Data Privacy:

How Big a Compliance Challenge?

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

January 2011

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

SCCE
SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

Health Care Compliance Association and
Society of Corporate Compliance and Ethics
6500 Barrie Road, Suite 250, Minneapolis, MN 55435
HCCA 888 580 8373 | SCCE 888 277 4977 or +1 952 933 4977
www.hcca-info.org | www.corporatecompliance.org

Introduction

Over the last several years sensitivity by both consumers and organizations to the need for enhanced oversight of data privacy has grown exponentially. HIPAA has raised sensitivities around the protection of health care information, and raised the costs for sharing that information inappropriately. In Europe stringent data requirements put strict limits on what data can be shared, even internally within an organization. And the Wikileaks phenomenon has led many organizations to put stricter controls on who has access to what data.

To assess the role that the compliance team is playing in managing expanding privacy regimes, the Society of Corporate Compliance and Ethics and Health Care Compliance Association fielded a survey in January 2011. The purpose was to both identify compliance officers' areas of responsibility as well as their assessment of the risk. The survey was completed by 518 compliance professionals.

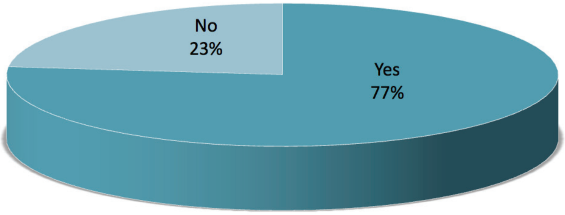
Executive Summary

Privacy has become a growing mandate for compliance professionals. Seventy-five percent of respondents reported that compliance is responsible for overseeing data protection and privacy. In addition, the amount of time spent on the issue has increased significantly, with 82% of respondents reporting an increase, and 77% expecting there to be more time invested in the next year. In general healthcare companies are finding this more of a challenge, but the numbers for non-healthcare companies are also substantial.

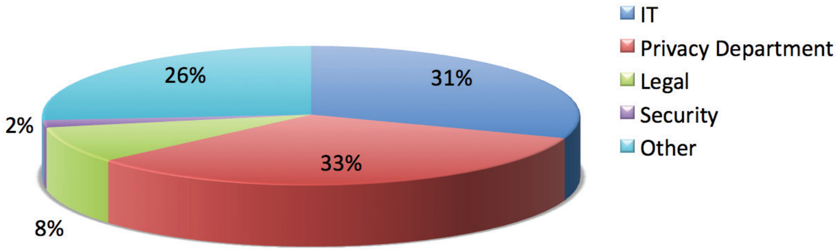
Findings

- **Despite the presence of groups specifically tasked with protecting privacy, in general privacy falls under the purview of the compliance department.** 77% of those surveyed reported that compliance is responsible for overseeing data protection and privacy, although it should be noted that outside of healthcare the number was just 62%. In those cases where compliance is not responsible for privacy, it is generally the responsibility of the privacy department (33%) or IT (31%).

Is compliance responsible for overseeing data protection and privacy in your organization?

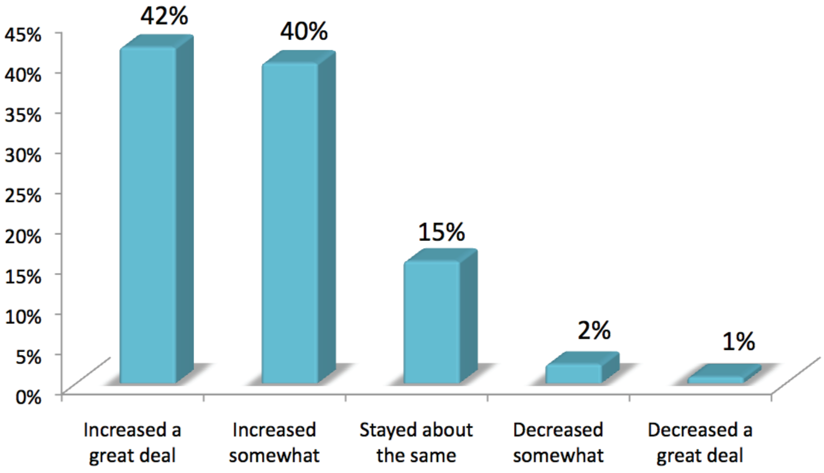


Who is responsible for privacy if not compliance?



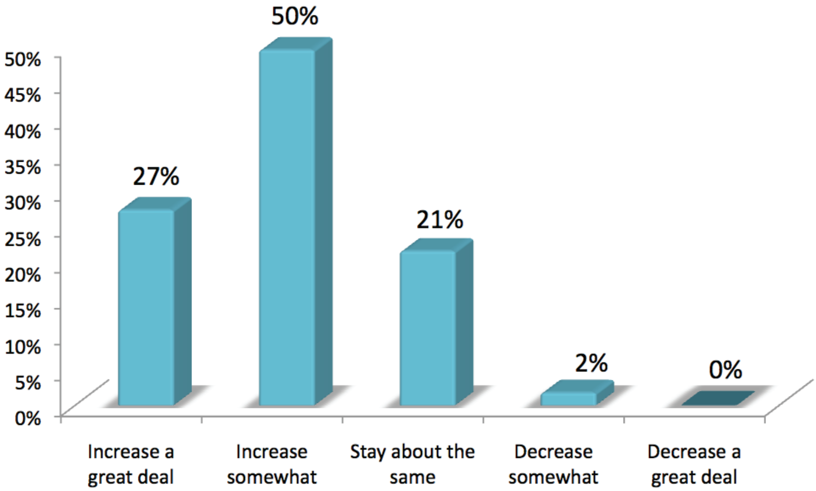
- **The amount of time the compliance team invests in privacy has increased notably in the last three years and that increase is expected to continue.** 42% of respondents report that the time invested has increased a great deal, and another 40% report it increased somewhat, with healthcare companies reporting more of an increase.

In the last three years, how has the time the compliance team spends on privacy changed?



- **Looking to the future, the expectations for increases in time invested in privacy compliance are somewhat tempered but significant.** 50% expect that the time invested in privacy will increase somewhat, and another 27% expect the time will increase a great deal. Notably just 2% expect any type of a decrease.

Over the next year, how do you anticipate the time the compliance team spends on privacy will change?



Tired of 24/7/365 compliance issues?

Try 4,500/30/12 instead.

4,500 compliance & ethics professionals joined in one community.

30 conferences a year to choose from, all with special members-only rates.

12 issues of *Compliance & Ethics Professional*, the exclusive SCCE member magazine.

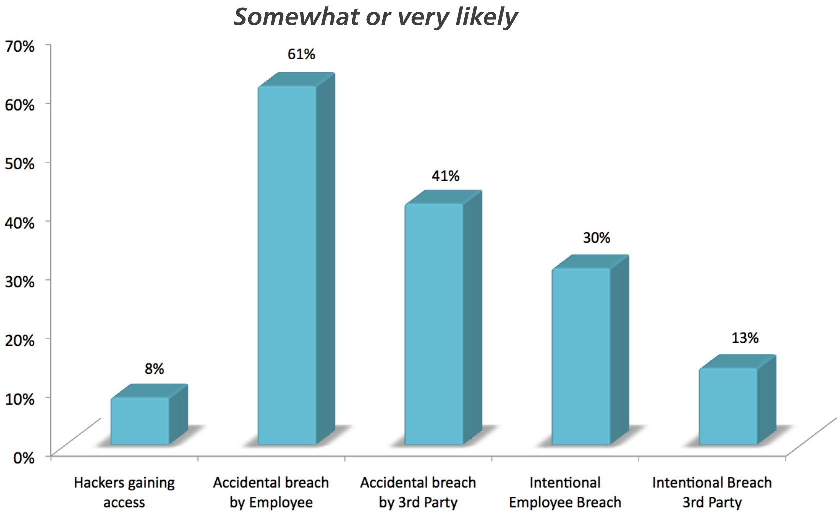
Join the Society of Corporate Compliance and Ethics.

Visit corporatecompliance.org to learn how you can enjoy the educational opportunities, networking, and support of the Society of Corporate Compliance and Ethics.

SCCE®

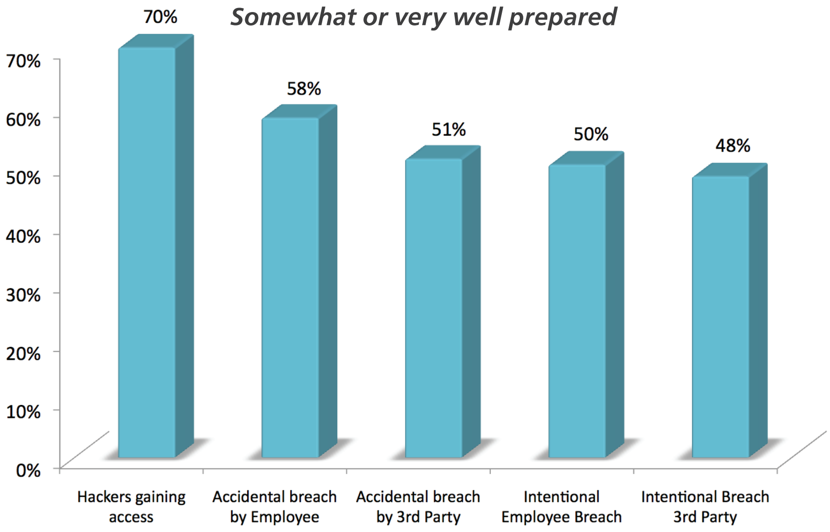
- ○ **Fears of an accidental breach far outweigh fears of an intentional breach.** Respondents were asked how likely they felt that data would be released through hacking attacks, intentional breaches by employees and third party vendors, and accidental breaches by employees and vendors. In general the feeling was that accidental breaches were far more likely. Just 8% felt that it was somewhat or very likely a hacker would gain access to the system, When it came to breaches by employees, 61% thought an accidental breach was somewhat or very likely, but just 30% thought the same of an intentional breach. Likewise 41% thought an accidental breach by a third party vendor was somewhat or very likely but only 13% thought an intentional breach was somewhat or very likely.

In thinking of potential privacy breaches, how likely do you think the following risks are for your organization?



- **While survey respondents felt relatively confident about preparations to fend off an attack by a hacker, they were less confident of their preparations to meet other challenges.** When it comes to hackers, 70% felt that their organizations were well or very well prepared. But the numbers dropped significantly when assessing other threats. For example, just 51% felt that they were well or very well prepared for an accidental breach by a third party.

How well prepared do you think your organization is to protect against the following potential privacy breaches?



Conclusions and Implications

- ○ **While organizations may now be getting ahead of the privacy curve, they are not yet ready to relax.** Compliance professionals have invested significant and increased time on the issue and expect to continue doing so. And, while the amount of work may be abating, it is far from being a static, managed issue.

- ○ **It's likely that further training and controls are necessary to fully manage the issue.** The fear of unintentional breaches suggest that employees and vendors still don't fully understand the need to safeguard data, and that despite training people will still make mistakes. This argues for both further training and hard controls that make it more difficult to share data that was not meant to be shared.

Methodology

Survey responses were solicited during January 2011 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 QuestionPro, a web-based third party solution. More than 500 responses were received from private and public companies as well as non-profits.