Data Breach Incidents & Responses

A survey by the Society of Corporate Compliance and Ethics and the Health Care Compliance Association

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

www.hcca-info.org / www.corporatecompliance.org

Executive Summary

Data breach incidents are very expensive for organizations, both in hard dollars and reputational costs. In addition to the notification and other requirements, the sting of bad press can make a bad situation even worse.

To better understand the costs of a data break, the Society of Corporate Compliance and Ethics and the Health Care Compliance Association jointly fielded a survey to determine the prevalence, causes and consequences of data breaches.

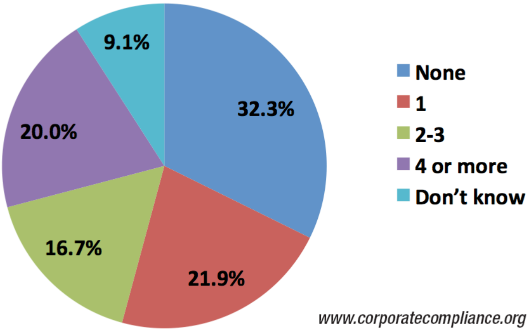
The results indicated that nearly 60% of respondents' organization had suffered an incident in the last year, and 20% had suffered four or more. The most common causes for a breach were lost paper files and misplaced portable memory devices rather than via database intrusions. Breaches were most likely to be by rank and file employees rather than IT.

Breach remedy costs tended to be lower than might be expected, with the vast majority reporting expenses of $50,000 or less per breach event.

Detailed Findings

- **More than half (59%) of respondents reported that their organization had suffered a data breach in the previous year.** Although 59% is a significant percentage of the respondents, what is perhaps more surprising is that more than 37% of these organizations experienced multiple breach incidents. Seventeen percent of respondents reported two or three incidents, while 20% reported four or more breaches.

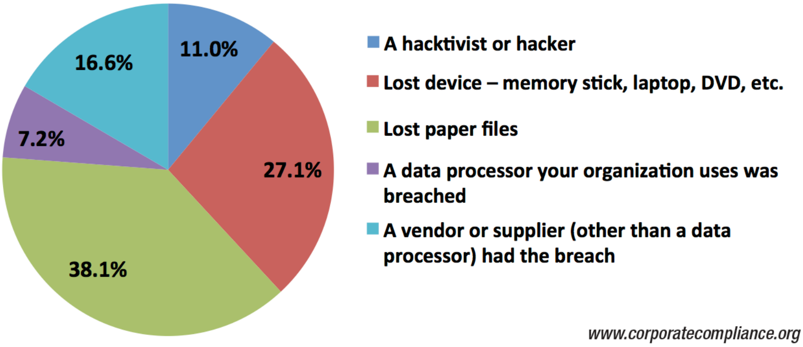
How many data breaches has your organization suffered in the last year?



www.corporatecompliance.org

- **Despite all the fears of intrusions by hackers/hacktivists, they were far from the most common cause of a breach.** Survey respondents reported that lost paper files (38%) were the most likely cause of their organization's last data breach. The next most common cause of a data loss was a lost device such as a memory stick (27%). Hacktivists were reported to have been behind the last data breach by only 11% of respondents. This data confirms the expectations of compliance professionals who, in a 2011 survey by the SCCE and HCCA, expressed far greater fear of an accidental data loss than they did from activity by hackers.

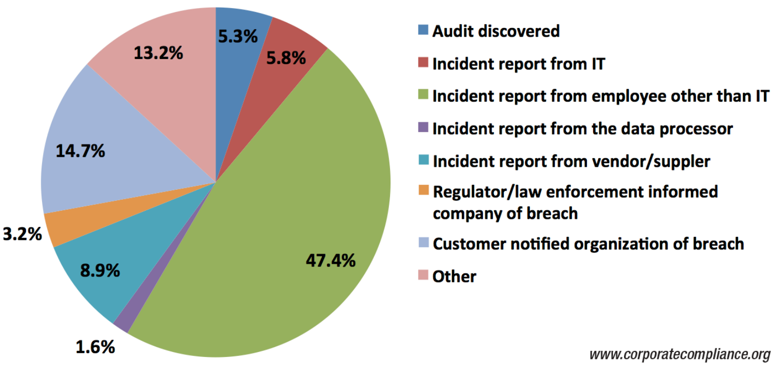
What was the source of the last data breach your organization suffered?



www.corporatecompliance.org

- **Consistent with the number of incidents due to lost physical documents and devices, breach reports did not typically come from IT.** Forty seven percent of respondents reported that the latest data breach was reported by an employee other than IT. Perhaps most intriguing was the fact that 15% reported that a customer had notified the organization of the breach.

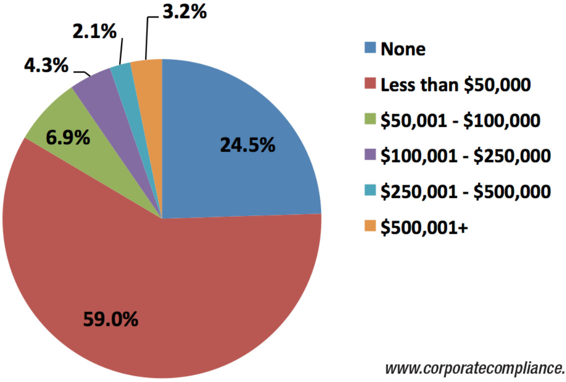
How was the breach discovered by your organization?



www.corporatecompliance.org

- **In a quarter of the cases respondents reported that resolving the breach came at no cost.** For another 59% the cost was reported to be less than $50,000. For a small percentage (3%) their remediation costs exceeded half a million dollars.

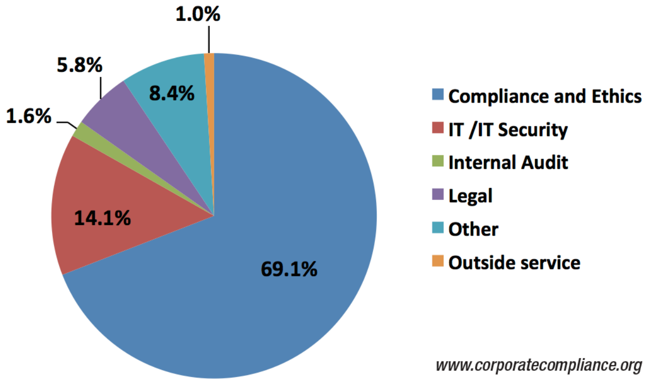
What would you estimate is the cost of resolving the last breach your organization encountered?



www.corporatecompliance.org

- **Remediation tended to be the responsibility of the compliance and ethics office.** Sixty nine percent of respondents reported that compliance and ethics led the remediation effort. The next most likely group to handle the response, not surprisingly, was IT at 14%. It should be noted, though, that responses were solicited among compliance and ethics professionals, which may have skewed the results.

What department in your organization led the remediation effort following the last data breach?



www.corporatecompliance.org

Conclusions and Implications

- **For all of the concerns about hackers and the porousness of data available electronically, old-fashioned lost documents and the proliferation of portable memory devices seems to be the greatest problem.** Organizations need to remain vigilant to this issue and continue to stress to employees the importance of printing out what is only necessary and being vigilant toward data security. As simple as it sounds, it is important to stress keeping control of documents and portable memory devices at all times.

- **Given the risk, employees must be encouraged to report data losses immediately.** The good news is that the data indicates that employees are willing to come forward regularly. Yet, as efforts to tighten controls over electronic data continue, focus could shift away from the individual employee's role in discovering and reporting data loss. Such a shift in focus could prove very costly to organizations.

- **At the same time, companies should not lose sight of the risk of a hacking attack.** Unlike paper documents, which may contain only a few records, having a system hacked could expose a plethora of confidential information. Hackers also often benefit from phishing attacks where employees credentials are compromised. Training employees on Internet safety, in the office and while on the road, is imperative.

- **While the costs for data breaches appear to be relatively low, organizations should not expect them to remain so.** The numbers in the research only reflect hard costs. They don't take into account lost business or brand value due to customer or partner mistrust or negative publicity. In addition, as privacy regimes grow globally organizations may expect greater penalties when data privacy laws are broken.

Methodology

Survey responses were solicited during October and November 2012 from compliance and ethics professionals in the database of the Health Care Compliance Association and Society of Corporate Compliance and Ethics. Responses were collected and analyzed using SurveyMonkey, a web-based third party solution. More than 450 responses from private and public companies as well as non-profits were received. Respondents came from a wide range of industries, but it should be noted that approximately three quarters were in the health care industry.