Advisen
Transforming • Insurance™

MITIGATING THE INEVITABLE: HOW ORGANIZATIONS MANAGE DATA BREACH EXPOSURES

Sponsored by

id experts®

March 2016

TABLE *of* CONTENTS

EXECUTIVE SUMMARY

Every organization—in every industry and of every size—that collects and stores sensitive data is exposed to cybercrime and is at risk for data breach. Highly publicized data breaches in both the private and public sectors continue to occur in large number and with great regularity, and show no signs of slowing down. Many more unreported data breaches that never make it to the media occur on a daily basis. Opportunistic criminals have become adept at identifying the most vulnerable targets and are continuously evolving in order to stay a step ahead of defenses.

The reality is that most organizations have already experienced a data breach whether or not they know it. The majority of breaches are, in fact, small, and may go undetected for a long time. Regardless of industry or size, companies increasingly realize that a breach of sensitive data is detrimental to their financial health. "We are highly concerned about our financial exposure, both in fines and penalties, third party claims, and reputational harm," said a risk manager responding to the survey.

More and more organizations rely on cyber liability insurance to help mitigate this risk. But while cyber liability insurance has proven effective in covering certain cyber-related losses, other types of losses may be excluded under the policy. Additionally, many breaches fall beneath the minimum number of records required to trigger coverage.

It was with this in mind that Advisen and ID Experts collaborated on a survey to gain insight into how businesses are preparing for and responding to data breach threats. The purpose of this study is to better understand how organizations are assessing their breach risks, what actions they are taking to prevent breaches and how they are managing their cyber insurance coverage gaps. The study also explores how organizations respond to data breaches and whether organizations are, or should be, engaging with third party vendors to manage breach response efforts while minimizing reputational, regulatory, and litigation risks.

KEY FINDINGS

- 80 percent of all surveyed organizations are concerned about the consequences of a large public data breach.
- 17 percent of respondents have experienced a data breach that they are aware of over the previous 12 months.
- The vast majority of the data breaches experienced are small consisting of a loss of fewer than 500 records.
- The median data breach is 100 records.
- Only 45 percent of respondents believe their company has adequate resources to detect all breaches.
- 75 percent of respondents have developed an incident response plan but only 42 percent have tested the plan.
- 60 percent of respondents said that the information technology (IT) department is responsible for managing the data breach response.
- 64 percent purchase cyber insurance.
- The vast majority of breaches fall below the cyber insurance policy deductible.
- Most organizations use internal resources to manage small breaches.
- 51 percent have selected data breach response vendors.
- 75 percent prefer to receive all cybersecurity risk services from a single vendor.

EVERYONE IS AT RISK

Organizations that hold sensitive data, regardless of their size, face data breach risks. In fact, most businesses, insurers, and cybersecurity professionals now accept that the question is no longer if a data breach occurs, but rather a matter of when and how bad will it be.

BUSINESSES MUST ASK THEMSELVES IF THEY ARE ADEQUATELY PREPARED TO IDENTIFY AND RESPOND TO THIS NOW NEARLY INEVITABLE DATA BREACH OCCURRENCE. ON THE SURFACE, THE DATA SUGGESTS THAT MANY ARE.

A large public breach can bring a tremendous amount of unwanted attention. As a result, it is no surprise that the vast majority of risk professionals surveyed (80 percent) worry about the consequence of such an occurrence. They express a range of concerns that are largely centered around the financial impact the breach will have on their business.

"Public perception and reputation damage alone would negatively impact business," explained one respondent. "Our biggest concern is the financial exposure both in fines and penalties as well as third party claims and reputation harm," another said. "It could impact business, which is our livelihood," stated another.

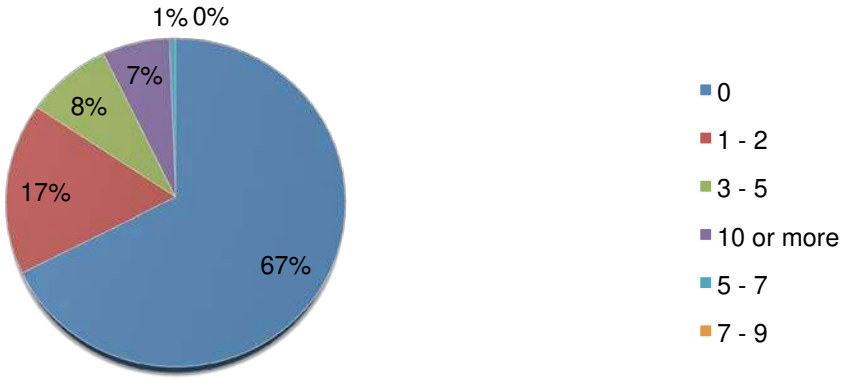
Hacker methods are continuously evolving allowing them to identify new vulnerabilities and penetrate even the most well-fortified websites and networks. Simultaneously, the ability to execute cyberattacks has become easier as hacking toolkits and contract hackers are readily available for purchase, rent, or hire on the Internet.

While it now is a near certainty that a company will at some point experience a data breach, what is not certain is the impact the breach will have on their business. It is widely accepted that organizations that proactively prepare for and manage data breach risk will significantly reduce the impact.

Businesses must ask themselves if they are adequately prepared to identify and respond to this now nearly inevitable data breach occurrence. On the surface, the data suggests that many are. Sixty-seven percent of the survey's respondents claimed to not have experienced a data breach in the previous 12 months, with another 17 percent saying they experienced only one or two breaches over that period (Exhibit 1). However, less than half (45 percent) of the respondents believe their organization has adequate resources to detect data breaches so many breaches may go undiscovered.

EXHIBIT 1:

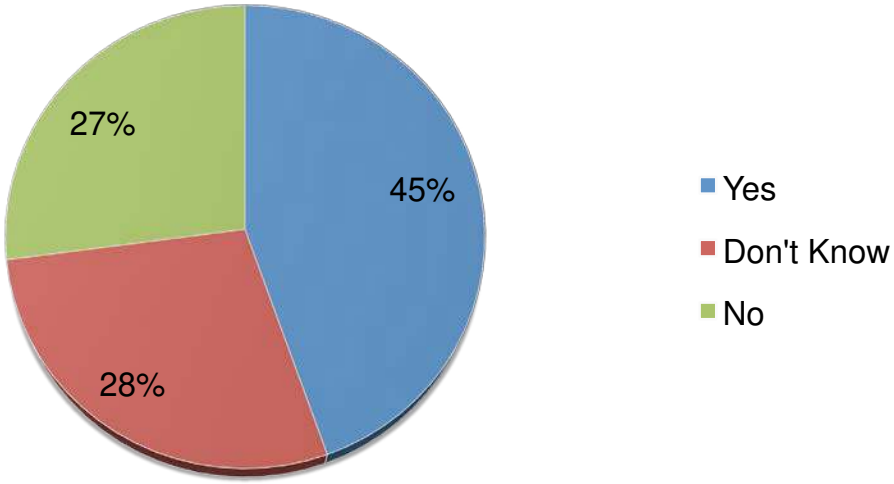
MOST ORGANIZATIONS HAVE EXPERIENCED A LOSS OF SENSITIVE DATA IN A SMALL BREACH AND IN MANY CASES MULTIPLE LARGE BREACHES. HOW MANY DATA BREACHES HAS YOUR ORGANIZATION EXPERIENCED IN THE LAST 12 MONTHS?



The unfortunate reality, however, is that many are likely experiencing breaches that have yet to be discovered. The reason for this may not be for lack of desire or for lack of trying, but rather because they simply do not have the qualified resources, processes or systems. Respondents were asked if they believe their organization has adequate resources to detect all data breaches. Forty-five percent said yes but the remaining 55 percent either said no or that they did not know (Exhibit 2).

EXHIBIT 2:

DO YOU BELIEVE YOUR ORGANIZATION HAS ADEQUATE RESOURCES TO DETECT ALL DATA BREACHES?



ASSESSMENT OF RISK

Risk professionals agree that having a clear understanding of exposures and vulnerabilities and developing a data breach incident response plan around those vulnerabilities is key to minimizing the potential for loss. A poorly managed response significantly increases the risk for costly fines, lawsuits, reputational harm, and customer identity theft.

Seventy-two percent of respondents said that they conduct a cybersecurity and privacy risk assessment at least annually (Exhibit 3).[1] Most said that they actively update their privacy and security policies, training, and internal resources.[2] And the majority (75 percent) has also developed an incident response plan (Exhibit 4).[3]

LESS THAN HALF (45 PERCENT) OF RESPONDENTS BELIEVE THEIR ORGANIZATION HAS ADEQUATE RESOURCES TO DETECT DATA BREACHES SO MANY BREACHES MAY GO UNDISCOVERED.

[1] Appendix: Exhibit 1 – "How do you assess your cybersecurity risk?"

[2] Appendix: Exhibit 2 – "Do you actively update the following?"

[3] Appendix: Exhibit 3 – "Do you have a data breach incident response team?"

EXHIBIT 3:

HOW OFTEN DO YOU DO A CYBER SECURITY AND PRIVACY RISK ASSESSMENT?

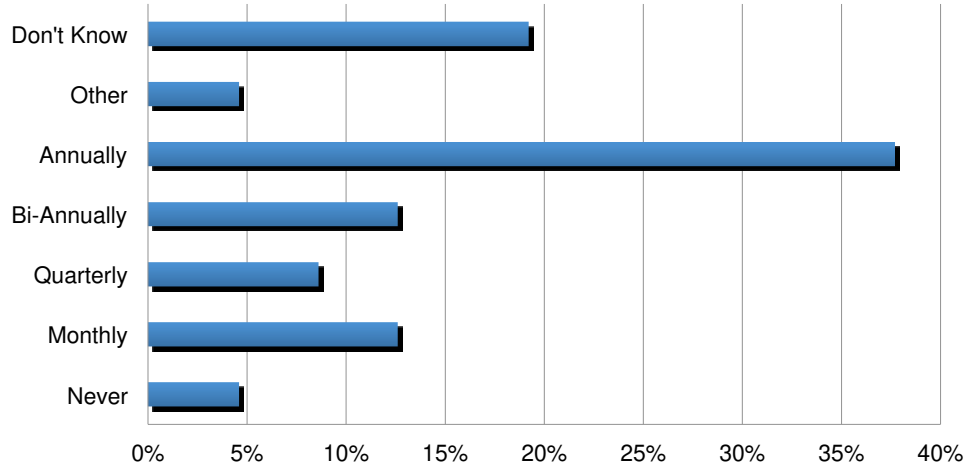
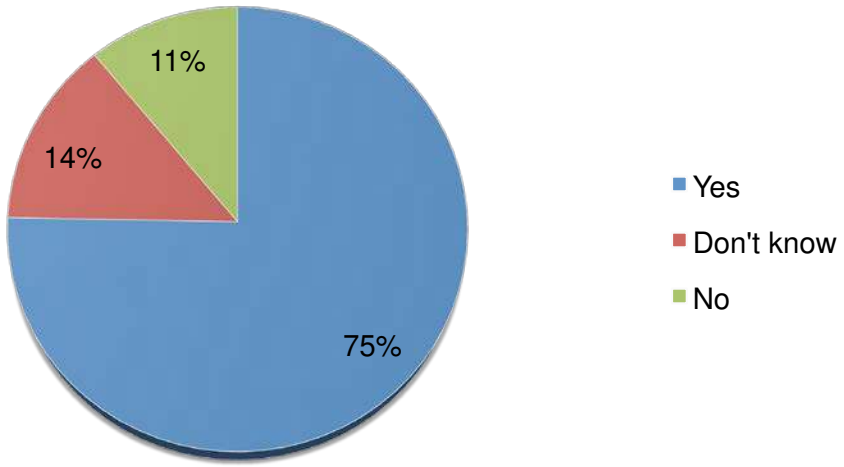


EXHIBIT 4:

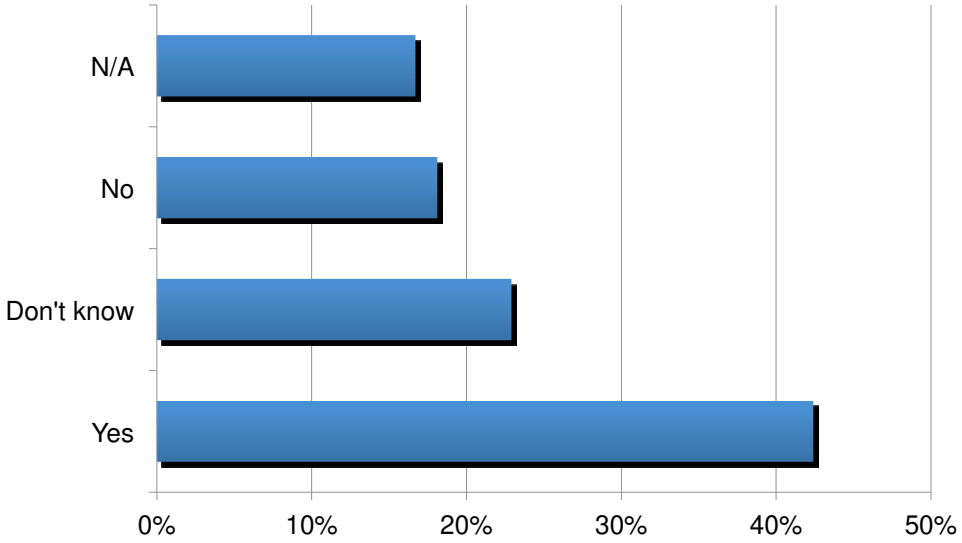
DO YOU HAVE A DATA BREACH INCIDENT RESPONSE PLAN?



Interestingly, however, while most organizations proactively develop and update their plans for effective data breach response, many do not test the effectiveness of the plan. Respondents who said that they have developed a data breach response plan were asked whether the plan has been tested. Forty-two percent said yes but a nearly equal 41 percent said no or that they did not know (Exhibit 5).

EXHIBIT 5:

IF YOU DO HAVE A DATA BREACH INCIDENT RESPONSE PLAN, HAS IT BEEN TESTED?



ACCORDING TO THE DATA THIS COULD CERTAINLY BE A POSSIBILITY SINCE MOST ORGANIZATIONS (60 PERCENT) CONTINUE TO LEAN ON THE IT DEPARTMENT FOR MANAGING THE DATA BREACH RESPONSE.

This leads to the question, why would organizations make the effort to develop a data breach response plan but not make the effort to test the plan's effectiveness? Could it be that the incident response plan is being tested but there is disconnect or lack of communication between the risk management and technology departments? According to the data this could certainly be a possibility since most organizations (60 percent) continue to lean on the IT department for managing the data breach response.[4]

This, however, leads to yet another question about the structure of the plan and the participants of the data breach response team. Cybersecurity experts recommend that a breach response team consist of a cross-section of internal personnel as well as external members. Data breach response teams often include executive management, legal, privacy/compliance, IT, information security, risk management, and other stakeholders from the company's various business units. External members often include privacy counsel, computer forensics and breach response specialists, and a crisis management firm.

Another and more likely scenario is that most organizations are simply ill prepared to manage data breach risks due to inadequate resources.

DATA BREACH RESPONSE – IS CYBER INSURANCE ENOUGH?

The survey respondents who experienced at least one data breach over the previous twelve months were asked the average size (# of records lost) of the breaches. Of the responses provided, the average was 2,200 records, however,

[4] Appendix: Exhibit 4 – "What role within your organization is responsible for managing the data breach response?"

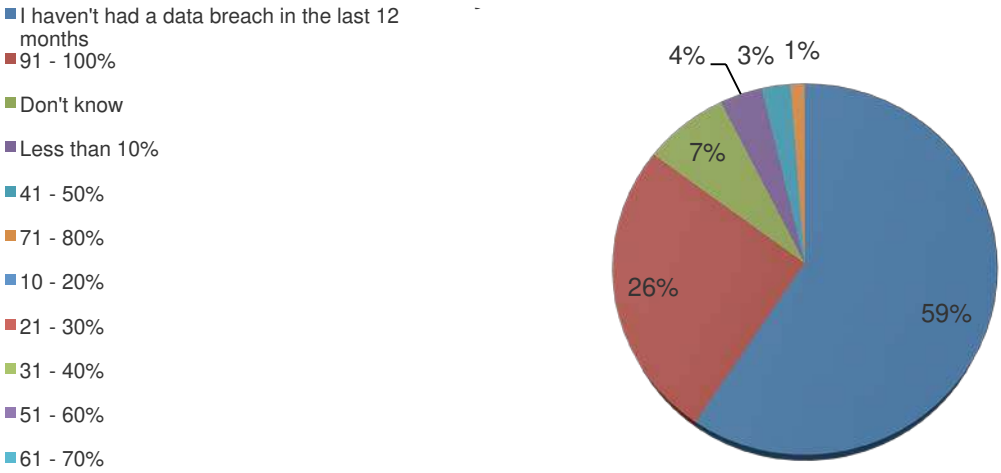
WHILE IT CERTAINLY HAS A ROLE TO PLAY, A SOLE RELIANCE ON IT CAN EXPOSE ORGANIZATIONS TO FINANCIAL LOSS AS BREACHES OFTEN REQUIRE PRIVACY AND REGULATORY COMPLIANCE. FOR THIS REASON, CYBERSECURITY EXPERTS SUGGEST THAT WHILE IT NEEDS TO BE INVOLVED RESPONDING TO A DATA BREACH IS NOT SOMETHING IT SHOULD OWN SOLELY.

the vast majority were small consisting of fewer than 500 records. The median was 100. Responding to small breaches can sometimes create challenges for organizations, including those that have cyber insurance (64 percent) because they fall beneath the minimum threshold required to trigger coverage[5].

In fact, of the respondents who purchase cyber insurance and have identified a data breach in the previous twelve months, nearly all fell below their deductibles (Exhibit 6)[6]. While cyber coverage is increasingly viewed as an essential part of many corporate insurance programs, it is designed to protect against low frequency but high severity occurrences.

EXHIBIT 6:

IN THE LAST 12 MONTHS WHAT PERCENTAGE OF YOUR DATA BREACHES FELL BELOW YOUR DEDUCTIBLE?



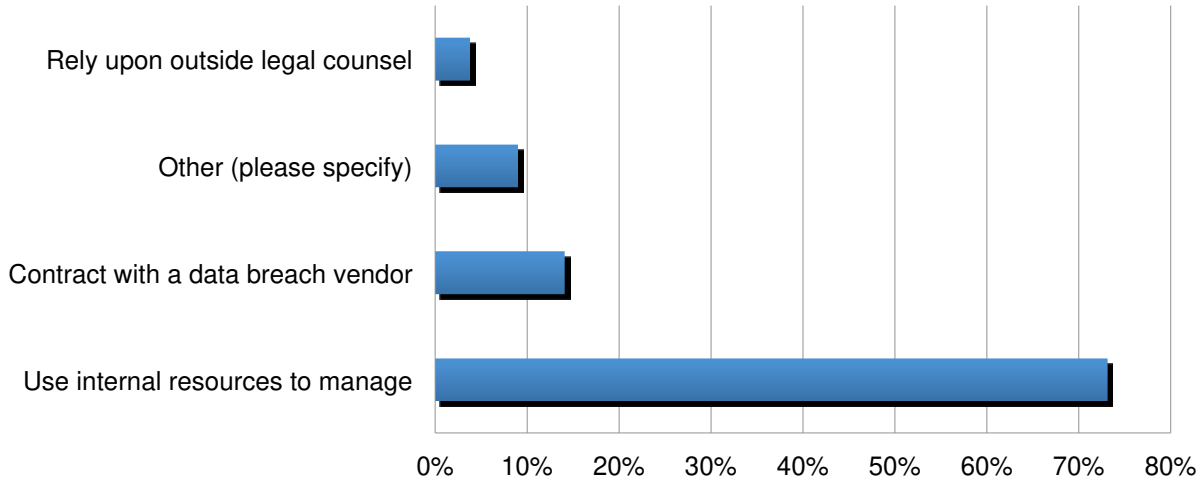
The vast majority of respondents said that they use internal resources to manage these small but high frequency claims that fall below their deductible (Exhibit 7). In fact, as noted previously, 60 percent of respondents said it is the IT department's responsibility to manage the breach response. While IT certainly has a role to play, a sole reliance on IT can expose organizations to financial loss as breaches often require privacy and regulatory compliance. For this reason, cybersecurity experts suggest that while IT needs to be involved responding to a data breach is not something it should own solely.

[5] Appendix: Exhibit 5 – "Do you purchase cyber liability insurance?"

[6] Appendix: Exhibit 6 – "How much is your deductible?"

EXHIBIT 7:

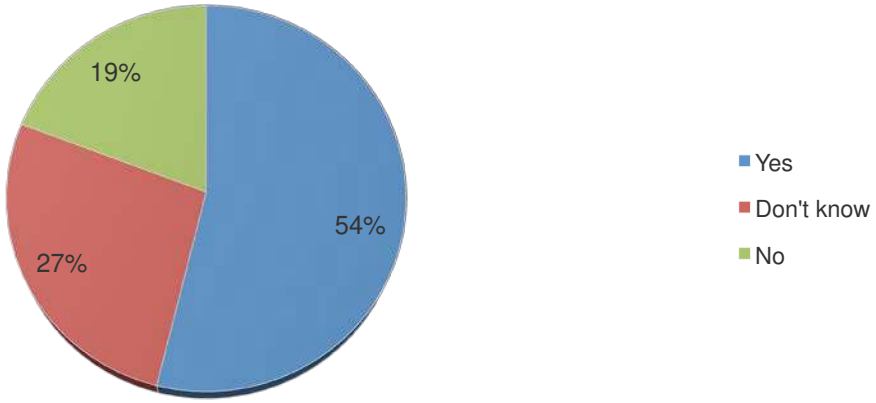
HOW DO YOU MANAGE SMALL BREACHES THAT FALL BELOW YOUR DEDUCTIBLE?



Cyber insurance is a relatively new coverage and the number of claims filed is comparatively few compared with more mature lines of business.[7] But in reality, even if a data breach is large enough to trigger coverage under a cyber insurance policy, organizations will still often be required to assume some of the financial burden. For example, the cost of the breach could have exceeded the amount of coverage purchased, or the losses could have fallen under one of the policies exclusions such as intellectual property, infrastructure, and/or reputational loss (Exhibit 8).

EXHIBIT 8:

DO YOU BELIEVE YOUR LIMITS ARE ADEQUATE FOR A LARGE DATA BREACH?

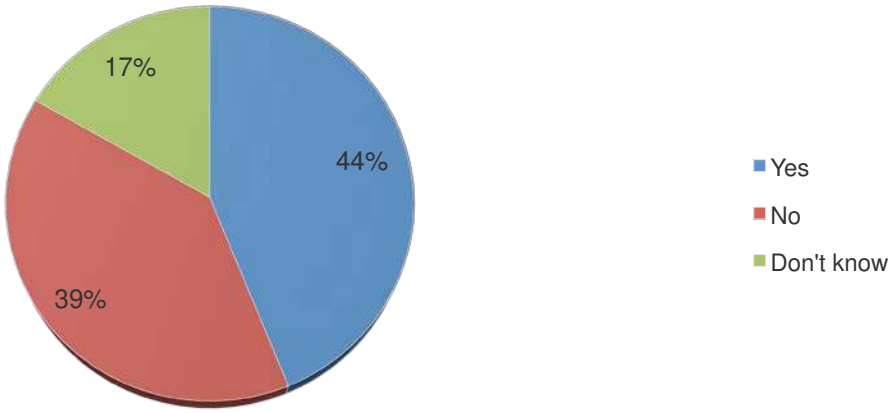


In addition to loss indemnification, cyber policies also provide access to a variety of tools and services such as risk assessment tools, data breach incident response plans, and educational resources, to help manage cyber security risks. Seventy percent of respondents said that their policy offers free tools to help manage their cybersecurity risks. Forty-four percent of the respondents said they have used them (Exhibit 9).

[7] Appendix: Exhibit 7 – "Have you ever had to file a claim under your cyber policy?"

EXHIBIT 9:

IF YOUR POLICY DOES OFFER FREE TOOLS, HAVE YOU USED THEM?



DATA BREACH RESPONSE – VENDOR SERVICES

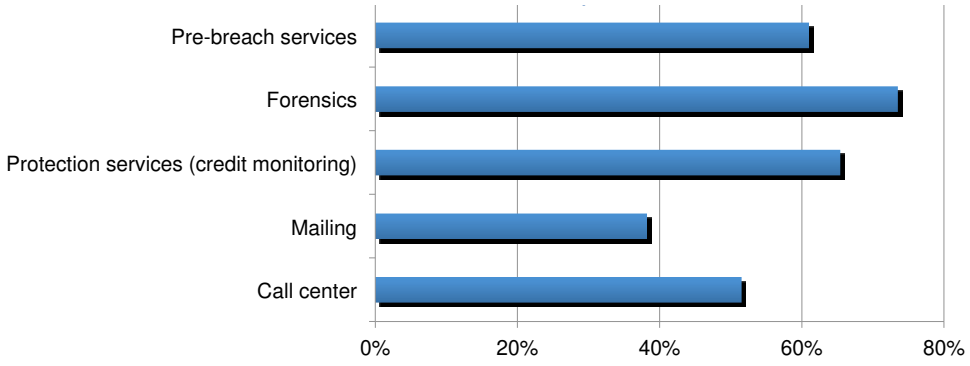
To cost effectively manage coverage gaps, many organizations who lack the resources and/or knowledge in-house, can benefit from the expertise provided by a full-service vendor equipped to manage a large breach response effort while minimizing reputational, regulatory, and litigation risks. Respondents were asked whether they have selected data breach response vendors. Fifty-one percent said yes but a nearly equal 49 percent said no or that they did not know.[8]

Respondents who had selected data breach response vendors were then asked how they made the selection. Fifty-nine percent chose their own vendors while the remaining 41 percent said their vendors were provided through their cyber insurance program.

Regardless of how they are chosen, breach response vendors offer a variety of services that mitigate cybersecurity risk and supplement cyber insurance policies by effectively managing exposures that are not covered by the policy. According to respondents the services that are most important are forensics (74 percent), protection services (65 percent), pre-breach services (61 percent), call center (51 percent), and mailing (38 percent) (Exhibit 10). Of which the vast majority (74 percent) would prefer to receive from a single vendor.

EXHIBIT 10:

WHAT SERVICES DO YOU THINK ARE MOST IMPORTANT FOR YOUR DATA BREACH RESPONSE VENDORS TO PROVIDE? (SELECT ALL THAT APPLY)



[8] Appendix: Exhibit 8 – "Do you have data breach response vendors selected?"

ABOUT THE SURVEY RESPONDENTS

Advisen and ID Experts collaborated on a survey designed to understand how organizations prepare and respond to data breach threats. Invitations to participate were distributed via email to risk managers, insurance buyers and other risk professionals. The survey was completed at least in part by 203 risk professionals.

The majority of respondents classified themselves as either Chief Risk Manager/Head of Risk Management Department (41 percent), or Member of Risk Management Department (not head).[9]

Thirteen macro industry segments are represented. Healthcare has the highest representation accounting for 22 percent of the total respondents. Other well represented industries include industrials at 13 percent, government and nonprofit at 12 percent, consumer discretionary at 10 percent, and professional services at 9 percent.[10]

The survey represents businesses of all sizes. Twenty-five percent of respondents have more than 15,000 employees, 23 percent have between 1,001 and 5,000, 22 percent have between 5,001 and 15,000, 17 percent have less than 500, and 13 percent have between 500 and 1,000 employees.[11]

The survey is also represented by businesses across all regions of the United States. Twenty-eight percent are located in the Northeast, 23 percent in the Southeast, 17 percent in the Midwest, 13 percent in the West, and 10 percent come from the Southwest.[12]

---

[9] Appendix: Exhibit 9 – "Which of the following best describes your role within your organization?"

[10] Appendix: Exhibit 10 -- "What is your industry?"

[11] Appendix: Exhibit 11 – "How many employees does your company have?"

[12] Appendix: Exhibit 12 – "Where are you located?"

APPENDIX:

EXHIBIT 1:

HOW DO YOU ASSESS YOUR CYBER SECURITY RISK?

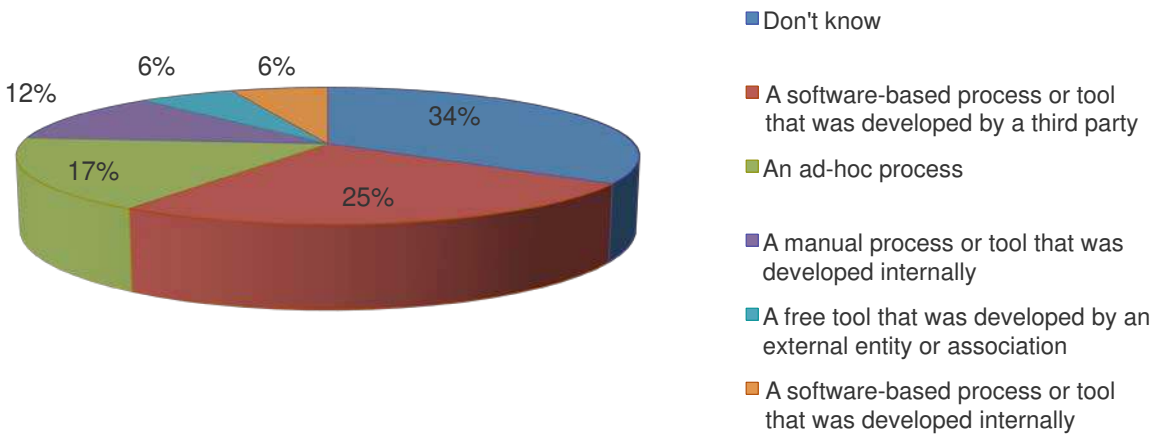


EXHIBIT 2:

DO YOU ACTIVELY UPDATE THE FOLLOWING?

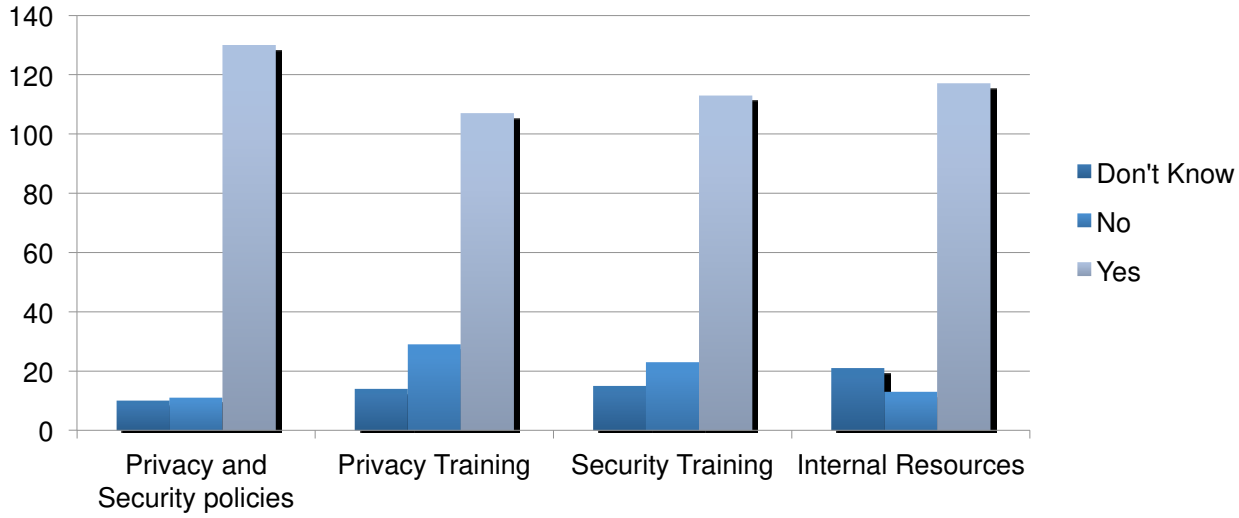


EXHIBIT 3:

DO YOU HAVE A DATA BREACH INCIDENT RESPONSE TEAM?

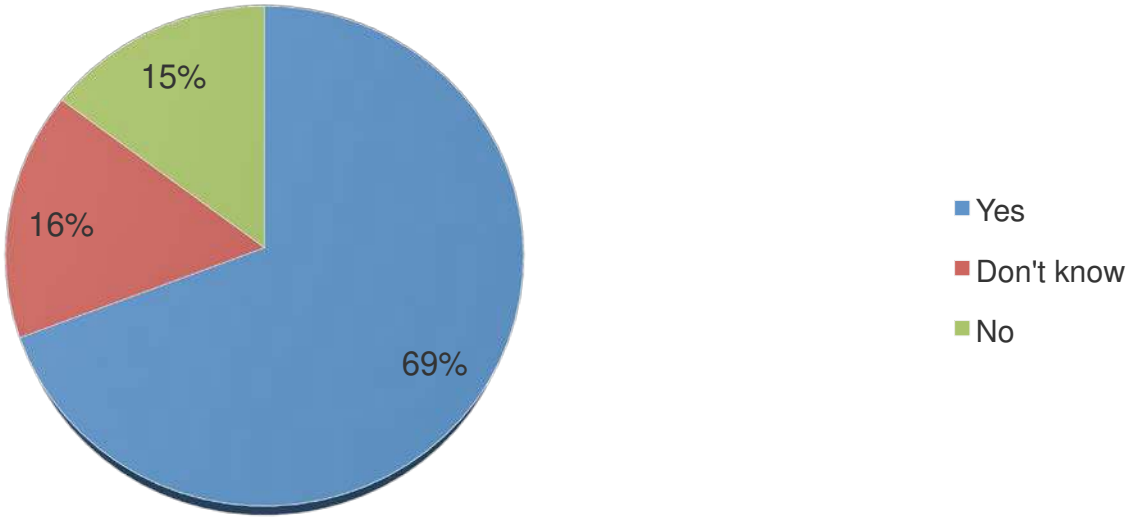


EXHIBIT 4:

WHAT ROLE WITHIN YOUR ORGANIZATION IS RESPONSIBLE FOR MANAGING THE DATA BREACH RESPONSE?

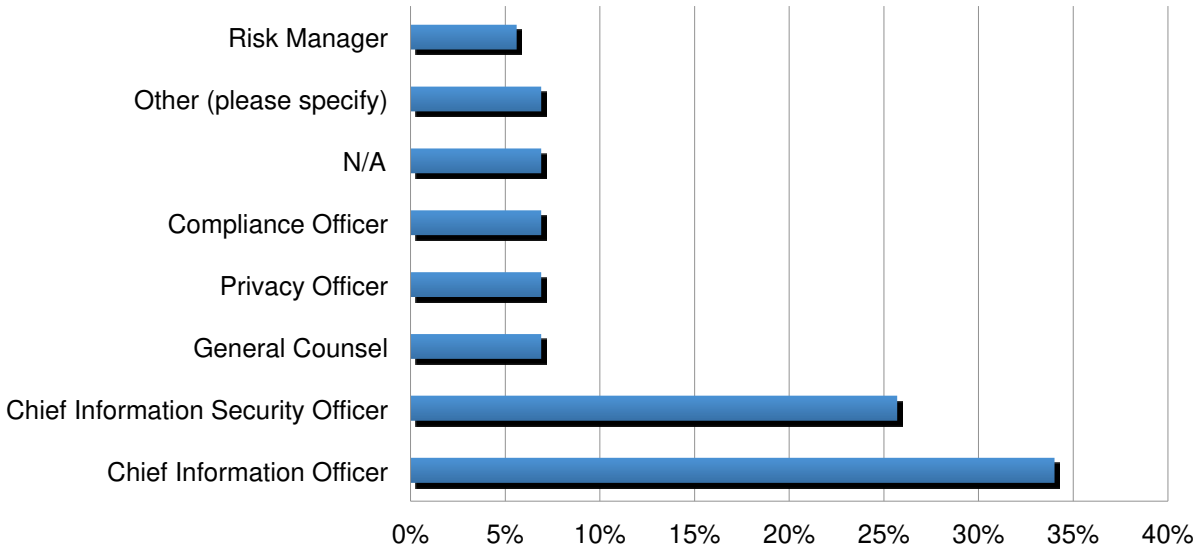


EXHIBIT 5:

DO YOU HAVE CYBER LIABILITY INSURANCE?

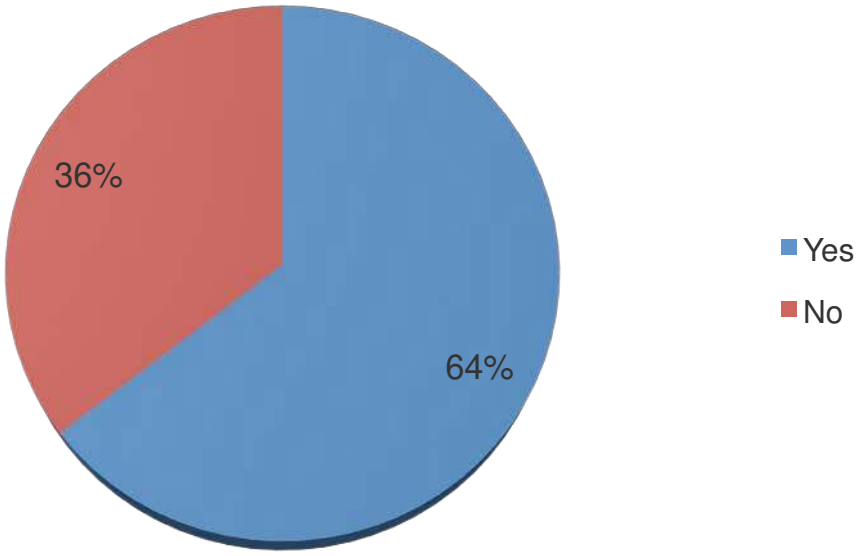


EXHIBIT 6:

HOW MUCH IS YOUR DEDUCTIBLE?

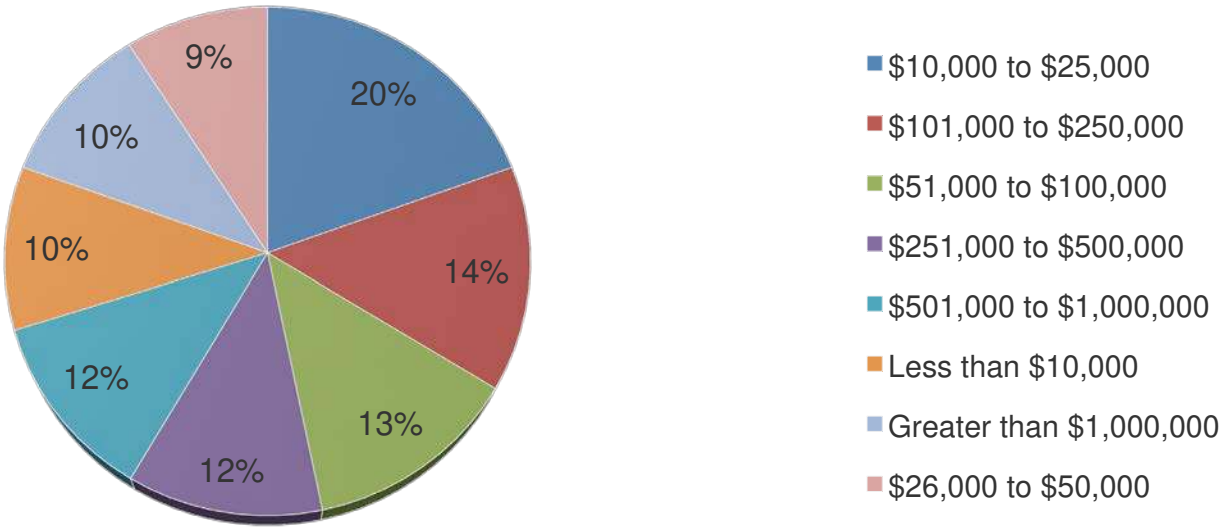


EXHIBIT 7:

HAVE YOU EVER HAD TO FILE A CLAIM UNDER YOUR CYBER POLICY?

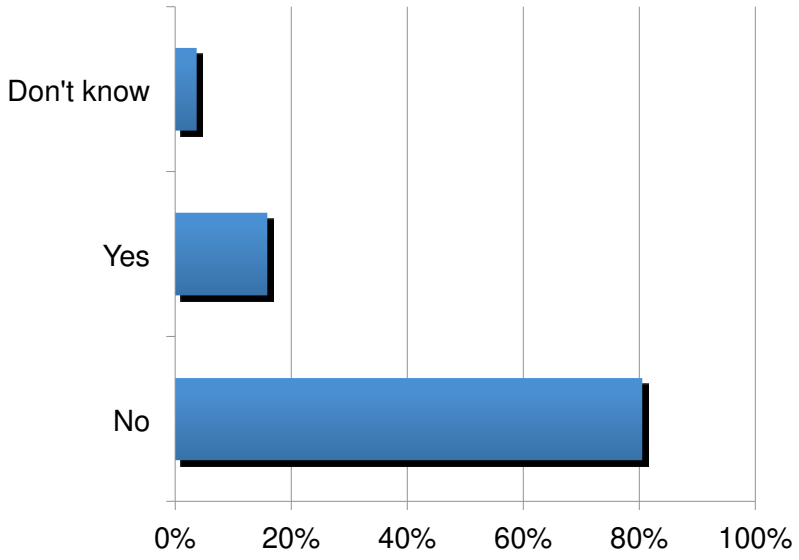


EXHIBIT 8:

DO YOU HAVE DATA BREACH RESPONSE VENDORS SELECTED?

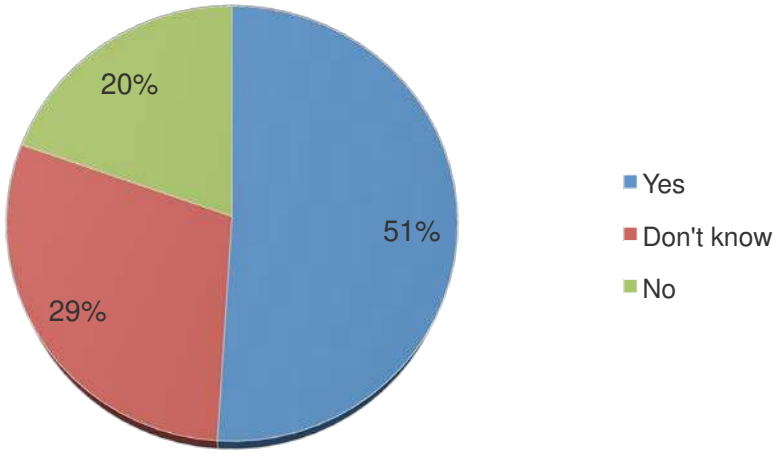


EXHIBIT 9:

WHICH OF THE FOLLOWING BEST DESCRIBES YOUR ROLE WITHIN YOUR ORGANIZATION?

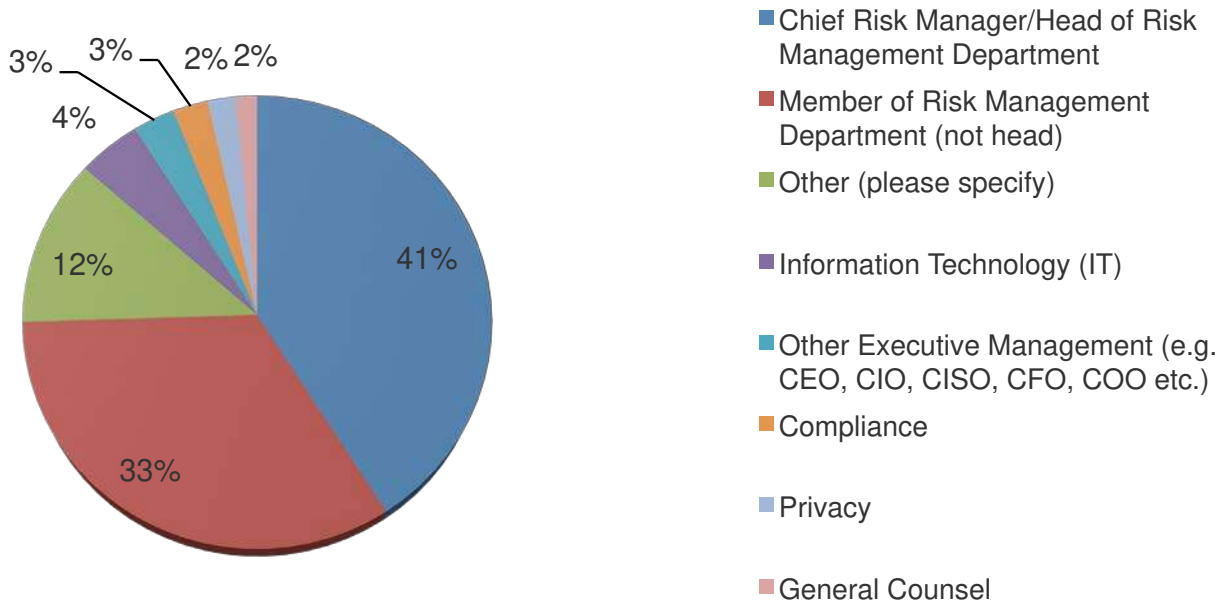


EXHIBIT 10:

WHAT IS YOUR INDUSTRY?

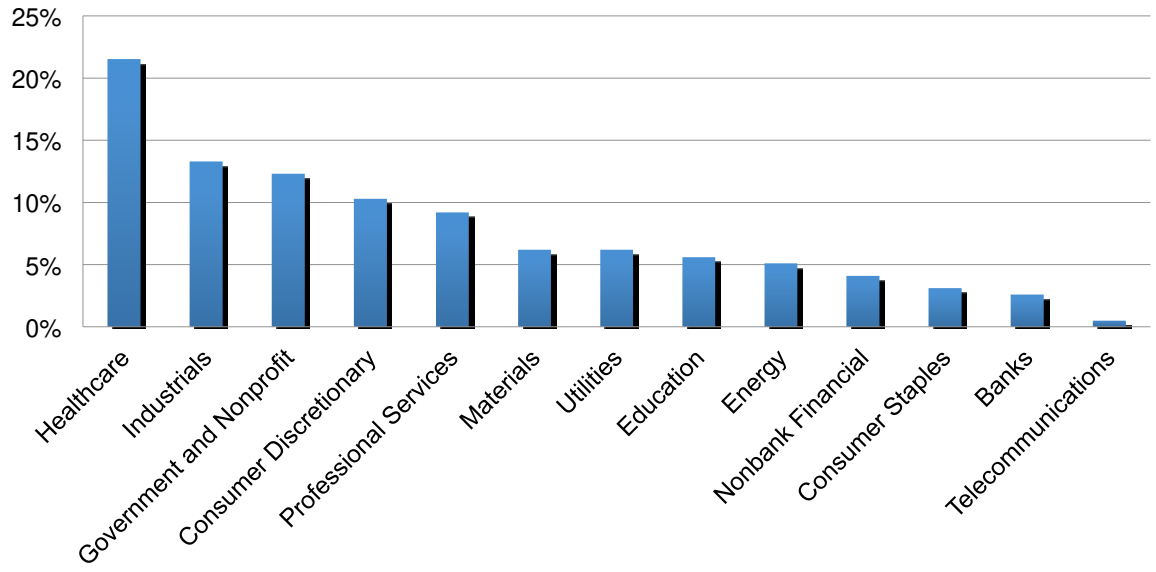


EXHIBIT 11:

HOW MANY EMPLOYEES DOES YOUR COMPANY HAVE?

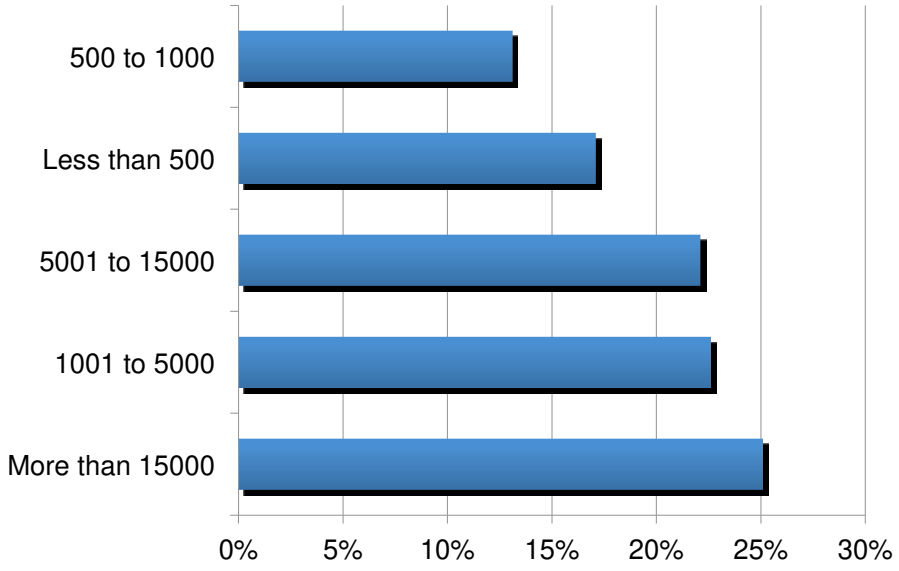


EXHIBIT 12:

WHERE ARE YOU LOCATED?