



Department of Justice



Office of Justice Programs

ADVANCE FOR RELEASE AT 4:00 P.M. EDT
WEDNESDAY, SEPTEMBER 17, 2008
www.ojp.usdoj.gov/bjs

BUREAU OF JUSTICE STATISTICS
Contact: Kara McCarthy: 202-307-1241
After hours: 781-308-3696

67 PERCENT OF RESPONDING BUSINESSES DETECTED CYBERCRIME IN 2005

WASHINGTON –Among 7,818 businesses responding to the National Computer Security Survey (NCSS), 67 percent detected at least one cybercrime in 2005, the Justice Department's Bureau of Justice Statistics (BJS) announced today. Nearly 60 percent of businesses detected one or more cyber attacks, 11 percent detected cyber thefts and 24 percent detected other computer security incidents. Computer viruses were the most common type of cyber attack, detected by 52 percent of reporting businesses.

The NCSS documents the nature, prevalence and impact of cybercrimes against businesses in the United States. Survey respondents represented 7,818 businesses out of the 7.3 million businesses identified nationwide in 2005. Of businesses reporting the number of incidents, 43 percent detected 10 or more cyber attacks, theft or other security incidents during the year. Computer viruses were about 7 percent of the incidents and cyber thefts were less than 1 percent. Other computer security incidents (92 percent)—primarily spyware, adware, phishing, and spoofing—were the most common.

The effects of these crimes were measured in terms of monetary loss and system downtime. Ninety percent of the businesses providing information sustained monetary loss. Cyber thefts accounted for more than half of the loss and cyber attacks for about a third. Approximately 68 percent of victims of cyber theft sustained monetary loss of \$10,000 or more. By comparison 34 percent of victims of cyber attacks lost \$10,000 or more.

System downtime affected 89 percent of businesses that provided downtime information. Sixty percent of system downtime was caused by computer viruses, 8 percent by denial of service, vandalism or sabotage, and 32 percent by other computer security incidents. System downtime lasted longer than 24 hours for about a third of victimized businesses.

Among survey respondents, businesses with the highest prevalence of cybercrime in 2005 included telecommunication businesses (82 percent of such businesses), computer system design businesses (79 percent) and manufacturers of durable goods (75 percent).

(MORE)

Nearly 75 percent of businesses victimized by cyber theft said that insiders—such as employees, contractors or vendors working for the business—were responsible for the crime. More than 70 percent of businesses victimized by cyber attacks or other computer security incidents said the suspected offenders were outsiders (hackers, competitors, and other non-employees).

Overall, 15 percent of victimized businesses said they reported cybercrimes to law enforcement authorities. Six percent of businesses detecting cyber attacks reported the incidents to authorities, compared to more than 50 percent of businesses detecting cyber thefts.

The President's National Strategy to Secure Cyberspace directs the Department of Justice to develop better data on the nature and prevalence of cybercrime and electronic intrusions. The NCSS was developed by the Bureau of Justice Statistics in partnership with the Department of Homeland Security. The Justice Department's Computer Crime and Intellectual Property Section and the Computer Intrusion Section of the Federal Bureau of Investigation Cyber Division also collaborated on the project.

The NCSS data collection was conducted over a seven-month period in 2006. A nationally representative sample of 35,600 businesses representing 36 economic sectors received the survey. Twenty-three percent of the selected businesses responded. Though the responses are not nationally representative, the NCSS is the largest survey conducted to date. Detailed findings for each of the 36 sectors are provided in this report.

The report, *Cybercrime against Businesses, 2005* (NCJ 221943), was written by BJS statistician Ramona R. Rantala. Following publication, the report can be found at <http://www.ojp.usdoj.gov/bjs/abstract/cb05.htm>.

For additional information about the Bureau of Justice Statistics' statistical reports and programs, please visit the BJS Web site at <http://www.ojp.usdoj.gov/bjs>.

The Office of Justice Programs, headed by Acting Assistant Attorney General Jeffrey L. Sedgwick, provides federal leadership in developing the nation's capacity to prevent and control crime, administer justice, and assist victims. OJP has five component bureaus: the Bureau of Justice Assistance; the Bureau of Justice Statistics; the National Institute of Justice; the Office of Juvenile Justice and Delinquency Prevention; and the Office for Victims of Crime. In addition, OJP has two program offices: the Community Capacity Development Office, which incorporates the Weed and Seed strategy, and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART). More information can be found at <http://www.ojp.gov>.

###