CHASE COST MANAGEMENT
an LAC Group company

WHAT PRICE PEACE?

KEY EXPENSE MANAGEMENT STRATEGIES FOR LAW FIRM DATA SECURITY

PRESENTED AT:
Thomson Reuter's 5th Annual Law Firm
CIO|CFO|COO Forum
June 3, 2015, New York City

Brett C. Don, Chase Cost Management

What Price Peace?

Key Expense Management Strategies for Law Firm Data Security

1 INTRODUCTION

Thomson Reuter's 5th Annual Law Firm CIO|CFO |COO Forum was held on June 3rd in New York City. Chase Cost Management (CCM) sponsored a panel discussion titled "What Price Peace? Key Expense Management Strategies for Law Firm Data Security". To generate discussion content for the session, CCM distributed a ten question survey to registered attendees.

A summary of the findings and conclusions is contained within this Executive Summary; the detailed survey results and CCM strategic analyses can be found on pages 5 - 14 of this Report.

2 FINDINGS & CONCLUSIONS

Approximately one-third of the law firms in attendance responded to the CCM survey.

The typical respondent profile is a person in the role of Chief Information Officer (CIO) or Information Technology Director with an AMLAW 200 firm comprised of 827 full-time attorneys and staff that generates more than $363M in gross annual revenues.

The typical participating firm spends just over $6.9M per year on information security (InfoSec) initiatives, or 1.9% of gross annual revenues. The primary driver for this investment is client requirements. This firm uses the collective wisdom embedded in the ISO 27001-02:2013 security standards to guide its InfoSec plan and has invested in some level of cyber-liability insurance to transfer some of the risk.

The typical responding firm is investing in four key areas of security in 2015: 1) strengthening its in-house security skills; 2) identifying gaps through internal and external security assessments; 3) transferring risk with new or updated cyber-liability insurance policies; and 4) training its attorneys and staff on the risks of electronic communications and best practices for identifying phishing emails.

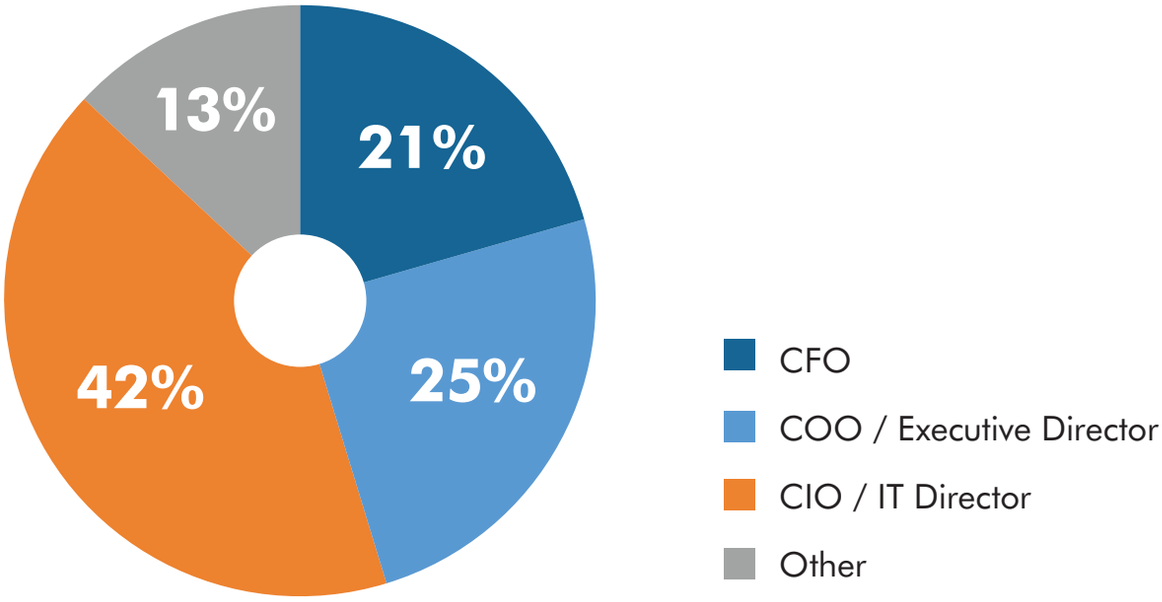
The panel agrees with these four priorities and added two more. Specifically, firms must also:

- **Gain visibility into the network.**
  Invest in services or technologies that identify specific anomalies to minimize the time an attacker spends inside a firm's network.

- **Be prepared to respond to an incident.**
  Every day there is a report of yet another breach. A FireEye system test of 1,200 businesses concluded that 97% of those businesses had already been compromised; no business is immune to these attacks. Firms should invest some time and money into developing an Incident Response Plan.

3 SURVEY RESULTS AND CCM STRATEGIC ANALYSIS

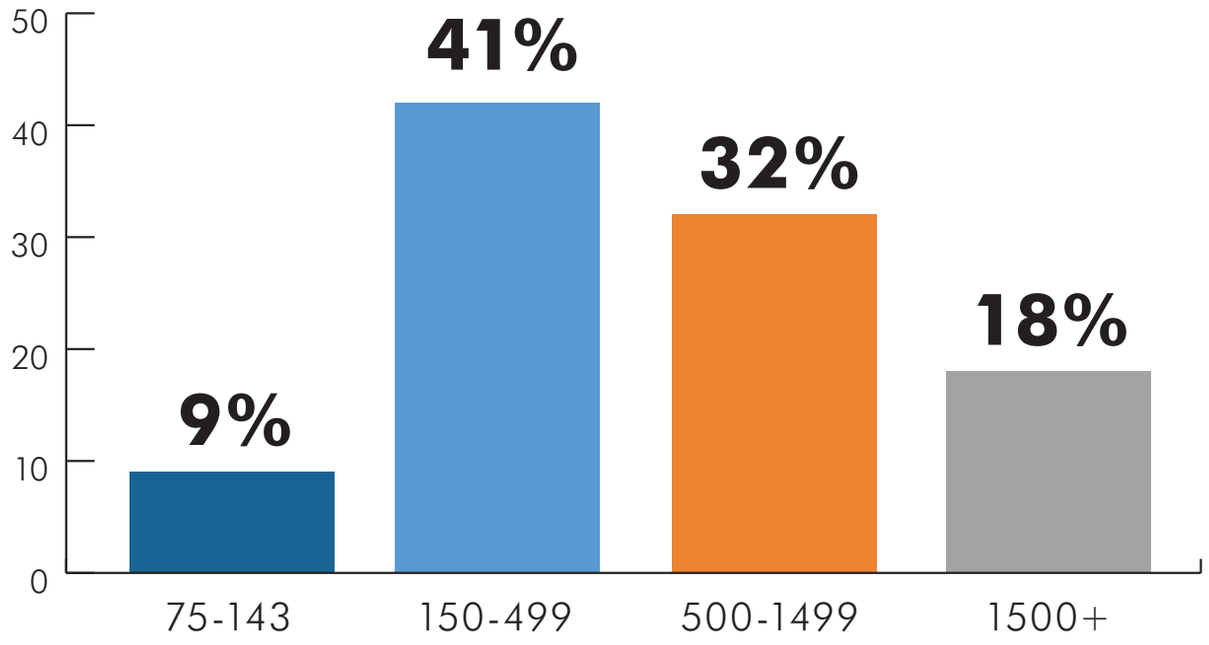
1 | What is your title?



ANALYSIS:

Given that the Forum sessions are designed to attract C-level executives from law firms, it is no surprise that 42% of respondents are heads of the technology function (Chief Information Officers or Information Technology Directors), 21% are heads of the finance function (Chief Financial Officers) and 25% of respondents are Chief Operating Officers and Executive Directors. The 13% of respondents categorized as other included Managing Partners, Chief Administrative Officers and Chief Information Security Officers.

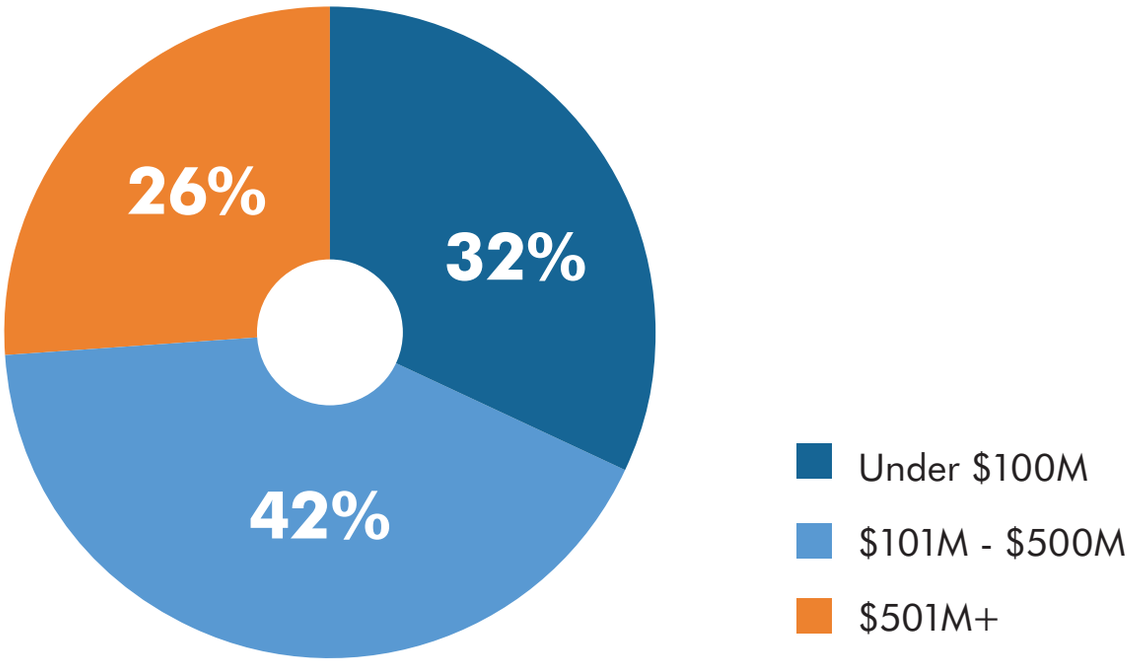
2 | Approximately, how many full-time equivalent attorneys and staff are in your firm?



ANALYSIS:

Exactly half of the survey respondents are employed by law firms with more than 500 full-time attorneys and staff (FTEs) and 50% are employed by firms with fewer than 500 full-time attorneys and staff. The average number of full-time attorneys and staff for all participating firms is 827.

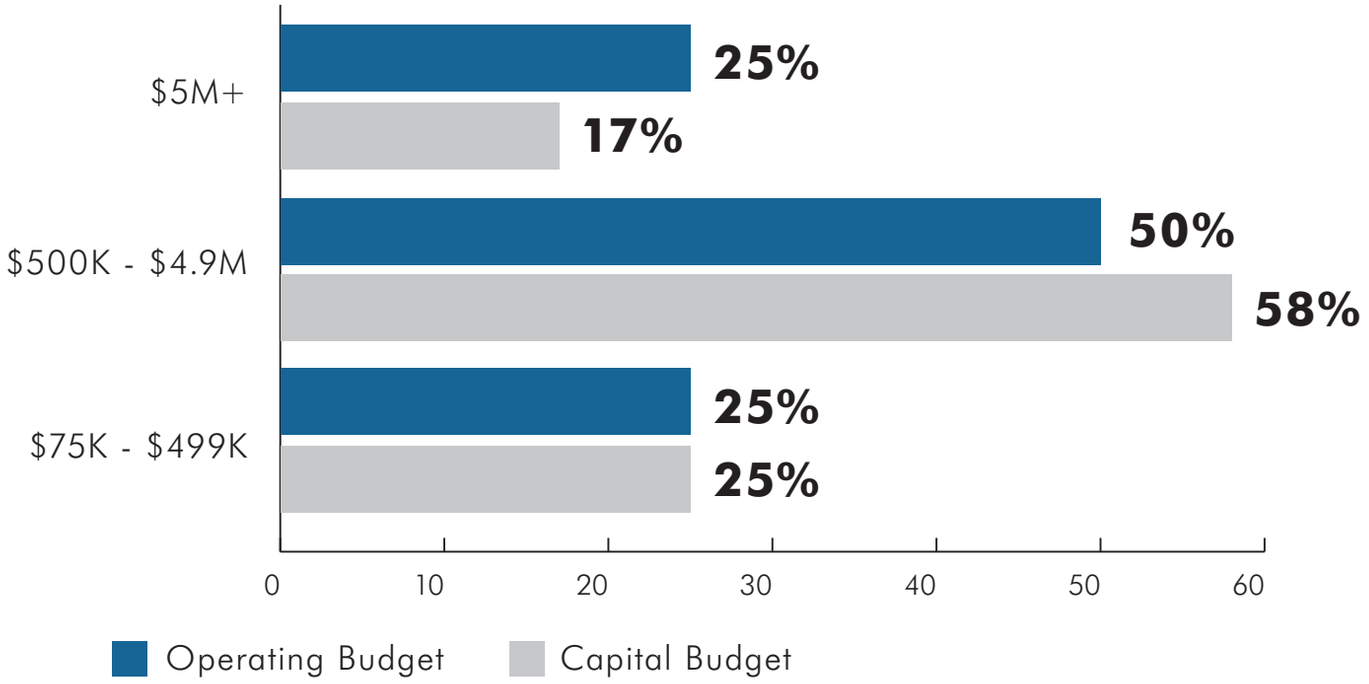
3 | What are your company's estimated annual gross revenues for 2015?



ANALYSIS:

Forty-two percent (42%) of the participating firms have annual gross revenues between $101M and $500M and 26% of the firms enjoy annual revenues exceeding $500M while 32% of the firms generate less than $100M in gross revenues.

4 | What is your 2015 budget for information security and compliance investments?

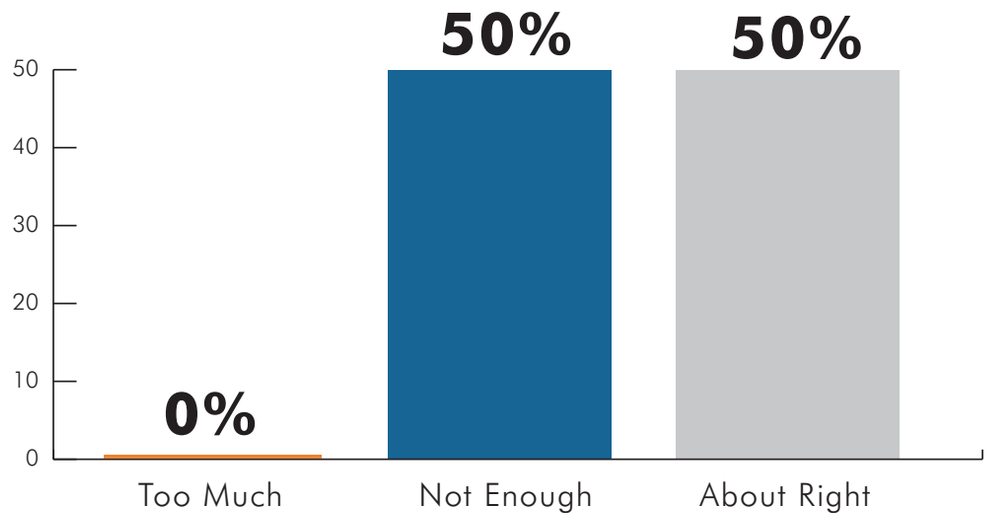


ANALYSIS:

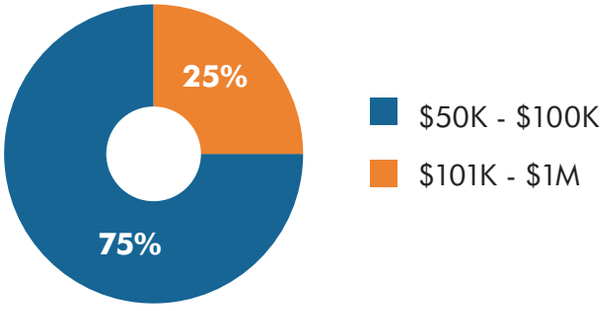
Participating firms plan to spend nearly $7M in 2015 on their information security and compliance initiatives including $4,709,833 on operating expenses and $2,270,333 on capital investments. The panel, generally, found these numbers to be high. One reason, the panel surmised, could be that most firms seem to include information security (InfoSec) investments within the annual information technology (IT) capital and operating budget requests and it may be difficult to extract only InfoSec expenditures.

CCM calculated the InfoSec investment as a percent of gross annual revenue and spend per FTE. The benchmark data provided by survey respondents for InfoSec spend is 1.92% of gross annual revenues (GAR) or $8,440 per FTE. The panel, generally, agreed that both benchmarks are a bit high. The firm of one panel member stated that their investment was about half the benchmark and just under 1% of GAR. The panel cautioned the audience to not get distracted by the 1.92% but, rather, use that benchmark as a data point to support a reasonable funding request for your firm.

5 | Given the size of your firm, practice areas and client base, do you think your total capital and operating budget for information security is too much, too little or about right?



You answered "not enough" in the previous question. What additional budget amount do you think you need for security-related initiatives (in dollars)?

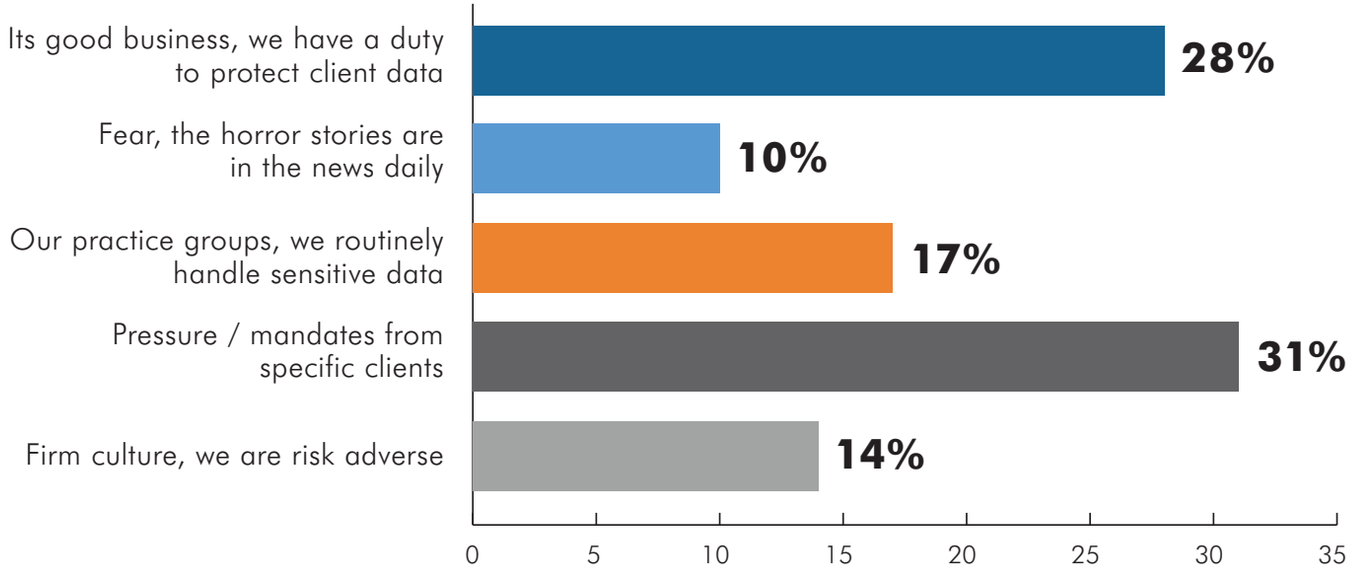


ANALYSIS:

Exactly half of the respondents think that their firm's InfoSec budget is not enough while 50% believe it meets their firm's current needs. Not surprising, no one felt their budget was too much.

For those indicating their budget was not enough, most think they need another $50K to $100K to meet current needs while 25% think they need somewhere between $101K and $1M added to their existing budget in order to meet current business needs. On average, participants feel they need an additional $306,250 per year to satisfy the firm's business requirements.

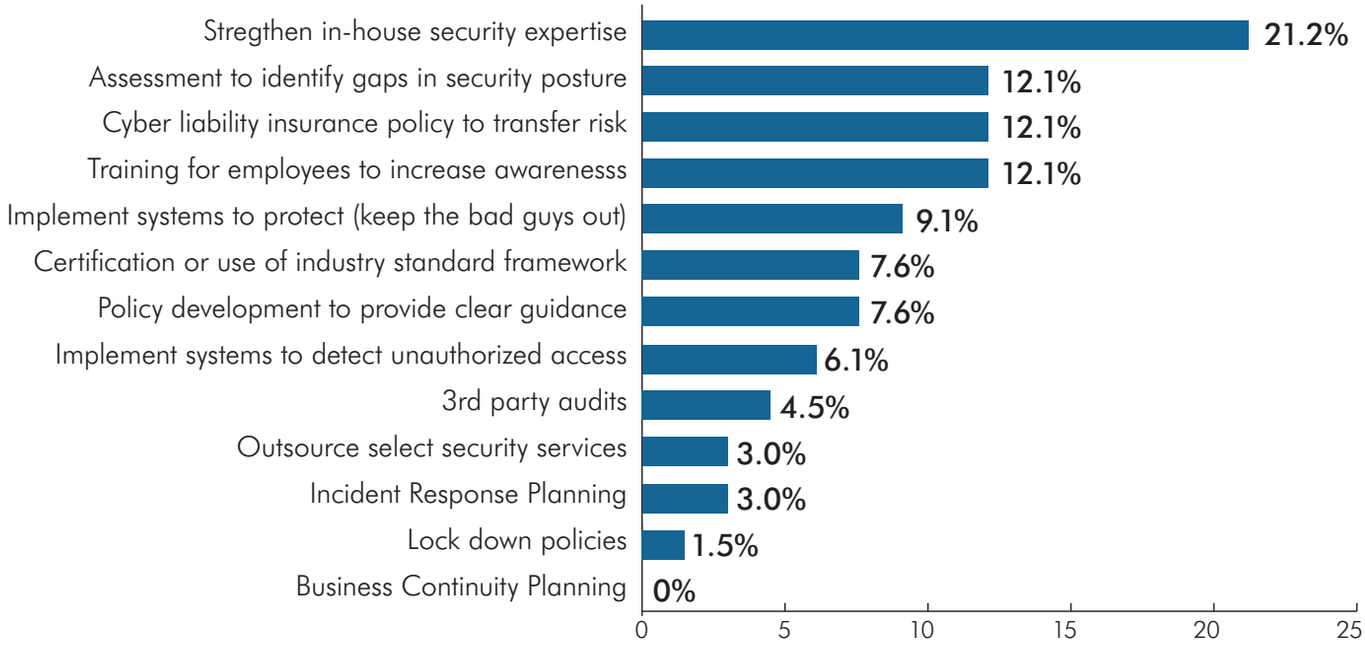
6 | What is your primary driver for your investments in information security?



ANALYSIS:

It was no surprise to the panel that the primary driver for InfoSec investments is client pressure and mandates for better protection of their information. The panel was slightly surprised that only about third of survey participants, or 31%, identified client requirements as the primary driver; the panel expected a higher percentage. The panel felt somewhat encouraged that nearly a third of respondents stated that, in the digital world we live in today, it is just good business to protect information assets. The panel feels that this is the new normal for law firm operations and, although clients are front and center, firms still have other factors to consider including protecting employee personal information and compliance with federal regulations like HIPAA.

7 | What are your top three security investment priorities for 2015?



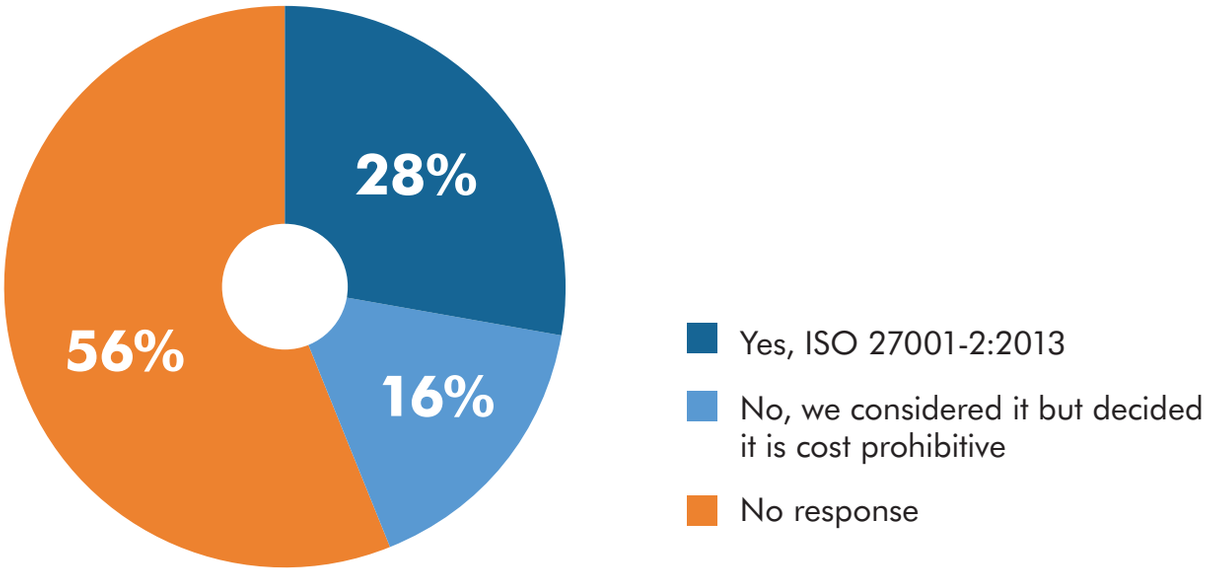
ANALYSIS:

The panel is encouraged to see that 21% of the participating firms plan to strengthen in-house security expertise. Traditionally, many law firms have chosen, likely to control expenses, to give the CIO or IT Director the responsibility for security management and an existing network systems engineer the responsibility for security operations. A hands-up survey of the audience suggests that most firms still do not have dedicated security staff. However, there were a few, albeit larger firms, who have managed to get support for four and five FTEs who are focused on information security initiatives.

The panel is hopeful that firms will continue to invest in employee training and not to simply "check a box". Over 12% of survey participants identified training as a priority in 2015. During a recent FireEye forum, a representative of the FBI's cyber security division stated that 76% of all attacks start with spear phishing emails. This combined with data from a recent ILTA LegalSec survey states that 71% of participating firms conduct security awareness training but only at time of hire and annually suggests that employee training must be a priority and become more of an embedded program rather than an annual event.

Finally, the panel was slightly surprised that Incident Response Planning is identified by only 3% of participating firms as a priority for 2015. This might suggest that firms have already invested in preparing a response plan. However, a recent ILTA LegalSec law firm survey suggests otherwise. That survey stated that 58% of participating firms do not have any form of an Incident Response Plan for a security event in place.

8 | Do you use an industry standard information security framework to guide your security decisions and investments?

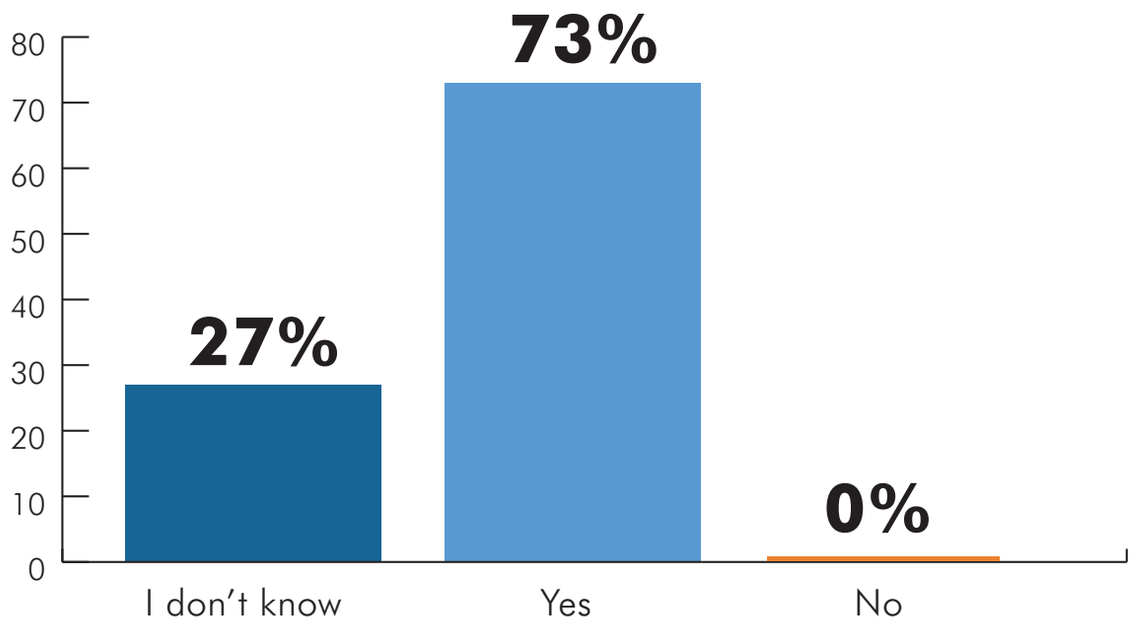


ANALYSIS:

The panel believes there is still some educating to be done around the use of industry standard security frameworks including the two most common that are in use today, ISO 27001-02:2013 and NIST-800-53. About 28% of those responding to the survey are using the ISO 27001-02:2013 security framework to guide their information security strategy; some have been certified and others use it simply as a guide.

The panel noted from personal experience that use of the ISO standards has, in large part, aligned the firm's security priorities with those of the client organizations, making client data privacy questionnaires and security audits palatable.

9 | Have you purchased a cyber-liability insurance policy to manage the risk of a data breach?



ANALYSIS:

Over 70% of respondents stated that their firms have invested in cyber liability insurance. In a previous question, over 12% of respondents stated insurance was a top priority in 2015.

The panel cautioned the audience that cyber liability insurance is not a replacement strategy for reasonable care. Firms must still invest in basic "blocking and tackling" (i.e., passwords, encryption, system patching, etc.) at a minimum to protect sensitive data. One panel member quoted a recent article about an insurance company refusing to payout a policy to a healthcare organization after a breach because the attack occurred as a result of an unpatched system. The insurance provider pointed to a "we don't cover stupid" clause in the policy that states the insured is responsible for ensuring that minimum required security practices are in place.

4 ABOUT CHASE COST MANAGEMENT

Chase Cost Management (CCM) was founded in 1998 in New York City, where it has been operating as a subsidiary of LAC Group since 2011. CCM provides strategic spend management consulting programs and services with proven results based on in-market experience, cost and spending data access, extensive vendor and SKU data, contract negotiation experience and benchmarking expertise. CCM serves Fortune 500 corporations, as well as major healthcare and biotech companies, government, law firms, universities and the pharma/bio industries.

CHASE COST MANAGEMENT
14 Penn Plaza, Suite 402
New York, NY 10122
Main: (212) 563-8600
Fax: (212) 563-8745
ccmchase.com