CYBERSECURITY PREPAREDNESS AND RESPONSE

A MIDDLE MARKET RISK MANAGEMENT PERSPECTIVE

Sponsored by THE HARTFORD

by Josh Bradford, Senior Editor, Specialty Editorial

TABLE OF CONTENTS

SURVEY OVERVIEW

The Hartford collaborated with Advisen on a comprehensive survey of middle market risk professionals. The purpose of the study was to gain insight into the cybersecurity preparedness and response strategies of businesses with revenues/ budgets between $15 million to under $1 billion.

The survey revealed that cyber risk is without question a concern of middle market businesses. In fact, 90 percent of respondents said their company's senior management is at least moderately concerned. But according to risk professionals, this concern has yet to fully translate into privacy and security investments and focus.

The survey also revealed that risk professionals see substantial room for improvement in the cybersecurity efforts of their organizations. It identified concerns over the ability to respond to a cyber-related crisis, and revealed questions about the competency of privacy risk identification and response.

Additionally, the survey discovered a continuing disconnect between information technology (IT) and risk management with regards to privacy and security in middle market companies. It also identified an inability to quickly adjust to the evolving cyber risk landscape.

Taken as a whole, there continues to be low hanging vulnerabilities which are not addressed in the middle market space. This survey is meant to highlight some of these vulnerabilities and provide risk professionals with a tool to help mitigate both privacy and security risk.

> Cyber risk is a real concern of middle market businesses, but hasn't yet fully translated into privacy and security investments and focus.

continued

KEY FINDINGS

29% Risk professionals are most confident in their network protection capabilities with 29 percent giving themselves "A" grade

9% Risk professionals are least confident in vendor management with only 9 percent giving themselves "A" grade

41% 41 percent of organizations who do not employ a dedicated privacy professional do so because they believe privacy is adequately addressed elsewhere within the organization

8% Of the organizations who conducted privacy impact assessments only 8 percent say that they have been extremely effective at identifying privacy risks

56% Of the privacy risks that have been identified by a privacy impact assessment, 56 percent of the organizations have put a formal plan in place to address most or all of them

85% / **8%** 85 percent of risk professionals say their company's senior management is at least moderately concerned about cyber risk but only 8 percent say they are extremely concerned

9% Only 9 percent of risk professionals feel their company is extremely well-positioned to respond to a cyber-related crisis

66% 66 percent of risk professionals expect their company to spend more on cyber protections in 2016 compared to 2015

41% / **28%** / **52%** 41 percent of risk professionals don't know what types of information their company stores on the cloud, 28 percent don't know what went into selecting their cloud service provider(s), and 52 percent don't know if their company chose to purchase privacy and security services as an add-on to the base cloud agreement

59% 59 percent of organizations have a cyber incident response plan. 55 percent of organizations have tested the plan.

76% 76 percent don't have or don't know if their company has a formal plan in place for dealing with a cyber extortion demand

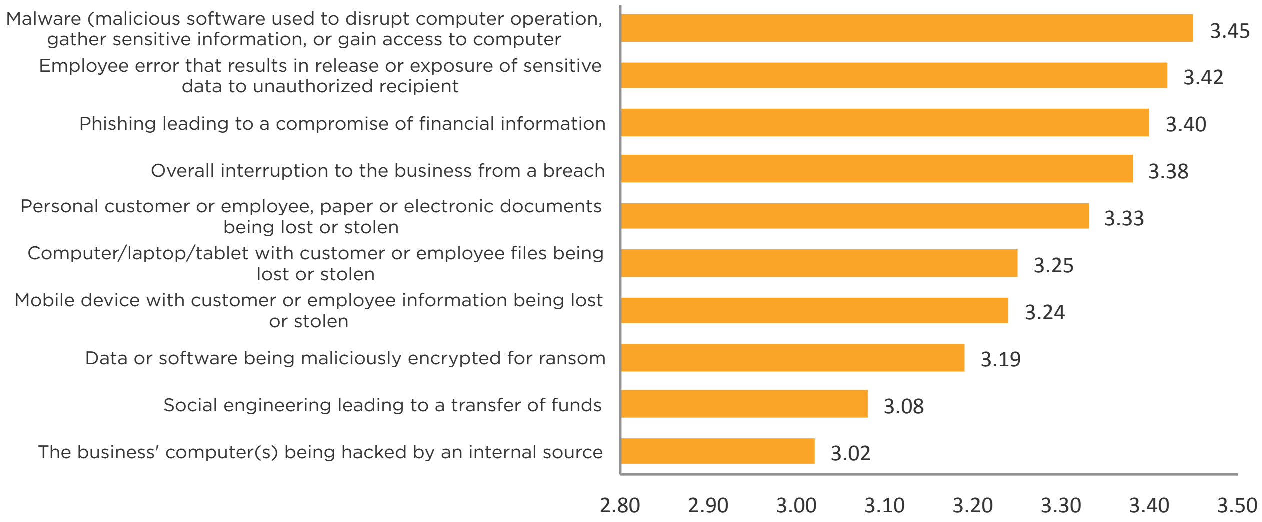
85% **85 percent of risk professionals say their company's senior management is at least moderately concerned about cyber risk. But only 8 percent say they are extremely concerned.**

CYBER RISK: A SELF-ASSESSMENT

Risk professionals believe executive management is concerned but not yet panicking about cyber risk. Just over 50 percent of respondents rated executive management's level of concern as strong or higher. (Appendix Exhibit 1)

According to respondents, executive management's top cyber-related concerns are malware, employee error resulting in release or exposure of sensitive data to an unauthorized recipient, and phishing leading to a compromise of financial information. (Exhibit 1)

Exhibit 1: For each of the following cyber risks, rate the level of concern you feel the senior management of your organization has for it.



But do risk professionals believe their company is prepared to protect against and respond to these threats? And, are the concerns at the executive management level translating into investments?

To answer these questions respondents were asked to compare the cybersecurity efforts of their company to the best they believe companies like theirs could do. They were asked to grade themselves on 10 unique cybersecurity functions.

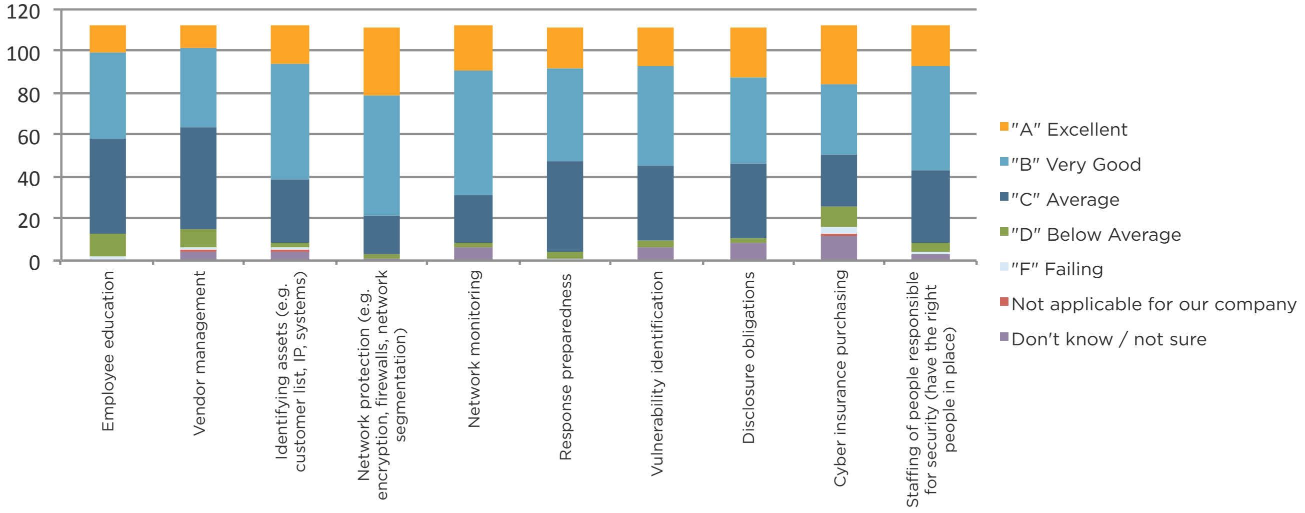
Do risk professionals believe their company can protect against cyber threats? Respondents graded themselves in 10 cybersecurity categories.

The vast majority of respondents graded themselves a "C" (average) or better for each function, though few gave themselves an "A" (excellent). The low percentage of "A" grades is an indication that while cyber risk is on the radar of most middle market organizations, increased focus and investment is needed at the executive management level to sure up defenses.

According to risk professionals, their company's biggest vulnerability is their inability to manage vendors with only 9 percent giving "vendor management" an "A" grade. This was followed by employee education at 12 percent, and identifying assets (e.g. customer list, IP, systems) at 16 percent.

Conversely, respondents are most confident in their company's network protection capabilities (e.g. encryption, firewalls, network segmentation) with 29 percent grading themselves an "A", followed by cyber insurance purchasing at 25 percent. (Exhibit 2)

Exhibit 2: How would you grade your company on each of the following cybersecurity efforts compared to the absolute best you believe companies like yours could do it?



According to risk professionals, their company's biggest vulnerability is their inability to manage vendors.

CYBER RISK: PREPAREDNESS

Privacy

In the context of cybersecurity, privacy involves establishing processes and procedures around the collection and usage of personal information. These processes have become increasingly important due to the growing cost of a privacy breach. Adequately addressing privacy risk, however, requires a substantial upfront investment.

About half of the surveyed organizations have invested in personnel dedicated to the issue of privacy. (Appendix Exhibit 2) The companies without a dedicated privacy professional said the leading reason is that privacy is adequately addressed elsewhere within the organization (41 percent). (Appendix Exhibit 3)

Nearly three quarters of respondents report having conducted a formal privacy impact assessment in the past five years for at least some business functions, new products, and new initiatives. (Appendix Exhibit 4) A privacy impact assessment (PIA) is defined by the U.S. government as an analysis of how personally identifiable information is collected, stored, protected, shared, and managed.

The largest percentage of respondents (28 percent) said the assessments are conducted annually. A noticeably high 33 percent, however, did not know the frequency by which they occurred. (Appendix Exhibit 5) The high percentage of uninformed risk professionals could indicate a communication breakdown between risk management and information technology (IT) departments.

While privacy risk is on the radar of most organizations, many risk professionals question their organization's competency in privacy-risk identification and response. Respondents who conduct privacy impact assessments were asked their effectiveness at identifying privacy risks; only 39 percent believed they were very or extremely effective. (Exhibit 3)

Nearly 75% of respondents report having conducted a formal privacy assessment.

Exhibit 3: How effective has your privacy impact assessment(s) been at identifying privacy risks?

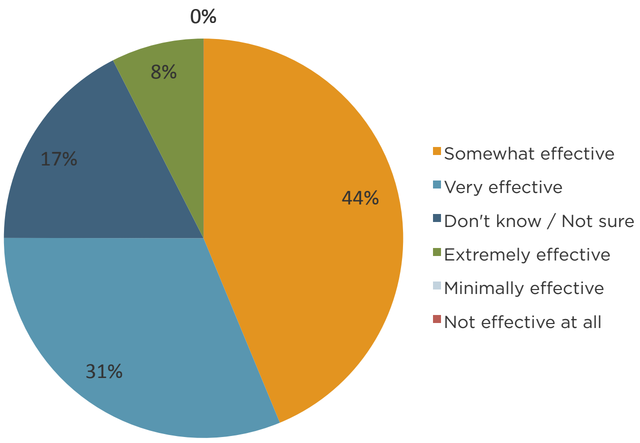
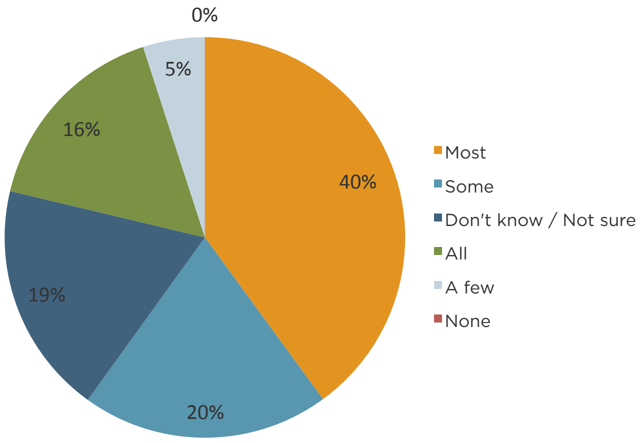


Exhibit 4: Approximately how many of the risks identified by the privacy impact assessment(s) had a formal plan put in place to address them?



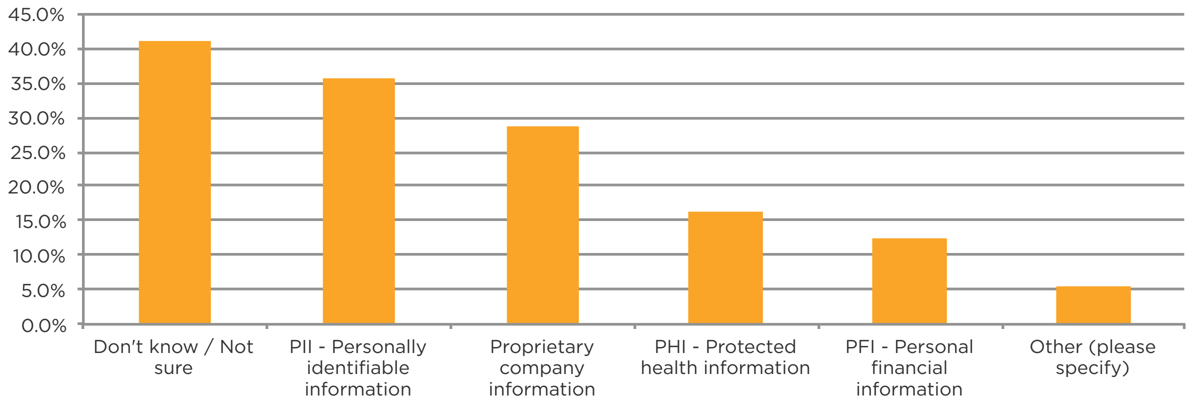
Additionally, only 16 percent said a formal plan has been implemented for "all" of the risks identified by the privacy impact assessment. (Exhibit 4) These are both indications that senior management's cyber risk concerns may not fully be translating into cyber risk investment and focus.

PRIVACY AS A SERVICE

The vast majority of surveyed organizations now utilize cloud services. (Appendix Exhibit 6) Cloud services are defined as services made available to users on demand via the internet from third party servers.

Respondents who utilize cloud services were asked the types of information their company stores on the cloud. Forty-one percent said they don't know or were not sure. (Exhibit 5) This high percentage of unknowns is yet another indication of disconnect between risk professionals and the information technology department. Disconnect that could expose organizations to loss.

Exhibit 5: Which types of information does your company store on the cloud service(s)? (Select all that apply)



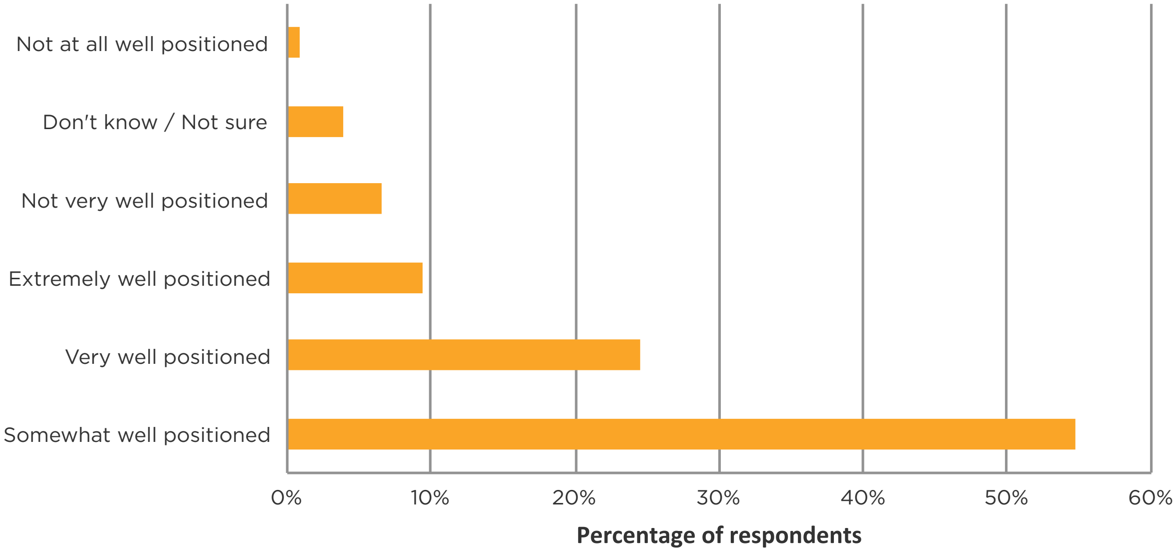
Additionally, a high percentage of respondents (29 percent) did not know what went into selecting their organization's cloud service provider, or if their company chose to purchase privacy and security services as an add-on to the base cloud agreement (52 percent). (Appendix Exhibit's 7 and 8)

> Organizations that "don't know" what information is stored by a cloud service provider could be exposed to loss.

CYBER RISK: RESPONSE

Most risk professionals do not believe they are adequately prepared for a cyber-related crisis. Only 9 percent believe their company is extremely well positioned. The majority (55 percent) say they are somewhat well positioned. (Exhibit 6)

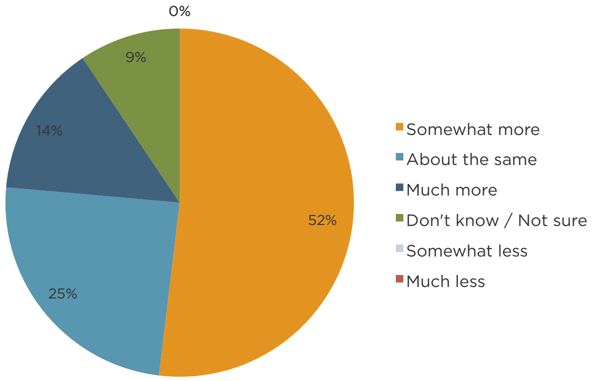
Exhibit 6: How well prepared do you feel your company is to respond to a cyber-related crisis?



Heightened cyber risk focus and awareness at the executive level could increase risk professionals confidence in this area. In previous year's executive management's cyber-risk concerns have rarely translated into substantial investments in the middle market segment.

This lack of cyber risk investment and focus, however, could be on the verge of changing. For example, survey respondents were asked how their company's spend on cyber protections in 2016 will compare to 2015, 64 percent said they expect to spend more. (Exhibit 7)

Exhibit 7: How will your company spend on cyber protections in 2016 compare to 2015? In 2016, do you think your company will spend…



CYBER INCIDENT RESPONSE PLAN

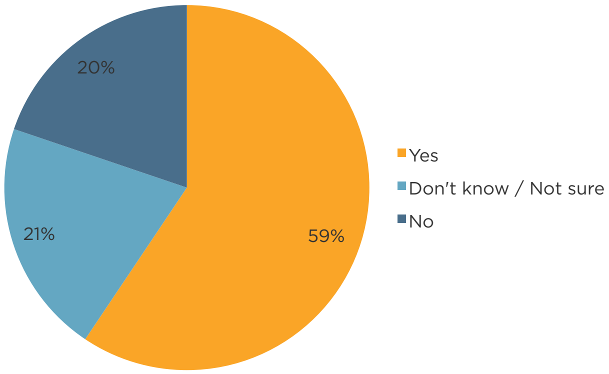
The likelihood an organization will at some point be impacted by a cybersecurity incident continues to grow. Whether caused by a bad actor, a breach of internal protocol, or simply by accident — when an incident occurs the financial consequences can be severe.

Various studies have revealed organizations with a tested cyber incident response plan fare much better during a cyber-related crisis. With this in mind, respondents were asked if their company has a formal cyber incident response plan. Sixty percent said yes, 20 percent said no, and a surprisingly high 21 percent don't know. (Exhibit 8)

The high percentage of respondents who don't know provides yet another example of a potential disconnect between the risk management and information technology departments of some middle market companies.

> Organizations with a tested cyber incident response plan fare much better during a cyber-related crisis.

Exhibit 8: Does your company have a formal cyber incident response plan?



The respondents who have a formal cyber incident response plan were asked if the plan has been tested. Fifty-five percent said yes, 32 percent said no, and 13 percent said don't know. (Appendix Exhibit 9) Cyber incident response testing and updates most frequently occur on an annual basis. (Appendix Exhibits 10 & 11)

EMERGING THREAT (CYBER EXTORTION)

The cyber risk landscape is constantly evolving. One emerging threat has proven lucrative for cyber criminals and a challenge for businesses is cyber extortion.

Cyber extortion is an attack or threat combined with a demand for money to avert or stop the attack. To execute cyber extortion, cyber criminals increasingly rely on a type of malicious software called ransomware.

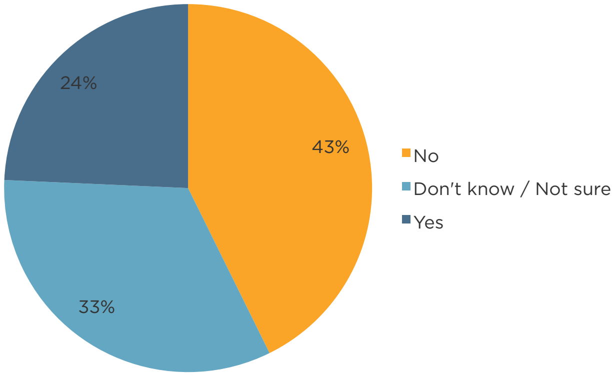
In recent months a wave of high profile ransomware attacks has been reported, most notably against the healthcare sector. It was with this in mind respondents were asked a series of questions on this emerging threat.

The good news is the vast majority of respondents (81 percent) have yet to be a victim of cyber extortion. (Appendix Exhibit 10) However, this may be more the result of luck than the adequacy of cybersecurity postures. It could also be risk professionals are unaware the company was a victim of cyber extortion attack.

Only 24 percent said they have a formal plan in place to deal with a cyber extortion demand. (Exhibit 9) Similarly, only 20 percent know how to obtain cryptocurrency such as bitcoin, which is often the cyber extortionists' currency of choice. (Appendix Exhibit 11)

> Cyber criminals rely on malicious software called ransomware and often expect payment in bitcoin.

Exhibit 9: Does your company have a formal plan in place for dealing with a cyber extortion demand?

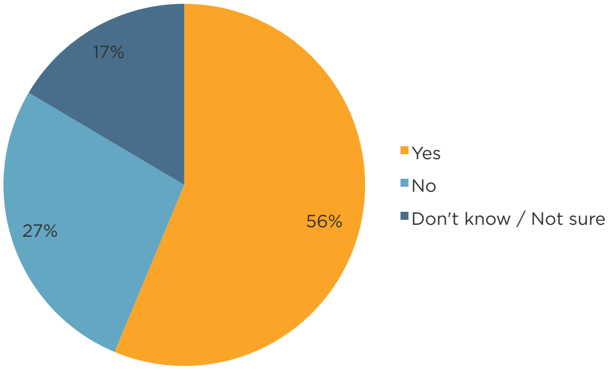


VENDOR SELECTION AND SERVICES

The effectiveness of cybersecurity preparation and response strategies often depends upon the resources a firm has in place. Rarely do firms have all the necessary expertise in-house.

Many of these services are often provided as part of a cyber liability insurance policy. Respondents were asked if their company purchases standalone cyber liability insurance. Fifty-six percent said yes, 27 percent said no, and 17 percent did not know. (Exhibit 10)

Exhibit 10: Does your company purchase standalone cyber liability insurance? This would be broader coverage than data breach coverage.



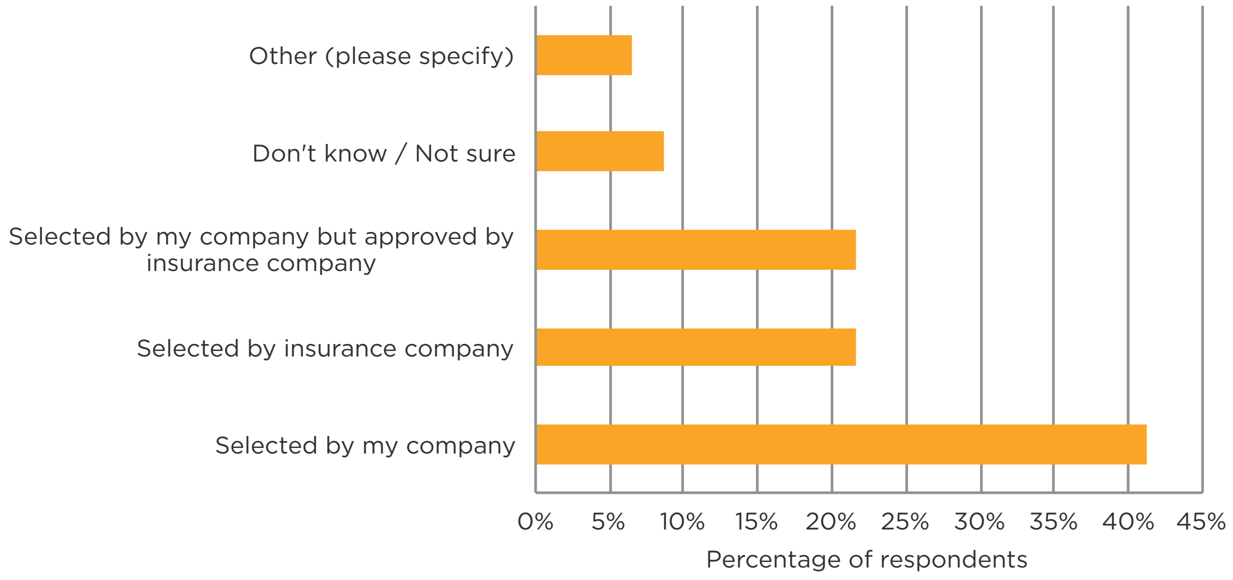
Although a substantial percentage of respondents rely on insurance as a component of their cyber-risk management programs, it appears the vendor services offered by insurers often are not utilized.

Respondents were asked if their company pre-selected third-party vendors to assist with breach preparation and response. Forty-four percent said yes, 31 percent said no, and 25 percent did not know. (Appendix Exhibit 14)

Of the respondents that have pre-selected third-party vendors, only 22 percent said they were selected by their insurance company. (Exhibit 11)

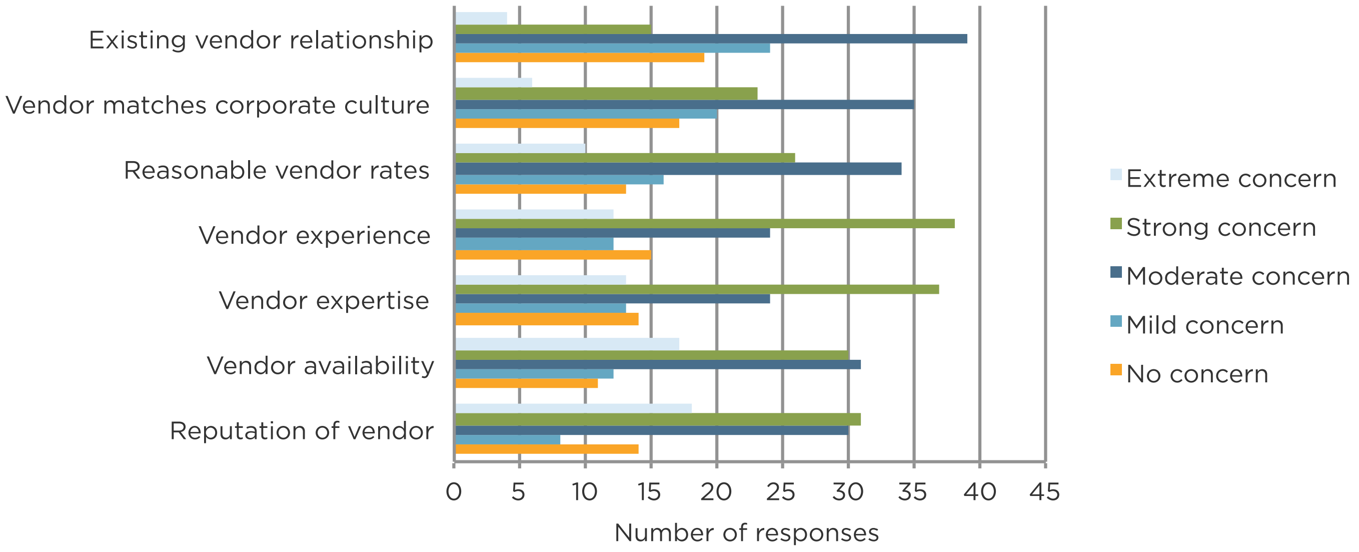
> Although respondents rely on insurance for cyber-risk management, the vendor services offered by insurers often aren't utilized.

Exhibit 11: How did your company select your data breach preparation and response vendors?



Finally, in the event of a breach, reputation was rated as the most important characteristic of a response vendor. Other important characteristics included vendor availability and expertise. (Exhibit 12)

Exhibit 12: In the event of a breach, how concerned are you about each of the following?



RECOMMENDATIONS

As evidenced by the results of this study, middle market businesses frequently leave low-hanging vulnerabilities unaddressed. Fortunately they can mitigate both privacy and security risk by taking some basic steps. Here are some recommendations from The Hartford.

1. **Build a Security-aware Organization**

   a. Cybersecurity isn't just about preventive technology; it requires the awareness and participation of everyone within the organization.

   High level security awareness is typically implemented through a top-down approach. Policies and procedures sanctioned by management convey to employees the importance of information security and the need for a collective effort.

   To learn more about how to build a security-aware organization, click here.

   b. Businesses and their employees should anticipate the real possibility of cyber extortion and take preventive measures now so they don't fall victim later. But in the unfortunate scenario that they do fall victim, it is important to understand how to respond.

   To learn more about how to respond if your company's data is taken hostage, click here.

2. **Establish Security Safeguards**

   a. Baseline measures should be put in place to help safeguard your sensitive data from unauthorized access and use.

   Small and midsize businesses (SMBs) make easy targets because they often lack the robust security that can keep hackers at bay. But there are steps SMBs can take to safeguard their sensitive data even with a limited budget.

   To learn more about what baseline measures are recommended to help safeguard SMBs' sensitive data from unauthorized access and use, click here.

   b. Most businesses do not have all the in-house security expertise to respond to and recover from a data breach. Even when they do, they often enlist the aid of outside vendors who make data breach response recovery their specialty.

   To learn more about how to form an incident response team to best meet your business needs, click here.

3. **Prepare for the Worst – Make Sure You Have an IRP**

   a. An incident response plan is designed to limit damage to your business and reduce recovery time and costs. All small and mid-size business owners should prepare an IRP.

   In order to do what it's intended to do, an IRP needs to be a living document with procedures that are tested and put into practice before your business falls victim to an attack.

   To learn more about creating and maintaining an IRP tailored to the cyber risks your business faces, click here.

Middle market businesses can mitigate both privacy and security risk by taking some basic steps.

ABOUT THE SURVEY AND RESPONDENTS

Advisen and The Hartford collaborated on a survey designed to better understand how mid-sized businesses are preparing for and responding to cybersecurity 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 131 risk professionals from companies with revenues/budgets between $15 million and $1 billion.

Most classified themselves as either Chief Risk Manager/Head of Risk Management Department (35 percent) or Member of Risk Management Department (not head) (34 percent). (Appendix Exhibit 15)

The industries represented include Healthcare at 16 percent, Financial Services and Manufacturing both at 13 percent, Technology at 9 percent, Education at 7 percent, Retail at 4 percent, Energy at 3 percent, Business & Professional, Construction and Contractors, Hospitality, Transportation, and Wholesalers & Distributers all at 2 percent, and Restaurants at 1 percent. Twenty-three percent of respondents classified themselves as Other. (Appendix Exhibit 16)

The survey represents a variety of business sizes. Forty-seven percent have revenues/budgets between $15 million to under $1 billion, 43 percent are greater than $1 billion, and 10 percent are less than $15 million. (Appendix Exhibit 17)

The survey was completed at least in part by 131 risk professionals with revenues/budgets between $15 million and $1 billion.

APPENDIX

Exhibit 1: How would you rate the overall level of concern of your company's senior management about cyber risk?

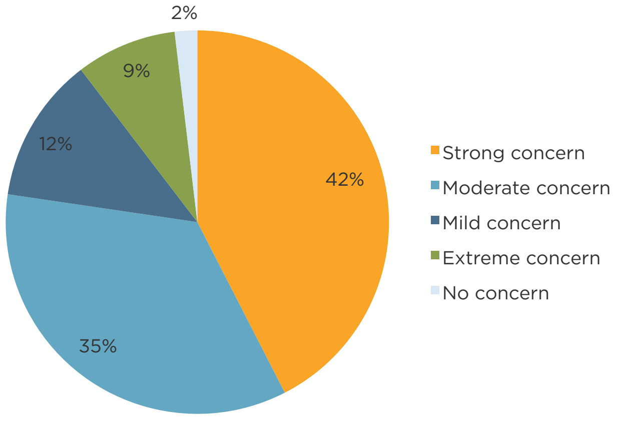


Exhibit 2: Does your company have dedicated privacy professional whose primary responsibility is privacy?

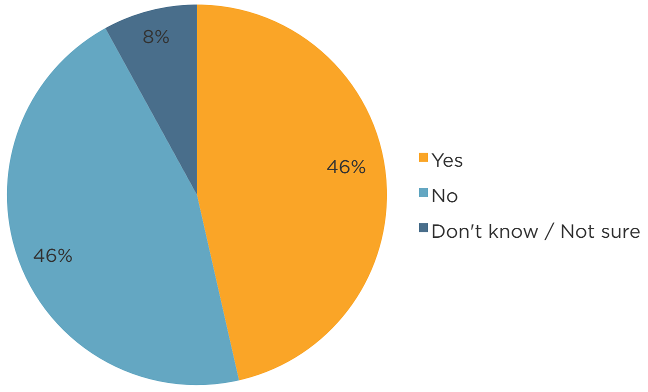


Exhibit 3: For what reasons does your company not employ a dedicated privacy professional? (Select all that apply)

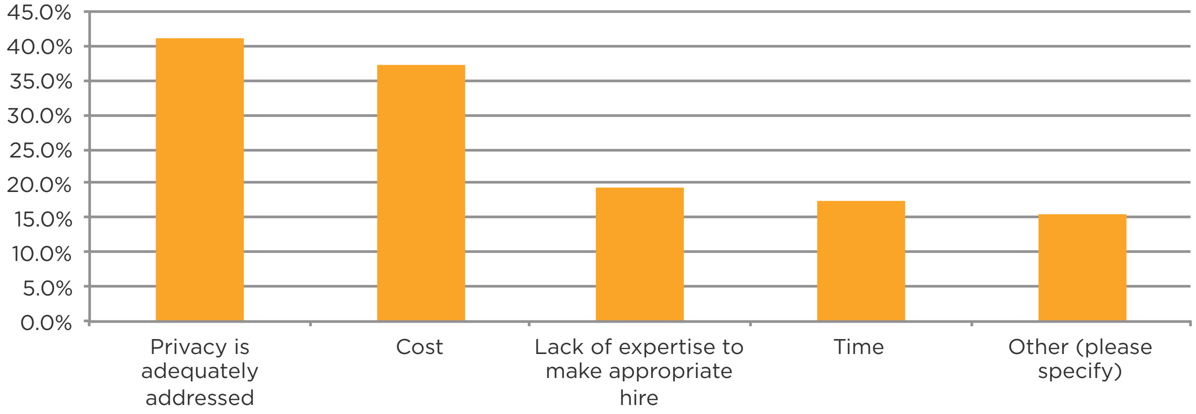


Exhibit 4: Has your company conducted a formal privacy impact assessment in the past 5 years?

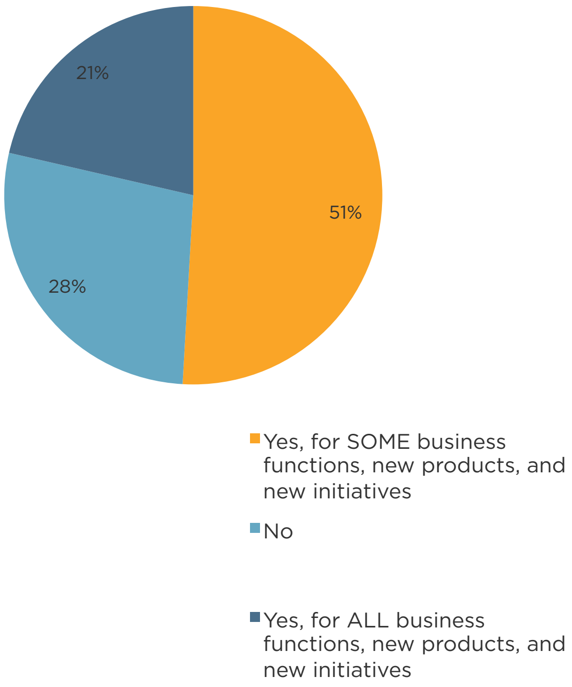


Exhibit 5: Approximately how often does your company conduct a privacy impact assessment?

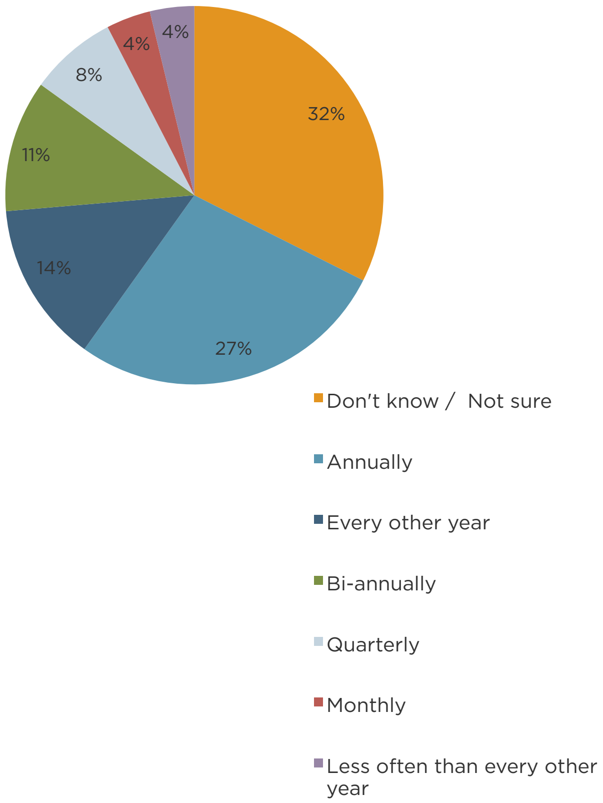


Exhibit 6: Does your company utilize any cloud services?

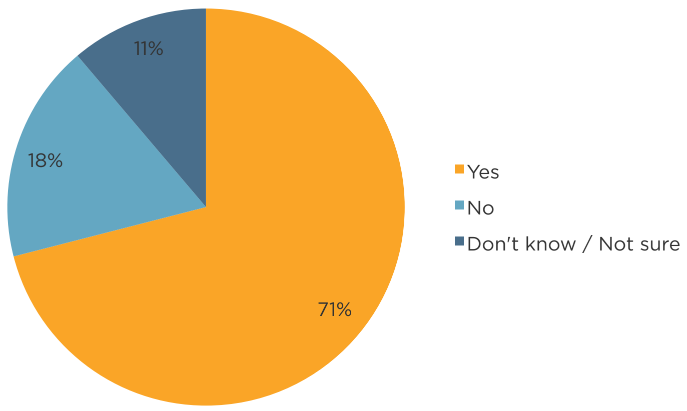


Exhibit 7: Which of the following did your company do when selecting your organization's cloud service provider(s)? (Select all that apply)

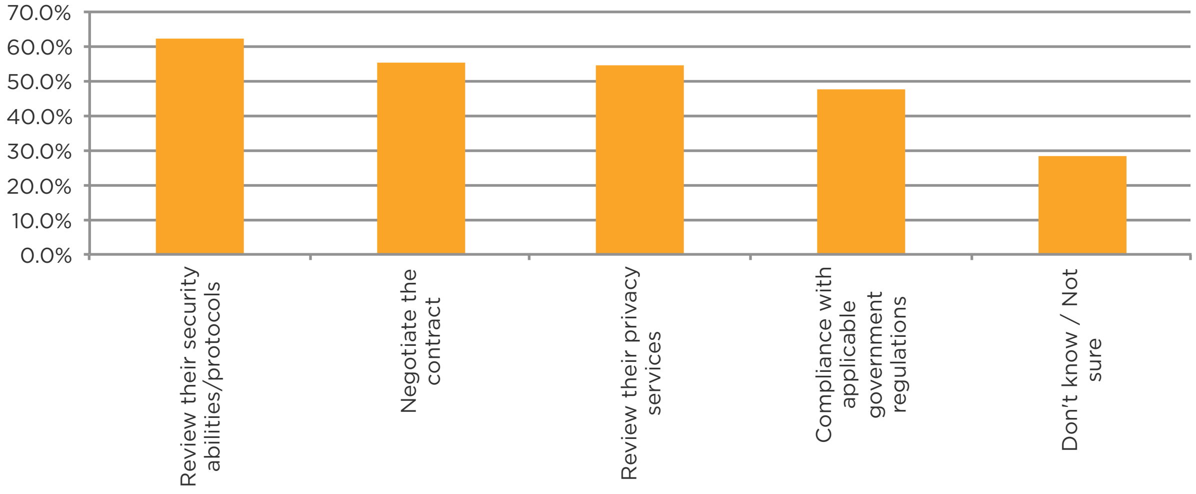


Exhibit 8: Did your company choose to purchase privacy and security services as an add-on to the base cloud agreement?

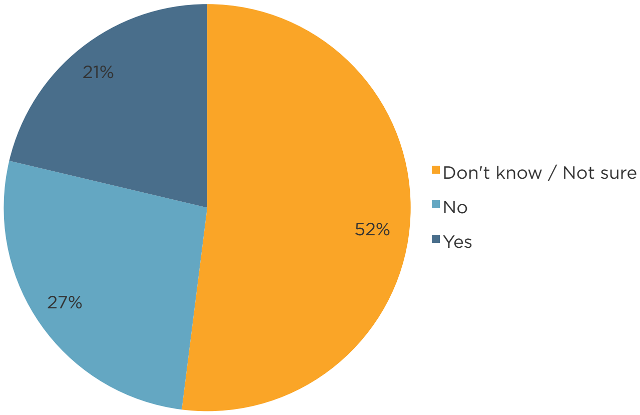


Exhibit 9: Has your company's cyber incident response plan been tested

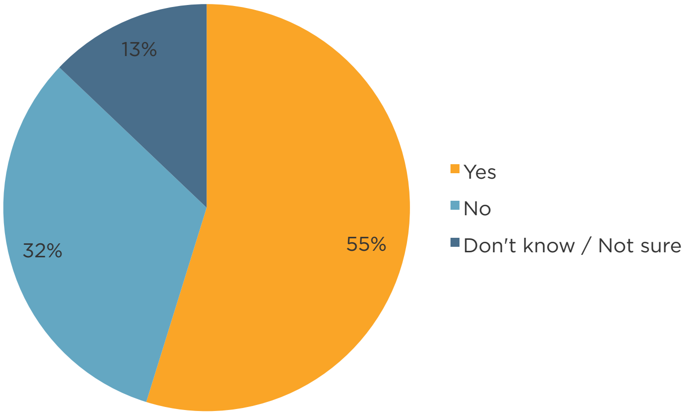


Exhibit 10: How frequently is your company's cyber incident response plan tested?

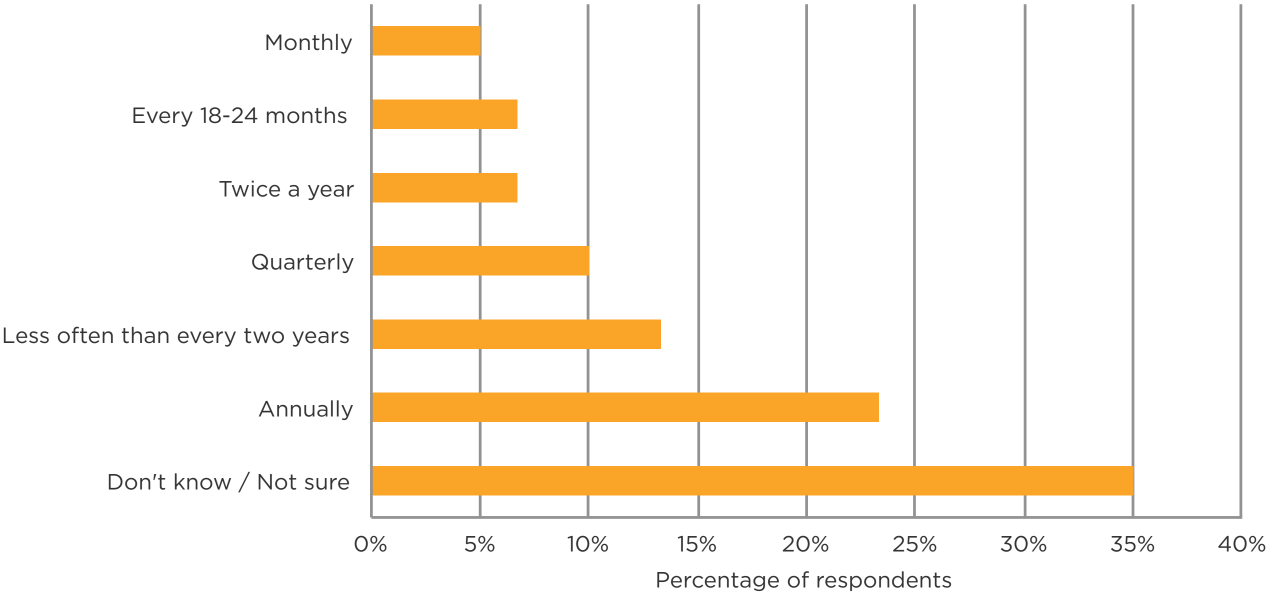


Exhibit 11: How frequently is your company's cyber incident response plan updated?

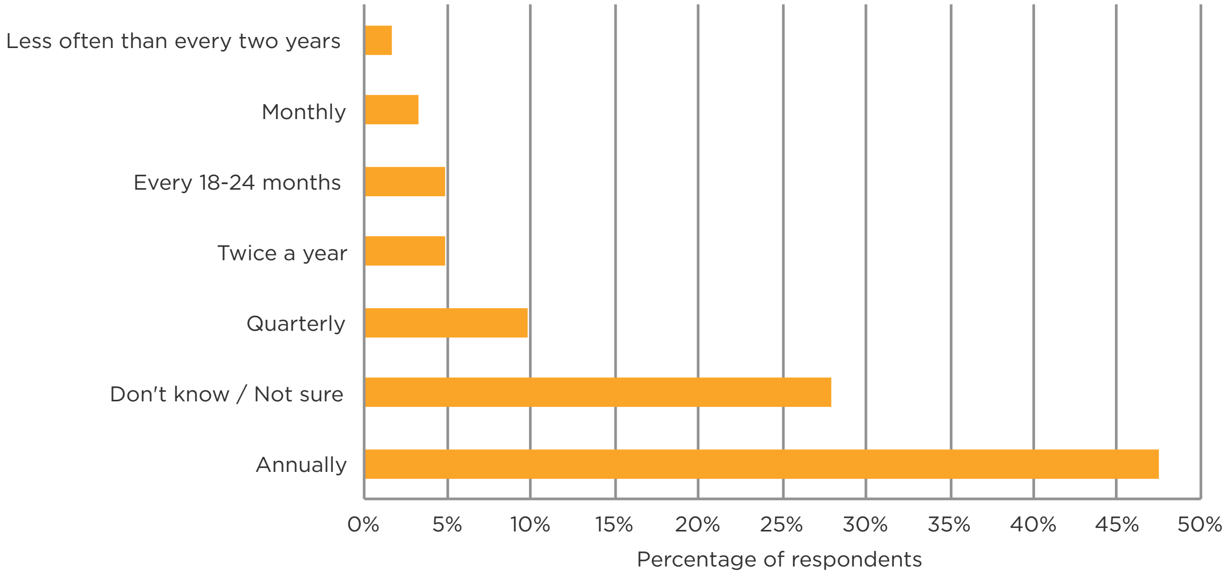


Exhibit 12: Has your company ever been a victim of cyber extortion?

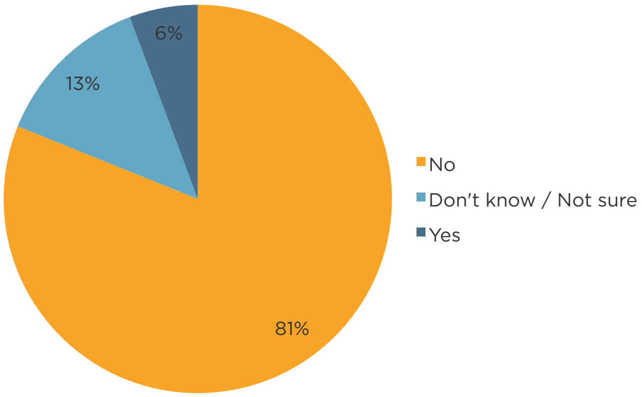


Exhibit 13: If your company ever decided it needed to pay a ransom for cyber extortion, does your company currently know how to obtain cryptocurrency such as bitcoin?

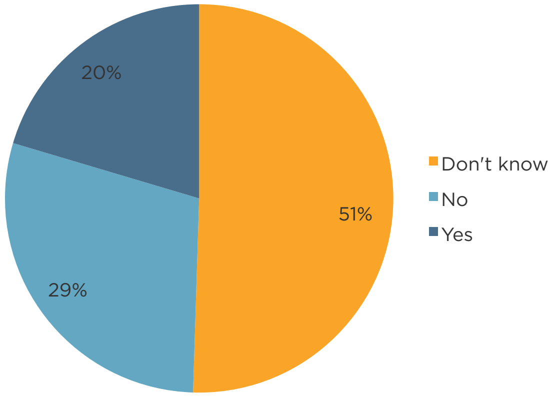


Exhibit 14: Has your company pre-selected third party vendors to assist with breach preparation and response?

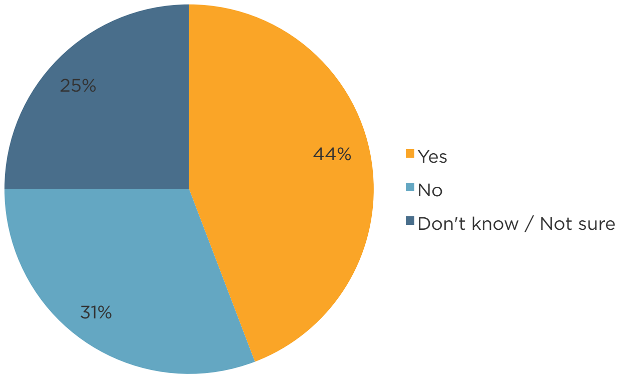


Exhibit 15: Which of the following best describes your role?

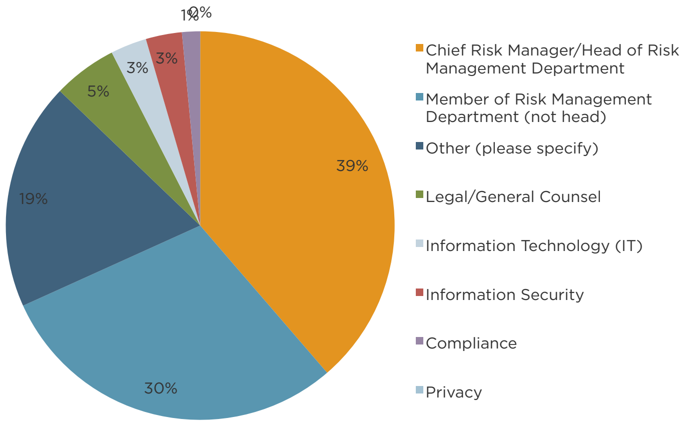


Exhibit 16: What is your company's industry?

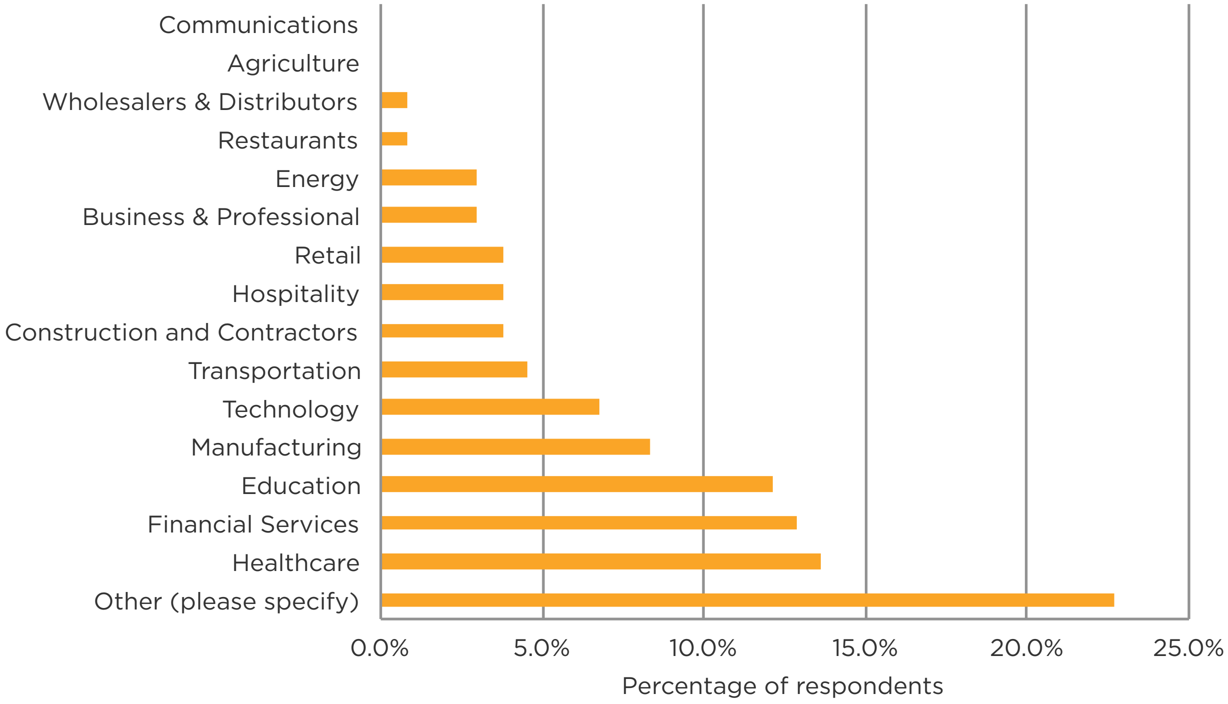
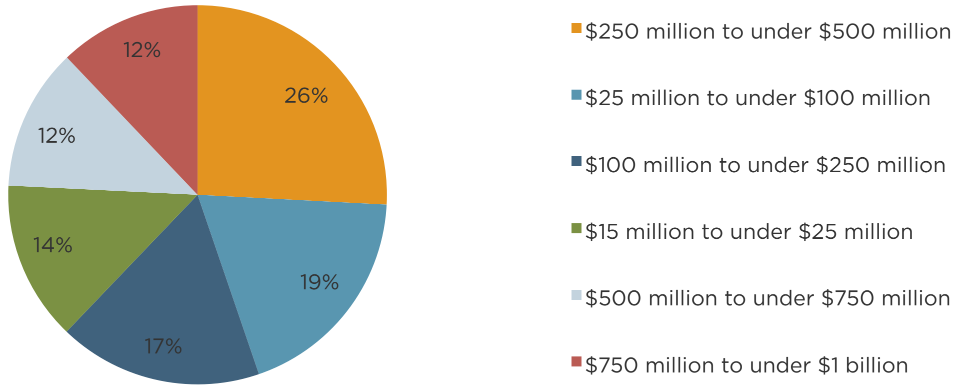


Exhibit 17: What is your annual revenue/budget (US $)?



Advisen
Transforming • Insurance℠

Prepare. Protect. Prevail.®

THE HARTFORD

Business Insurance
Employee Benefits
Auto
Home

This document outlines in general terms the coverages that may be afforded under a policy from The Hartford. All policies must be examined carefully to determine suitability for your needs and to identify any exclusions, limitations or any other terms and conditions that may specifically affect coverage. In the event of a conflict, the terms and conditions of the policy prevail. All coverages described in this document may be offered by one or more of the property and casualty insurance company subsidiaries of The Hartford Financial Services Group, Inc. Coverage may not be available in all states or to all businesses. Certain products may be provided on a surplus lines basis and require the use of a surplus lines broker. Surplus lines policies are generally not protected by state guaranty funds. Possession of these materials by a licensed insurance producer does not mean that such producer is an authorized agent of The Hartford. To ascertain such information, please contact your state Department of Insurance or The Hartford at 1-888-203-3823. All information and representations herein are as of September 2016.

The Hartford® is The Hartford Financial Services Group, Inc. and its subsidiaries, including issuing companies, Hartford Fire Insurance Company, Hartford Life Insurance Company and Hartford Life and Accident Insurance Company. Its headquarters is in Hartford, CT.

The information contained in this document has been developed from sources believed to be reliable. However, the accuracy and correctness of such materials and information has not been verified. We make no warranties either expressed or implied nor accept any legal responsibility for the correctness or completeness of this material. This information should not be construed as business, risk management, or legal advice or legal opinion. Compliance with any of the recommendations contained herein in no way guarantees the fulfillment of your obligations as may be required by any local, state or federal laws. Advisen and The Hartford assume no responsibility for the discovery and/or elimination of relevant conditions on your property or at your facility.