Hewlett-Packard Company
3000 Hanover Street
Palo Alto, CA 94304

hp.com

News Release

HP Research: Cybercrime Costs Rise Nearly 40 Percent, Attack Frequency Doubles

Security intelligence solutions key to mitigating impact

Editorial contacts

Kristi Rawlinson, HP
+1 650 799 7061
kristi.rawlinson@hp.com

Michelle Doss, HP
+1 214 263 7497
michelle.doss@hp.com

www.hp.com/go/newsroom

PALO ALTO, Calif., Oct. 8, 2012 — HP today unveiled new research indicating that the cost and frequency of cybercrime have both continued to rise for the third straight year.

According to the third annual study of U.S. companies, the occurrence of cyberattacks has more than doubled over a three-year period, while the financial impact has increased by nearly 40 percent.(1)

Conducted by the Ponemon Institute and sponsored by HP, the 2012 Cost of Cyber Crime Study found that the average annualized cost of cybercrime incurred by a benchmark sample of U.S. organizations was $8.9 million. This represents a 6 percent increase over the average cost reported in 2011, and a 38 percent increase over 2010. The 2012 study also revealed a 42 percent increase in the number of cyberattacks, with organizations experiencing an average of 102 successful attacks per week, compared to 72 attacks per week in 2011 and 50 attacks per week in 2010.

“Organizations are spending increasing amounts of time, money and energy responding to cyberattacks at levels that will soon become unsustainable,” said Michael Callahan, vice president, Worldwide Product and Solution Marketing, Enterprise Security Products, HP. “There is clear evidence to show that the deployment of advanced security intelligence solutions helps to substantially reduce the cost, frequency and impact of these attacks.”

The most costly cybercrimes continue to be those caused by malicious code, denial of service, stolen or hijacked devices, and malevolent insiders. When combined, these account for more than 78 percent of annual cybercrime costs per organization. Additional key findings include:

- Information theft and business disruption continue to represent the highest external costs. On an annual basis, information theft accounts for 44 percent of total external costs, up 4 percent from 2011. Disruption to business or lost productivity accounted for 30 percent of external costs, up 1 percent from 2011.
- Deploying advanced security intelligence solutions can mitigate the impact of cyberattacks. Organizations that deployed security information and event management (SIEM) solutions realized a cost savings of nearly $1.6 million per year. As a result, these organizations experienced a substantially lower cost of recovery, detection and containment than organizations that had not deployed SIEM solutions.

- Cyberattacks can be costly if not resolved quickly. The average time to resolve a cyberattack is 24 days, but it can take up to 50 days according to this year's study. The average cost incurred during this 24-day period was $591,780, representing a 42 percent increase over last year's estimated average cost of $415,748 during an 18-day average resolution period.
- Recovery and detection remain the most costly internal activities associated with cybercrime. On an annual basis, these activities account for almost half of the total internal cost, with operating expenses and labor representing the majority of the total.

"The purpose of this benchmark research is to quantify the economic impact of cyberattacks and observe cost trends over time," said Dr. Larry Ponemon, chairman and founder, Ponemon Institute. "We believe a better understanding of the cost of cybercrime will assist organizations in determining the appropriate amount of investment and resources needed to prevent or mitigate the devastating consequences of an attack."

In conjunction with this third annual study of U.S. companies, cybercrime cost studies also were conducted in Australia, Germany, Japan and the United Kingdom. HP is hosting a series of webinars highlighting the findings from these studies, with the U.S.-focused webinar taking place Nov. 7. Additional information about this webinar, and those taking place in other regions, is available at www.hpenterprisesecurity.com/ponemon-cost-of-cyber-crime/.

HP is changing the enterprise security landscape with the HP Security Intelligence platform, which uniquely leverages advanced threat research and powerful correlation of security events and vulnerabilities to deliver security intelligence spanning IT operations, applications and infrastructure.

Additional information about HP Enterprise Security Solutions is available at www.hpenterprisesecurity.com/solutions.

HP's premier Europe, Middle East and Africa client event, HP Discover, takes place Dec. 4-6 in Frankfurt, Germany

About HP
HP creates new possibilities for technology to have a meaningful impact on people, businesses, governments and society. The world's largest technology company, HP brings together a portfolio that spans printing, personal computing, software, services and IT infrastructure to solve customer problems. More information about HP (NYSE: HPQ) is available at http://www.hp.com.

[1] The Ponemon Institute pursued field-based research that involved interviewing senior level personnel and collecting details about actual cybercrime incidents. This research culminated with the completion of case studies involving 56 organizations located in the United States. Many of the organizations are multinational corporations.