Data Breach Incidents, Causes, and Response

November 2016

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

SCCE

HCCA

corporatecompliance.org • hcca-info.org

Executive Summary

In October and November of 2012 the Society of Corporate Compliance and Ethics and the Health Care Compliance Association conducted a survey among compliance professionals to better understand the impact and frequency of data breaches. At the time breaches were very much in the news, just as they are today.

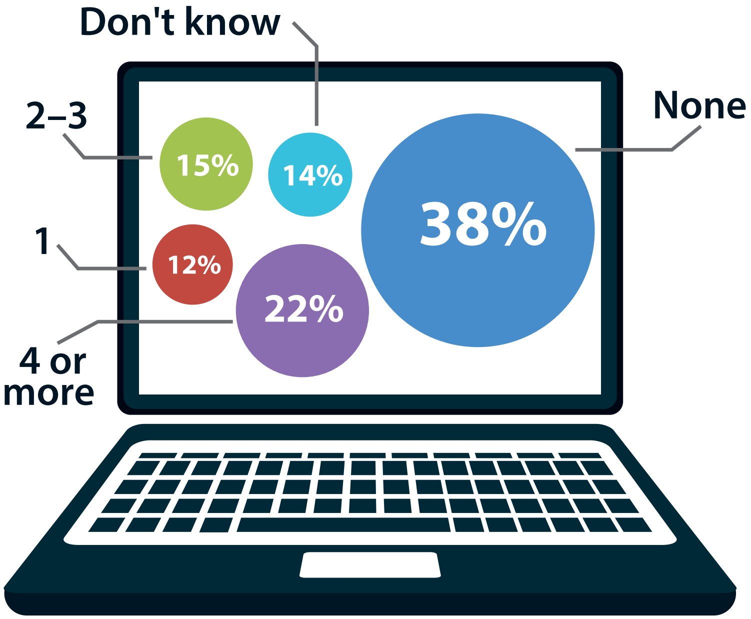
To assess whether and how much things had changed in the past four years, SCCE and HCCA fielded the same survey again. The results were surprising: in spite of all the headlines of increased risk, relatively little has changed when it comes to both managing the issue and the number of incidents. In fact, what's remarkable is that on many measures the numbers were down.

Key Findings

- **Remarkably, despite all the attention paid to the issue, 38% of respondents reported that their organization had not suffered a data breach in the last year.** Company size, however, played a large role. While 51% of organizations with 1,000 employees or less reported a breach, 81% of those with 100,000 or more employees had been breached.

- **Also, remarkably, the number of respondents who reported no breaches was up.** In 2012 32% reported no incidents, which is 6 percentage points less than the current survey.

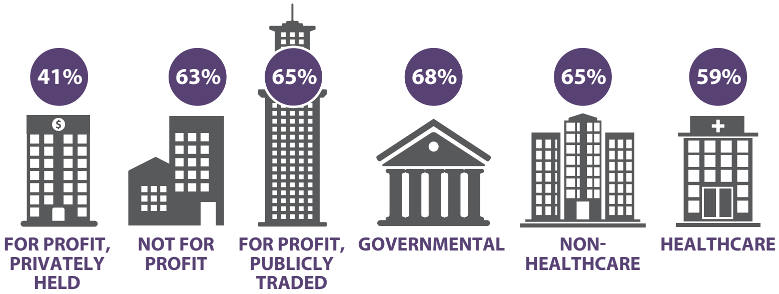
How many data breaches has your organization suffered in the last year?



Society of Corporate Compliance & Ethics / corporatecompliance.org

- **The reported likelihood of having a breach also varied by organization type and industry.** For profit, privately held companies were least likely to report having a breach. 41% of respondents from organizations of this type reported that their organization had a breach. That compares to 65% of publicly traded companies, 63% of non-profits and 68% of respondents from governmental institutions. At the same time, 59% of healthcare respondents reported having a breach vs. 65% from other industries.

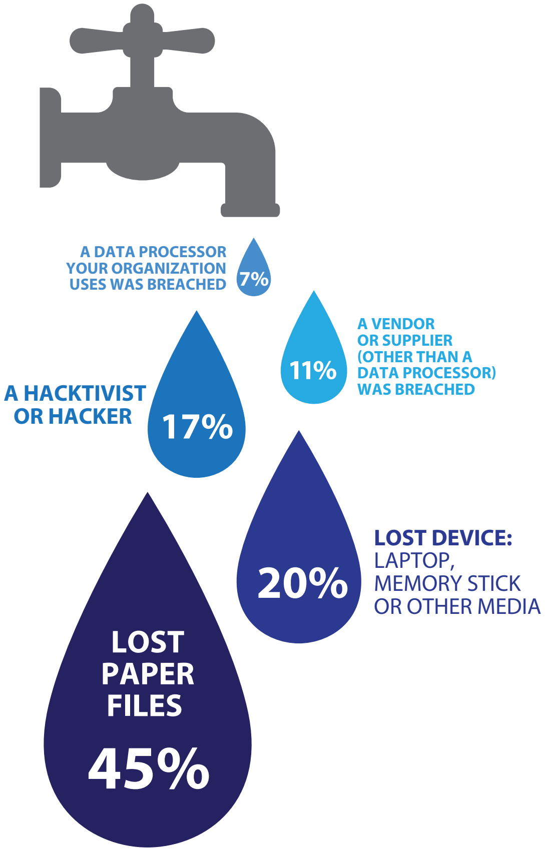
Suffered at least one breach in the last year



Society of Corporate Compliance & Ethics / corporatecompliance.org

- **Hackers proved to be far less of a threat than simple, human error.** Just 17% reported that a hacktivist or hacker was the cause of the breach, up from 11% in 2012. Far more likely to cause a breach were a lost device (20%) and lost *paper* files.

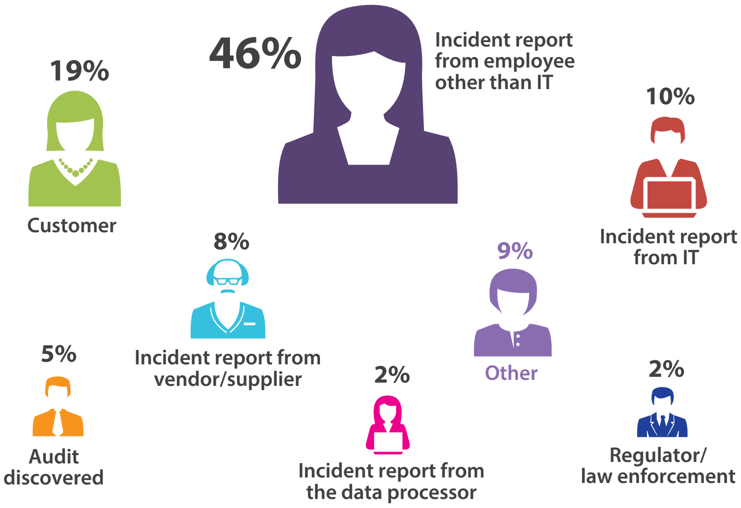
What was the source of the last data breach your organization suffered?



Society of Corporate Compliance & Ethics / corporatecompliance.org

- **Employees were the #1 source of reporting an incident.** When asked how was the last incident discovered, survey respondents reported that audits discovered just 5%, and IT reported just 10%. By contrast, employees other than IT reported 46%. While at first glance the number may be surprising, it makes sense given that the largest source of breaches were lost devices and files.

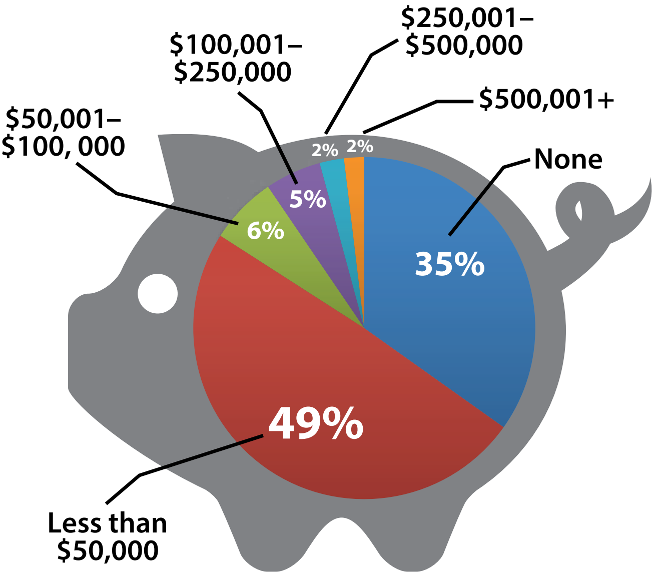
How was the breach discovered by your organization?



Society of Corporate Compliance & Ethics / corporatecompliance.org

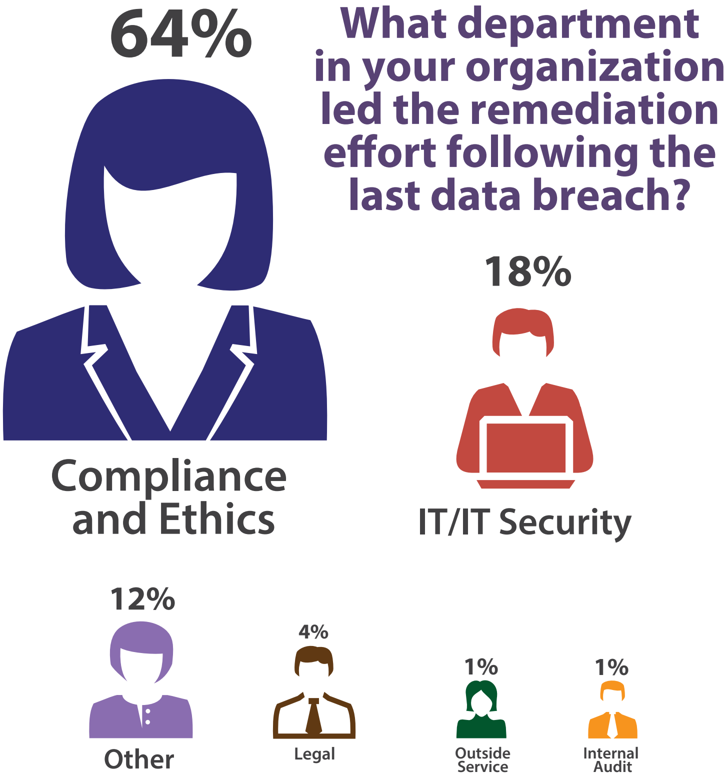
- **Despite headline grabbing breach costs, incidents are not that expensive.** Thirty-five percent of respondents reported that the last breach at their organization came at no cost, which is up from 25% when the survey was last fielded. Another 49% reported that the breach cost $50,000 or less.

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



Society of Corporate Compliance & Ethics / corporatecompliance.org

- **Compliance and ethics programs generally drive remediation efforts.** Sixty-four percent of respondents reported that remediation was compliance led, off slightly from 69% in 2012. The next most popular answer was IT at just 18%.



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

Society of Corporate Compliance & Ethics / corporatecompliance.org

- **The picture changes dramatically, however, when the latest breach was due to a hacker attack.** In those cases 60% of survey respondents reported that IT took the lead in remediation, compared to just 18% of the time overall. And, costs were much higher. In general, 35% of incidents were remediated at no cost. However, when a hack occurred, that number drops to just 20%, meaning 80% of the time there were expenses incurred.

When the latest breach was due to a hacker attack…

60% of the time **IT** led remediation

80% of the time **costs** were incurred

Society of Corporate Compliance & Ethics / corporatecompliance.org

Conclusions/Implications

- **Despite the headlines, the likeliest cause of a data breach is employee mistakes.** Lost files and devices are a far greater day-to-day threat than hackers.

- **Greater thought should likely be given to how data gets handled.** With employee errors so plentiful and risky, more training may not be enough. Organizations may want to reassess who has access to what data, and even what data may be printed out.

- **The impact of hacking should not be dismissed.** Despite the lower incident rate, an attack can have a huge impact. The research shows hacking incidents are significantly more expensive and likely more disruptive to organizations.

- **If hacking incidents increase, the leadership role of compliance may change.** So long as internal human errors are the primary cause of data incidents, compliance is uniquely suited to taking the lead in efforts to prevent, find and fix problems. However, if the balance shifts towards external threats, IT may take more of a leadership role.

Methodology

Survey responses were solicited during October and November 2016 from compliance and ethics professionals in the database of the Society of Corporate Compliance and Ethics and Health Care Compliance Association. Responses were collecting and analyzing using SurveyMonkey, a web-based, third-party solution. More than 700 responses were received individuals at private and public companies, as well as non-profits and government entities.