

Don't Base Security Decisions on Industry Surveys

Rich Mogull

A Computer Security Institute survey again reports that business losses from cybercrime are declining. But surveys of this type are still too uncertain methodologically to form the basis of sound security strategy.

NEWS ANALYSIS

Event

On 14 June 2006, the Computer Security Institute (CSI) released a preview of the results of its annual Computer Crime and Security Survey, showing reported business losses from cybercrime as having fallen for the fourth consecutive year. The CSI said the businesses responding to the survey reported average losses to cybercrime of \$167,713 in 2005 — an 18 percent reduction from the previous year. CSI will publish the full report in July 2006.

Analysis

The CSI's latest report of decreasing losses from cybercrime appears to be good news. However, Gartner believes that security administrators should view the findings of all such surveys with extreme skepticism. A recent survey by Deloitte Touche Tomatsu, for example, reported that security breaches at financial institutions had increased significantly over the same time period, which would seem to contradict the CSI findings.

Unfortunately, surveys of this type frequently reflect the agendas of those being surveyed more than they do objective reality. Security administrators who want more funding tend to exaggerate problems, while those who want to show they are doing a good job may de-emphasize them. Security vendors complicate matters further by developing their own sets of statistics, which the news media frequently repeat as fact.

Furthermore, the nature of security incidents has changed significantly in recent years. For example, losses caused by Web site vandalism and worms have declined, but losses from data exposures have risen. The CSI has surveyed the same group of respondents over many years but has not used a consistent loss model — and even if a consistent model had been used, the nature of attacks has changed enough to invalidate direct comparisons to the past.

The underlying problem is that the IT industry lacks:

- A clear, mutually agreed-on method of evaluating the frequency and the cost of security breaches
- Agreed-on definitions of what constitutes a security breach
- Clear definitions of intellectual property, without which it is impossible to place an accurate price tag on intellectual property losses

Recommendation for Security Administrators

Do not base strategic security planning decisions on industry reports or surveys until common definitions and methodologies are developed and accepted industrywide.

Analytical Source: Rich Mogull, Gartner

RECOMMENDED READING

- "User Survey: Security Summit Reveals Spending Patterns, Worldwide, 2005" — Traditional threats, such as viruses and worms, continue to dominate security spending worldwide. **By Vic Wheatman**

- "Management Update: Eight Steps Needed to Define Reasonable Security" — Eight key elements should be considered when determining what constitutes due care in security.
By Vic Wheatman and Paul Proctor

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509