

Data Breach Incidents & Responses

Health Care Compliance Association & the Society of Corporate Compliance and Ethics
October and November 2012

OBJECTIVE:

This survey was conducted in order to better understand the costs associated with a data breach.

METHODS USED:

Responses were collected from compliance and ethics professionals from the database of the Health Care Compliance Association and Society of Corporate Compliance and Ethics. Over 450 responses were collected from private and public companies and non-profits from a wide range of industries. Additionally, three quarters of the responses were from the healthcare industry.

KEY FINDINGS:

- 59% of respondents reported that their organization had suffered a data breach in the previous year.
 - 37% experienced multiple breaches.
- The highest source of the latest data breach was due to lost paper files (38%), followed by a lost device such as a memory stick (27%).
 - Hacktivists were reported to be behind only 11% of the breaches.
- 47.4% of breaches were reported by an employee other than IT.
 - 14.7% reported that a customer had notified the organization of a breach.
- 59% reported that resolving the breach cost less than \$50,000.
 - 24.5% reported that resolving the breach came at no cost.
 - 3.2% responded that the breach cost them over half a million dollars.
- 69% responded that remediation tended to be the responsibility of the compliance and ethics office. (Important to note that responses were collected from compliance and ethics professionals.)
 - Followed by IT at 14%.

CONCLUSION:

- In reality, lost documents, not hackers seem to be the greatest problem in terms of data breaches. Organizations should continue to stress the importance of keeping control of documents and only print out what is necessary.
- Companies should not lose sight of the risk of a hacking attack. Unlike paper documents, which may contain only a few records, having a whole system hacked could expose a great number of confidential information.
- Employees should be encouraged to report data losses immediately.
- The costs of data breaches are in general relatively low, but it is important to take into account lost business or brand value due to customer or partner mistrust or negative publicity.

[Full Report](#)