a method to use the knowledge gained from these incidents to avoid similar incidents in the future, or increase the speed and effectiveness of eradicating intrusions once detected.

The Commission does not have an incident response plan or an incident detection program. Without these key building blocks, it is not possible for senior management to receive actionable information regarding security incidents.

Problem Areas

Problem Area 1:

The Commission does not have an incident response plan.

The Commission has a document that consists of 98 pages of largely redundant boilerplate from documents generated by the National Institute for Standards and Technology (NIST), and inappropriately borrowed sections from documents defining the program mission of the U.S. Computer Emergency Readiness Team. U.S. CERT is a component of the Department of Homeland Security whose mission is to "improve the nation's cybersecurity posture, coordinate cyber information sharing and proactively manage cyber risks to the nation." An example of this includes the following passages from pages 78-79 of the Information Security Incident Response plan, dated March 2010, Version 3.0:

- *Report on new and novel attack techniques used in the exploitation of systems;*
- *Report on malicious code found in the wild to promote awareness and encourage appropriate action;*

- *Work with the community to develop tools and techniques to nullify the effects of exploits as they occur…*

These tasks are specific for the agency whose mission it is to help serve the government community, but they are not appropriate for the Commission.

We spoke with several operational and network security technical staff about the Information Security Incident Response plan, but we were unable to find anyone who had actually read, much less used this "plan."

In developing this plan, the Commission focused on compliance with various regulatory standards. A focus on compliance unfortunately can place a higher value on paperwork instead of the actual strength of program implementation. The Commission's incident response plan contains all the right words, but it fails to detail a plan that is specific and useful to the Commission.

The Commission recently discovered that Trojan software was installed on some of its systems. While no information security program can be expected to deny all penetration attempts, this event demonstrated a lack of preparedness by the Commission to either detect or respond to serious information security incidents.

The Commission's response to this incident highlighted a number of problems:

1. Not all systems at risk for the Trojan were checked by staff. Of the systems checked by operational staff, records were not created detailing which systems were checked by whom, at what time, and the methods used to check these systems.
2. Users were not notified that their personal data had been stolen. A keystroke-logging Trojan affected at least 59 Commission users since February, 2009. We interviewed 6 of the affected users and asked whether they had been notified about any security incidents involving their data. Several responded that their hard drives had been swapped, but none were notified with any specifics of the incident.
3. Despite detection on June 9, 2011, the Trojan software was still on the network as late as July 8, 2011.

An effective incident response plan must include the tasks of checking all systems at risk, and of recording the actions taken to assess these systems. With sufficient planning, this will ensure a comprehensive assessment, and can give the Commission confidence that the impact of an incident is fully known and remediation is complete.

Users must be notified when their data has been stolen. With a keystroke-logging incident such as that experienced recently, any activity the users performed on their computers was recorded and taken, including their credentials to login to banks, email, and other platforms. Users should be made aware of these types of incidents, so they can change passwords or take other steps to protect themselves.

During the response to the recent incident, remediation was performed by "sneaker-net." Help Desk staff were assigned to physically walk to affected systems and replace their hard drives. It is inefficient to rely on this as a primary response. The attacker did not walk into the building to install the software on each user's system; the Commission's primary response should not employ such a slow, haphazard, and ineffective means of undoing his work. The Commission needs to develop and practice automated, high-speed solutions to perform system-wide detection and removal of malware in the event of an incident.

The Commission has the tools and staff available to create an effective incident response program, but this will not happen unless the focus shifts from compliance to risk management.

Recommendation 1:

Develop a useful, concise incident response plan specific to the Commission's staff, tools, and networks.

Recommendation 2:

Develop a listing of all networks and systems to be checked when an incident occurs.

Recommendation 3:

Record information regarding incident handling to include what was checked, who performed the check, when these systems were checked, how they were checked, and the results of these checks. If any systems are not checked, reasoning for doing so should be recorded.

Recommendation 4:

Develop a procedure to notify and counsel users when their systems have been compromised.

Recommendation 5:

Define a threshold to determine when an incident is widespread and ensure any widespread incidents are communicated to all Commission staff.

Problem Area 2:

The Commission does not have an incident detection program.

The Commission's focus on compliance resulted in the assignment of staff to create or oversee the creation of documentation. Staff were not assigned to analyze traffic and detect abnormal activity. While sophisticated attacks are designed to avoid detection, all of them result in system changes and logged events that can lead to their detection. The Trojan attack had been generating error events on the firewall since March 2010, but because staff and systems were not dedicated to incident detection, the attack continued until June 2011. The incident was finally detected by a new member of the operations staff during the testing of a new network analysis tool.

The Commission's antivirus detection software serves as a primary line of defense against malware such as that recently found. The antivirus in use by the Commission did not detect the Trojan malware. Upon testing, it was found that antivirus software from other major vendors was able to detect the infection. One strategy organizations use is to employ antivirus from multiple vendors to increase the probability of detection. The Commission can deploy antivirus from another vendor and perform repeated, scheduled scans of the fileservers to detect malware not identified by the antivirus product in use on workstations.

Recommendation 6:

Assign staff dedicated to the detection of incidents.

Recommendation 7:

Improve monitoring so that staff are alerted to unexpected traffic being denied by security infrastructure.

Recommendation 8:

Implement weekly scanning of fileservers with antivirus software different than that used on workstations and email systems.

Management Comments and Our Analysis

On September 27, 2011, Chairman Deanna Tanner Okun provided management comments on the draft audit report. The Chairman agreed with our assessment that there are two problem areas in that the Commission does not have an incident response plan, and it does not have an incident detection program, and that the Commission will implement the recommendations detailed to strengthen its incident management program. The Chairman's response is provided in its entirety as Appendix A.

Scope and Methodology

Scope:

- This audit focused on the Commission's Incident Response program, including a review of the Commission's documented procedures, and past performance of incident management.

Methodology:

1. Review documented procedures.
2. Assess documentation concerning prior incidents.
3. Interview program staff to assess their knowledge and roles related to incident detection.
4. Analyze incident detection tools in use to assess their capabilities, and identify potential gaps in coverage.
5. If evidence of previous incidents exists, contact users to gather information concerning their experience, including guidance received by technical staff.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix A: Management Comments on Draft Report

Chairman

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

CO76-JJ-049

September 27, 2011

MEMORANDUM

TO: Philip M. Heneghan, Inspector General

FROM: Deanna Tanner Okun, Chairman

SUBJECT: Management Response to the Inspector General's Draft Audit Report, "Audit of Incident Management"

I appreciate the opportunity to review the Inspector General's draft report, *Audit of Incident Management*, dated August 25, 2011, and to provide comments.

The Inspector General's draft report found the Commission's incident response plan lacks the specifics required to enable staff to successfully respond to IT security incidents. The report identified two areas for improvement: (1) the Commission does not have an incident response plan, and, (2) it does not have an incident detection program.

We agree with the findings. The Commission is dedicated to ensuring that it develops the programs and processes that will allow it to effectively and efficiently respond to IT security incidents. Thank you for reviewing the Commission's incident response program and making the recommendations to strengthen its IT security activities.

"Thacher's Calculating Instrument" developed by Edwin Thacher in the late 1870s. It is a cylindrical, rotating slide rule able to perform complex mathematical calculations involving roots and powers quickly. The instrument was used by architects, engineers, and actuaries as a measuring device.

To Promote and Preserve the Efficiency, Effectiveness, and Integrity of the U.S. International Trade Commission

U.S. International Trade Commission
Office of Inspector General
500 E Street, SW
Washington, DC 20436

Office: 202-205-6542
Fax: 202-205-1859
Hotline: 877-358-8530
OIGHotline@USITC.gov