AFP® ASSOCIATION FOR FINANCIAL PROFESSIONALS

2015 AFP Risk Survey

REPORT OF SURVEY RESULTS

Supported by

MARSH & McLENNAN COMPANIES

MARSH · GUY CARPENTER · MERCER · OLIVER WYMAN

2015 AFP

Risk Survey

REPORT OF SURVEY RESULTS

January 2015

Supported by

ASSOCIATION FOR FINANCIAL PROFESSIONALS

Association for Financial Professionals
4520 East-West Highway, Suite 750
Bethesda, MD 20814
Phone 301.907.2862
Fax 301.907.2864
www.AFPonline.org

MARSH & McLENNAN COMPANIES

MARSH GUY CARPENTER MERCER OLIVER WYMAN

With uncertainty as the new normal, agility and response to emerging risks is key

As the AFP risk survey series has demonstrated, earnings uncertainty and risk forecasting remain a persistent challenge for businesses across all industries. Risk and uncertainty are a fact of life in today's business environment. This development has been clearly recognized by respondents to the *2015 AFP Risk Survey*, who indicate that their organizations are seeking to better leverage data and analytics to support improved risk identification and inform their overall business strategy. Businesses are also evaluating a broader universe of risks, which requires an increased allocation of resources to risk management efforts, as risk becomes more explicitly incorporated into core strategy considerations.

Given the increasing adoption of true enterprise-wide approaches, risk management is becoming embedded in an organization's ongoing, core management processes, informing critical decision making. No longer crisis or event-driven, this process is geared towards better financial and strategic decisions and operational execution. Constantly adapting and refining the approach to risk management must be a key priority for companies in the current environment.

The response to cyberthreats stands as a very real test case for the ability of organizations to successfully extract value from their enterprise risk approach. This year's survey data regarding organizational responses to cyberrisk suggests that improvements must be made in the risk management process in order to address emerging, disruptive and transformative risks.

While many organizations have made strides in addressing mitigation, prevention and response to emerging risk, some key principles have not yet been effectively applied. For example, the survey data suggests that responses to cyberthreats tend to focus primarily on technical solutions, rather than a full enterprise approach involving processes, training, education and proactive response planning across all functions.

Most importantly, this year's survey data again indicates that respondents do not anticipate a significant decline in earnings uncertainty or difficulty of financial forecasting in the upcoming years. In light of this, companies must learn from both their own experience and peer organizations in developing nimble responses to emerging risks and trends. Organizations that develop the capacity to quickly deploy capabilities in response to an uncertain business environment will be best positioned to thrive as volatility increases.

Alex Wittenberg
Partner, Oliver Wyman and Executive Director,
Marsh & McLennan Companies Global Risk Center

Introduction

The business environment faced a number of challenges in 2014. The crisis in Ukraine and the resulting economic sanctions posed and continue to pose a significant challenge to the already weak recovery of the Eurozone. Tumbling oil prices especially in the last half of the year added to economic woes in some countries, gave some investors "pause," while at the same time provided a boost to some consumers.

Additionally, 2014 saw breaches in cybersecurity at many high-profile organizations. Media coverage of these "hack attacks" was widespread and organizations had to quickly go into damage control to protect their reputations. In the U.S., political and regulatory uncertainty continued, and the results of November's mid-term elections did little to resolve that uncertainty.

Against this backdrop, it is imperative that financial professionals stay ahead of the curve. They need to equip themselves–and therefore their organizations–with tools that enable them to be more efficient in predicting and responding to risk factors.

To gauge financial professionals' views of the current risk environment, the Association for Financial Professionals® (AFP) surveyed its senior level corporate practitioner membership in October of 2014. The *2015 AFP Risk Survey* not only examines how companies manage risk, but focuses more specifically on cyberrisks. Key highlights include:

- Political/regulatory uncertainty is a top risk to earnings over the next three years.
- The greatest concern among financial professionals in the event of a cyberattack is reputational damage to their organizations.
- Organizations are not completely prepared to respond to cyberattacks.

This fourth risk survey was again the result of a partnership between AFP and Oliver Wyman, part of Marsh & McLennan Companies. AFP thanks Oliver Wyman for its support of this survey, for help in crafting the survey questions, and for providing key insights into current risk issues. The Research Department of the Association for Financial Professionals is solely responsible for the content of this report.

KEY FINDINGS

ASSOCIATION FOR FINANCIAL PROFESSIONALS

2015 AFP Risk Survey

REPORT OF SURVEY RESULTS

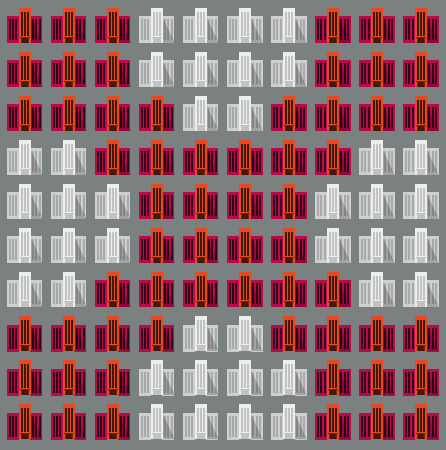
EARNINGS RISK FACTORS

IN THE NEXT 3 YEARS

1 out of 3

companies were a target of cyberattack over the past 18 months.

The most severe impact is a strong hit to the company's reputation with customers and vendors.



60%

of companies do not have a response plan for a cyberbreach.

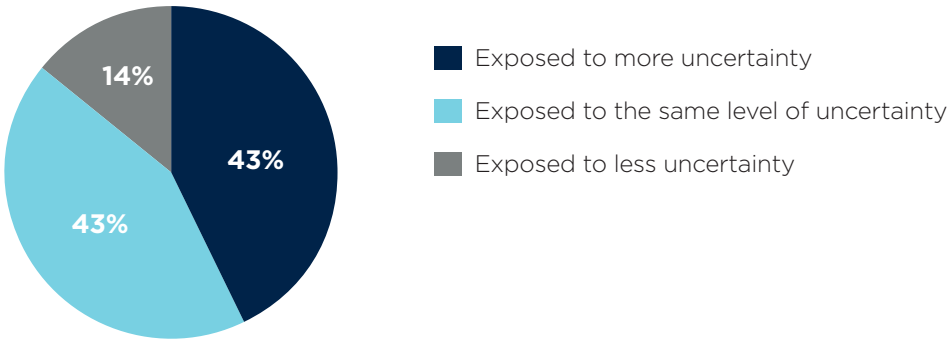
Uncertainty in Earnings Prevail

In the face of a solidifying economic recovery in the U.S. but enduring hesitation in many European and Asian economies, businesses are exposed to high levels of uncertainty surrounding their earnings. Forty-three percent of financial professionals believe their organizations are exposed to greater earnings uncertainty today than three years ago. Another 43 percent indicate the level of uncertainty is unchanged. While still significant, the share of financial professionals reporting increased exposure to earnings risk has declined compared to recent years; in the *2013 AFP Risk Survey*, 59 percent of survey respondents indicated their organizations had increased exposure to earnings risk.

Only 14 percent of financial professionals report that their organizations are operating under conditions of less uncertainty compared to three years ago. Survey respondents from publicly owned companies (47 percent) and those at larger companies (with annual revenues of at least $1 billion) more frequently report their companies are subject to a greater amount of uncertainty than do their counterparts from other companies.

At **43%** of companies, earnings uncertainty has grown over the past 3 years

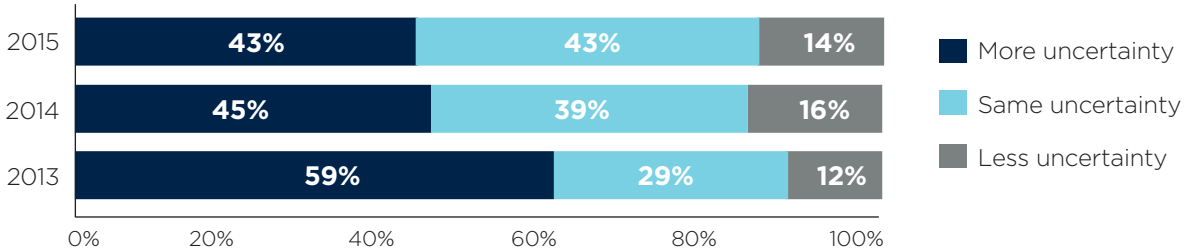
Change in Exposure to Uncertainty in Earnings Relative to Three Years Ago
(Percentage Distribution of Organizations)



Financial professionals' view that exposure to earnings risk has declined is likely due to a strengthening U.S. economy, including a rising stock market and declining unemployment. However, while perceptions of earnings uncertainty may be leveling off, 86 percent of respondents (close to the 84 percent reported in 2014) report the same or higher levels of uncertainty. This may reflect the view that uncertainty has become the "new normal."

Earnings uncertainty has become the "new normal"

Change in Exposure to Uncertainty in Earnings
(Percentage Distribution of Organizations)



Business/Operations a Top Reason for Earnings Uncertainty

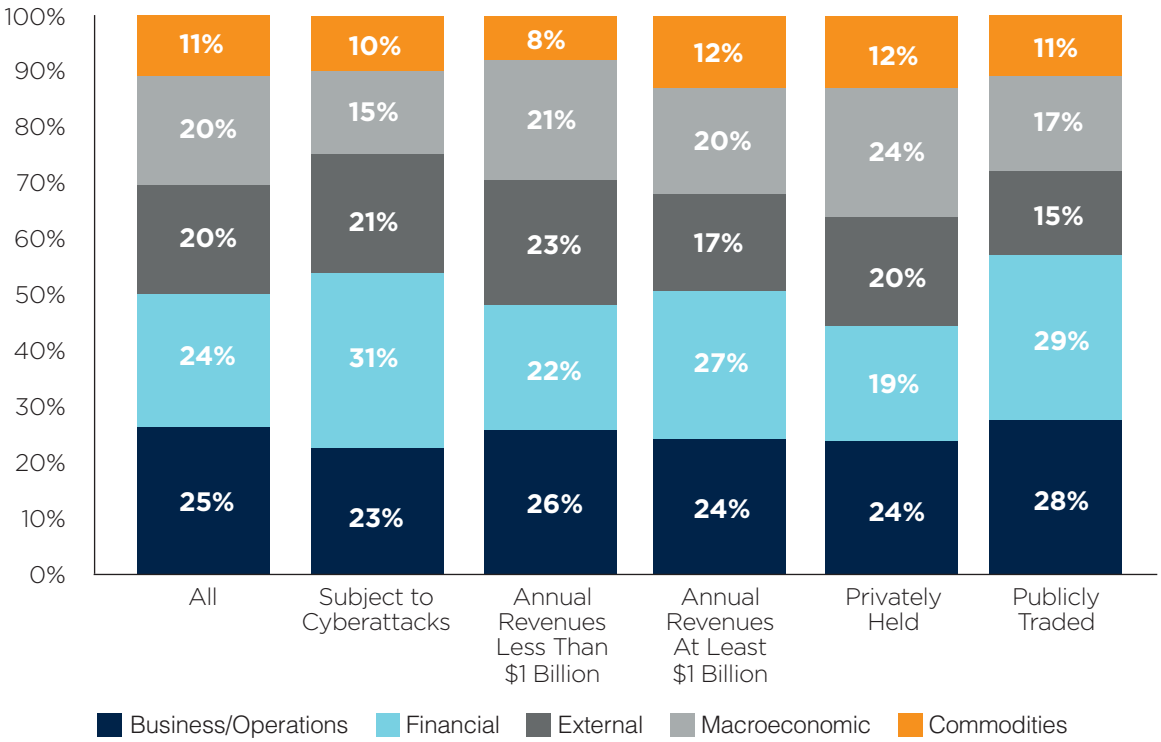
The key factors impacting corporate earnings are as diverse as the survey respondents' organizations themselves. The range of responses also reflects the adoption of a holistic enterprise risk approach and a broader assessment of the risk landscape taken by financial professionals as they move from a narrower perception of risks within the financial area to a wider view of risk management which includes business and operational risks.

The top three drivers of earnings uncertainty are unchanged from those reported in last year's survey; however, their rank order differs. In last year's survey (the *2014 AFP Risk Survey*) the top three primary drivers of earnings uncertainty were financial factors (cited by 26 percent of survey respondents), external factors (25 percent) and business/operations (23 percent). In this year's report, the most frequently mentioned primary drivers of earnings uncertainty are business/operations—cited by 25 percent of financial professionals. Those are followed by financial factors (cited by 24 percent of survey respondents) and external factors (20 percent).

Other drivers of earning uncertainty are macroeconomic factors and commodities. The share of financial professionals reporting macroeconomic factors as primary drivers of uncertainty is 20 percent—essentially unchanged from the share reported in last year's survey but less than the 30 percent just two years ago. Meanwhile, the 11 percent of financial professionals reporting commodities as the primary source of earnings risk was up from the seven percent reported one year ago. [1]

Primary Drivers of Increase in Exposure to Earnings Uncertainty

(Percentage Distribution of Organizations that Have Experienced Greater Earnings Uncertainty)



Note: Total for Privately Held companies does not add to 100 percent due to rounding.

1. Business/operations risks include supply chain disruptions, production interruptions, litigation, labor, outsourcing, IT and cyber risks. Financial factors include credit, liquidity, interest rate and currency/FX risk. Examples of external factors are country risk, regulatory, natural disasters) while macroeconomic factors are risks such as GDP growth and inflation.

Financial Professionals Anticipate Forecasting Risk Will Be More Challenging in 2017

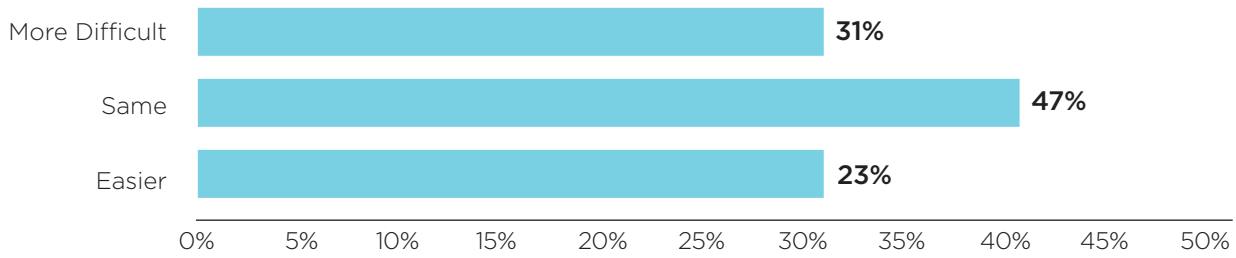
As the range of categories of earnings uncertainty broadens, forecasting risk remains a major challenge. The world is becoming more interconnected and complex and businesses must move at an increasingly faster pace. This global interconnectivity is a breeding ground for new levels of uncertainty. Thanks to technology and instantaneous communication, the sheer volume of data being collected, shared and analyzed in the course of business decisions grows daily.

Consequently—and not surprisingly—a large majority of survey respondents report that forecasting risk continues to be challenging. Slightly more than three-fourths of financial professionals—78 percent—indicate that accurately forecasting risk is either as difficult or even more difficult as it was three years ago. At the other end of the spectrum, less than one-fourth of financial professionals find forecasting risk to be easier today. As was the case with earnings uncertainty, survey respondents from larger companies (with annual revenues of at least $1 billion) are more likely than their peers at smaller organizations (annual revenues of less than $1 billion) to report it was more difficult to forecast risk (38 percent versus 27 percent). This likely reflects larger companies' exposure to risks due to their operating in international markets.

Global interconnectivity is a breeding ground for new levels of uncertainty

78% indicate that accurately forecasting risk is either as difficult or even more difficult as it was three years ago

Difficulty of Forecasting Risk Today Relative to Three Years Ago (2011)
(Percentage Distribution of Respondents)



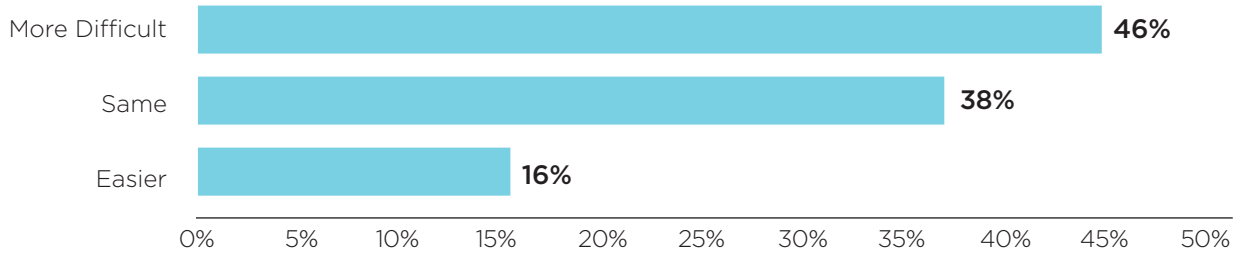
The difficulty in forecasting risk today compared to three years ago has abated somewhat. In the *2013 AFP Risk Survey* (based on survey data collected during October 2012), 53 percent of financial professionals indicated it was more difficult to forecast risk in 2012 than it was in 2007. Today, 31 percent indicate forecasting risk is more difficult compared to three years ago (2011).

However, over the four-year period of the risk survey series, the share of respondents indicating that forecasting remained a significant challenge compared to previous years has been fairly consistent. Indeed, the consensus view is that forecasting risk will only become more difficult in the future. Forty-six percent of financial professionals anticipate that it will be more difficult to forecast risk three years from now while just 16 percent expect this task to become easier. Given that most expect earnings uncertainty to remain the same or increase in the future, these findings indicate that forecasting risk will continue to pose significant challenges in the years to come.

Financial professionals' opinions about the ease or challenge of forecasting risk today compared to three years ago or three years in the future differ little regardless of their organization size or ownership type.

Nearly **1/2** of financial professionals anticipate forecasting risk will grow more difficult over the next 3 years

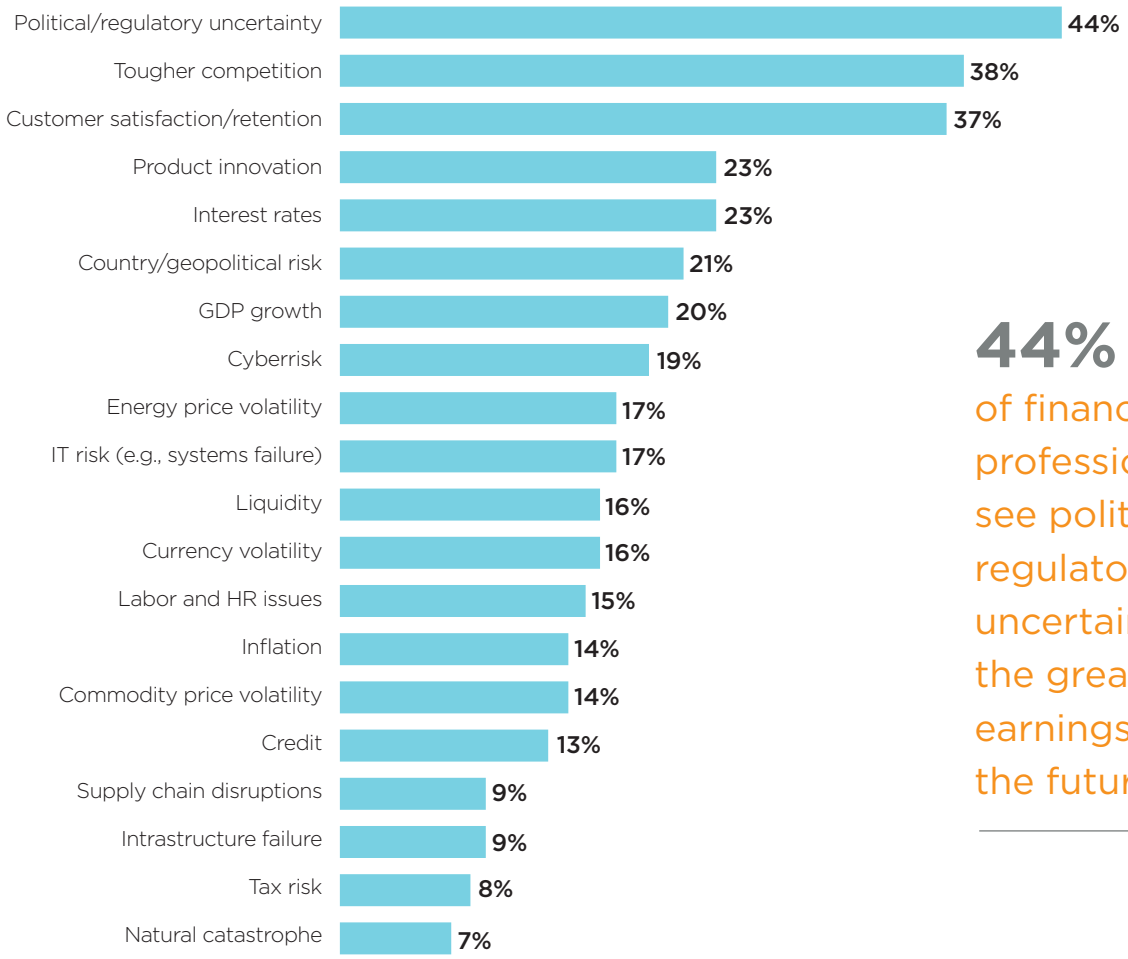
Anticipated Difficulty of Forecasting Risk Today Versus Three Years From Now (2017)
(Percentage Distribution of Respondents)



Risk Factors Having the Greatest Impact on Earnings in the Next Three Years

There are a number of risk factors that can impact a company's earnings. Financial professionals rank the highest risk factor affecting organization earnings in the next three years as political/regulatory uncertainty (44 percent). Financial professionals also cite tougher competition and customer satisfaction/retention to be the most prevalent risk factors impacting their firms' earnings in the future.

Key Risk Factors which will have the Greatest Impact on Organizations' Earnings in the Next Three Years
(Percent of Respondents)



44%
of financial professionals see political/ regulatory uncertainty as the greatest earnings risk in the future

Those top-three ranked factors are identical to those reported in last year's survey. Still, the share of financial professionals indicating political/regulatory uncertain as the #1 risk factor for future earnings decreased slightly, from 48 percent to 44 percent. This small decline perhaps reflects a minor thawing in the political gridlock in Washington DC over the past year, although the figure reflects a continued apprehension in this area.

Meanwhile, 38 percent of financial professionals cite competition as a major challenge to earnings, down from the 48 percent who held this view last year. Financial professionals from organizations with annual revenues of at least $1 billion are more likely than those from smaller ones to suggest country/geopolitical challenges will have a significant impact on earnings over the next three years (27 percent versus 17 percent). Again, this is not surprising given that larger companies are more likely to have global or international supply chains that can be impacted by country or geopolitical risk. Larger companies are also more likely to have their earnings affected by energy/price volatility than are smaller ones (23 percent versus 14 percent). Financial professionals from privately owned companies indicate greater concerns regarding customer satisfaction/retention than do those from publicly traded firms (43 percent versus 33 percent).

Changes in Risk Factors Expected to Have Greatest Impact on Organization's Earnings over Next 3 Years

Risk Ranking	2013	2014	2015
1	Customer Satisfaction/ Retention	Competition	Political and Regulatory Uncertainty
2	Regulatory Risk	Political and Regulatory Uncertainty	Tougher Competition
3	GDP Growth	Customer Satisfaction/ Retention	Customer Satisfaction/ Retention
4	Political Risk	Interest Rate	Product Innovation
5	Interest Rate	GDP Growth	Interest Rate

Organizations Are Actively Mitigating Risk Exposure in Direct Response to Current and Emerging Threats

Just under two-thirds (65 percent) of financial professionals report that their companies are adopting various strategies to respond to risks and exploit opportunities in the face of a changing business environment.

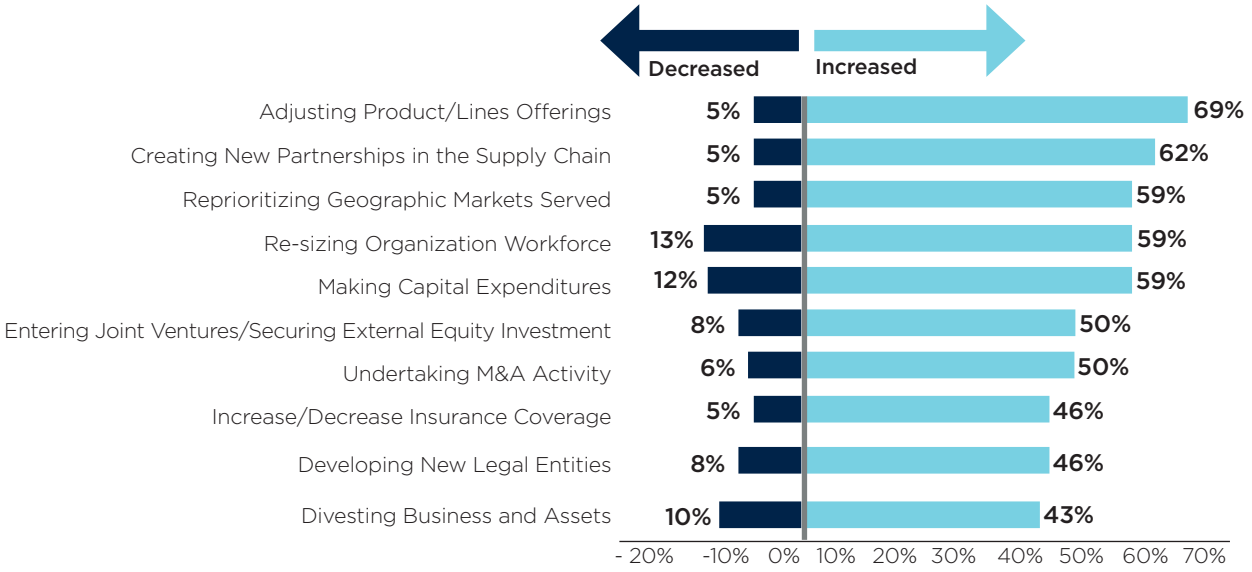
Consistent with the high ranking of tougher competition and customer satisfaction/retention as key risks, the survey results reflect organizations' greater focus on strengthening their competitive position and offerings. Seven out of ten financial professionals (69 percent) report that their organizations are adjusting product lines or offerings and 62 percent of companies are extending or creating new supply chain partnerships. More than half of organizations are increasing capital expenditures, expanding their workforces and re-prioritizing their geographic markets (each cited by 59 percent of respondents).

Other approaches organizations are adopting to counter current and business risks are expanding M&A activity and a greater emphasis on entering joint ventures and securing external equity investment (each cited by 50 percent of respondents). Smaller but significant shares of respondents report that their companies are increasing their insurance coverage or developing legal entities (each cited by 46 percent of respondents) while 43 percent of organizations are focusing on divesting business activity.

65% of companies are adopting strategies in response to risks

Actions Taken in Response to Current and Emerging Business Risks

(Percent of Organizations)



Risk Data and Analytics Used to Support Business Strategy

In addition to those actions organizations are taking to respond to uncertainty, financial professionals believe that more effective use of risk data and analytics will support improved risk identification and inform overall business strategy. The focus on risk identification aligns with other data captured in this survey. As financial professionals focus on a broader array of risks and as risk forecasting is viewed as increasingly challenging, the need for and importance of robust risk identification increases.

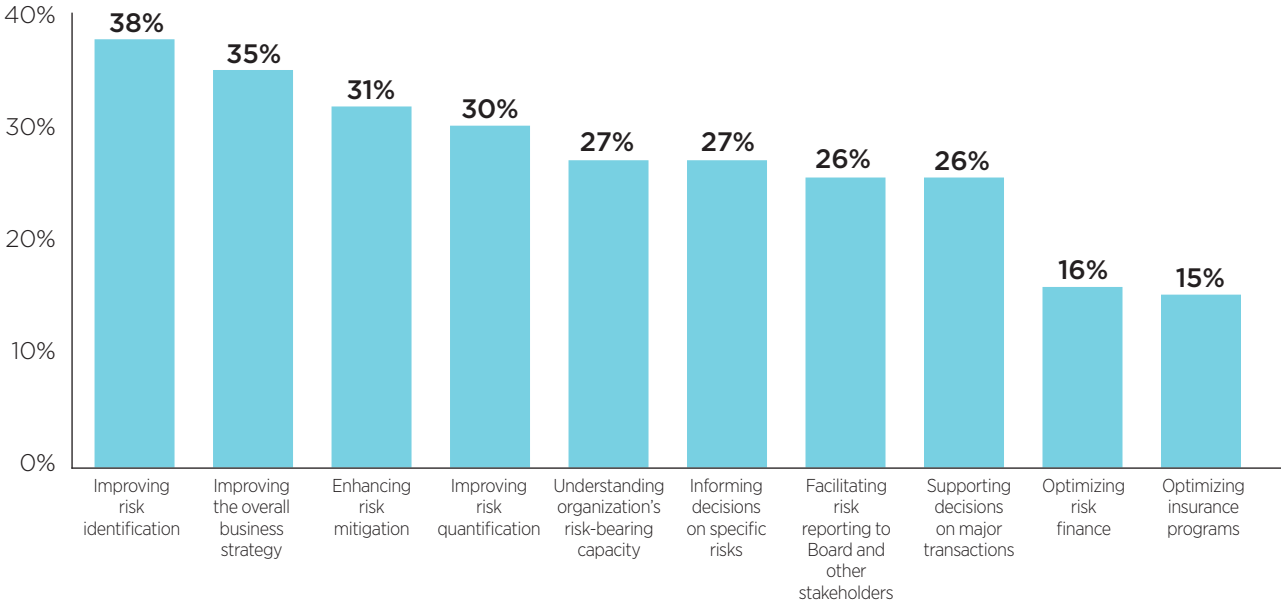
Companies are increasingly integrating risk management into key decision making

Key Decisions That Would Benefit from Improved Risk Analytics

Risk identification	**38 percent**
Informing overall business strategy	**35 percent**
Enhancing risk mitigation	**31 percent**
Improving risk quantification	**30 percent**

Effective Integration of Risk Data and Analytics in the Organization

(Percent of Organizations)



Overall, this year's survey data suggest that companies are increasingly integrating risk management into key decision making. Financial respondents are taking a broader view of "risks" beyond just financial ones, enabling a more holistic view of the potential risks that can affect their organizations. They are placing a stronger emphasis on risk identification and seeking to apply risk information to inform business strategy, enhance risk mitigation, and their organizations' risk-bearing capacity.

Cyberrisks

The overall trend toward enterprise risk management and improved management of emerging risks is tested when examining how financial professionals and their organizations respond to cyberrisks. As noted in the introduction to this report, the *2015 AFP Risk Survey* focuses on cyberrisks and how financial professionals are helping their organizations respond to those challenges.

During 2014, a number of companies were victims of high-profile cyberattacks that targeted payment systems, customer contact information and other corporate proprietary data. Looking at these risks on both a strategic and operational level and the response to those risks can illustrate if organizations are better able to develop comprehensive solutions to manage emerging and evolving risks or if there are still challenges in moving from reactive to proactive risk management.

One Out of Every Three Companies Has Suffered a Cyberattack

Advancement in technology and information systems has provided companies with significant opportunities for greater productivity, efficiency and profitability. Rapidly developing information technologies have also benefited vendors and customers.

But the same technology that has introduced many benefits can potentially leave organizations more vulnerable and exposed should these technology systems be compromised. For example, 17 percent of survey respondents report that IT risk (systems failure) could have a significant impact on their organizations' earnings going forward. Nine percent note both risks of supply-chain disruptions and infrastructure failure—two key operational areas that are heavily dependent on IT and connectivity.

A third of financial professionals (34 percent) report that their organizations have been subject to a cyberattack in the past 18 months. Such attacks range from malware to data breaches and hackavism.

Survey respondents from larger companies (with annual revenues of at least $1 billion) and publicly traded ones report higher incidences of cyberattacks than do their counterparts from smaller organizations. This is not surprising as larger firms are more likely to be high profile and thus more attractive targets for malicious hackers. The larger organizations may also be subject to a greater number of requirements to report cyberbreaches.

34% of companies have been targeted with a cyberattack in the past 18 months

Organization a Target of Cyberattacks in the Past 18 Months
(Percentage Distribution of Organizations)

	All	Annual Revenues Less Than $1 Billion	Annual Revenues At Least $1 Billion	Privately Held	Publicly Traded
Yes	34%	30%	43%	24%	43%
No	66	70	57	76	57

Cyberattacks Can Severely Impact Company's Reputation

Cyberattacks can have far-reaching effects. According to 45 percent of survey respondents, the most severe likely impact resulting from a cyberattack is damage to the company's reputation. Indeed, 51 percent of financial professionals from companies that have actually suffered cyberbreaches cite reputational effects as the most severe result. Survey respondents from larger organizations (with revenues of at least $1 billion) are also more likely than those from smaller ones (revenues under $1 billion) to be concerned about the effect of a cyberattack on their companies' corporate standing (55 percent vs. 37 percent).

Beyond reputational damage, the most widely cited severe impacts of a cyberattack are:

- Financial liability (cited by 29 percent of survey respondents)
- Direct revenue loss (14 percent)
- Regulatory investigations (10 percent)
- Fines (2 percent)

Damage to the company's reputation is the most feared impact from a cyberattack

Most Severe Impact on Organization Resulting from a Cyberattack
(Percentage Distribution of Organizations)

	All	Subject to Cyberattacks	Annual Revenues Less Than $1 Billion	Annual Revenues At Least $1 Billion	Privately Held	Publicly Traded
Strong hit to corporate reputation	45%	51%	37%	55%	40%	45%
Financial liability	29	27	29	30	35	30
Direct revenue loss	14	12	17	9	13	18
Regulatory investigations	10	8	14	4	10	6
Fines	2	2	2	2	2	1

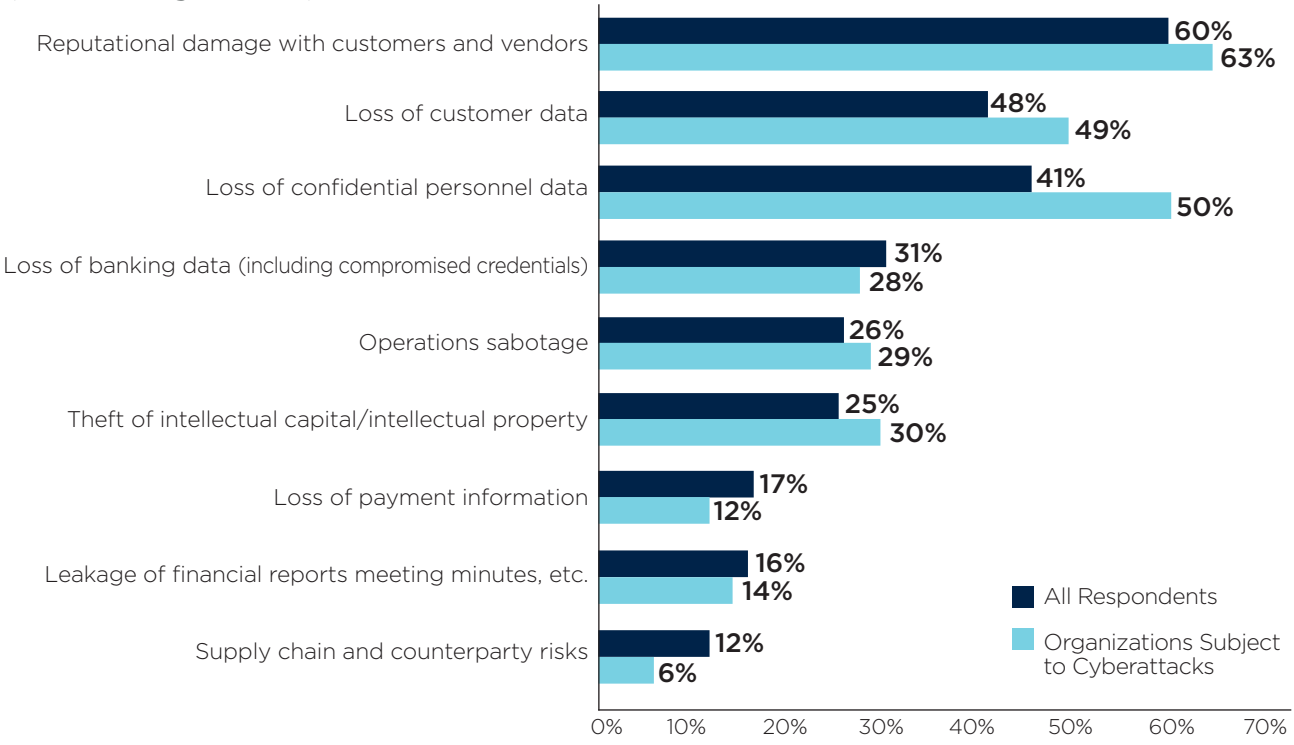
Financial Professionals are Concerned about Impact on Company Reputation after a Cyberattack

Looking forward, respondents continue to believe that the overarching impact of a cyberattack is the reputational damage among their customers, vendors and employees. Reputational damage can be viewed as a "meta-risk" resulting from other losses relating to cyberbreaches, including the loss of data.

The reputational impacts and damage to a company from a high-profile cyberattack can be significant. For example, high-profile breaches in the retail space have led to significant financial ramifications, stemming in large part from reputational effects. Perhaps the most notable example was Target, whose sales, profits and stock were significantly impacted after suffering a widely publicized data breach during the 2013 holiday season.

The loss of proprietary information is more than just an inconvenience for organizations. Recovering from a cyberattack is also becoming increasingly challenging—and costly. Recovering and replacing confidential data requires an immense amount of time and resources to rectify. Since 2010, the number of registered cyberattacks worldwide has been increasing at a rate of 23 percent per year and currently stands at 116 every day.[2] In 2014, the annual average cost for a company that suffered a successful cyberattack was $8.5 million for retailers, $20.8 million for financial services firms, $14.5 million for technology sector organizations, and $12.7 million in communications industries.[3]

Key Areas for Concern with Regards to Cyberrisk
(Percent of Organizations)



Half of the practitioners from companies which have experienced a cyberattack are concerned about the loss of confidential personnel data, compared to 41 percent of those from companies that have not been subject to cyberattacks.

2. Source: Symantec Internet Security Threat report; Ponemon 2012, 2013 Costs of Cyber Crime study; The Global State of Information Security® Survey 2014; The Betterly Report Cyber/Privacy Insurance market survey 2013; Cybersecurity Market report by Marketsandmarkets, June 2012.
3. Source: Ponemon 2014 Cost of Cyber Crime Study: United States

Technical Changes and Safeguards Are Not the Only Responses to Cyberattacks

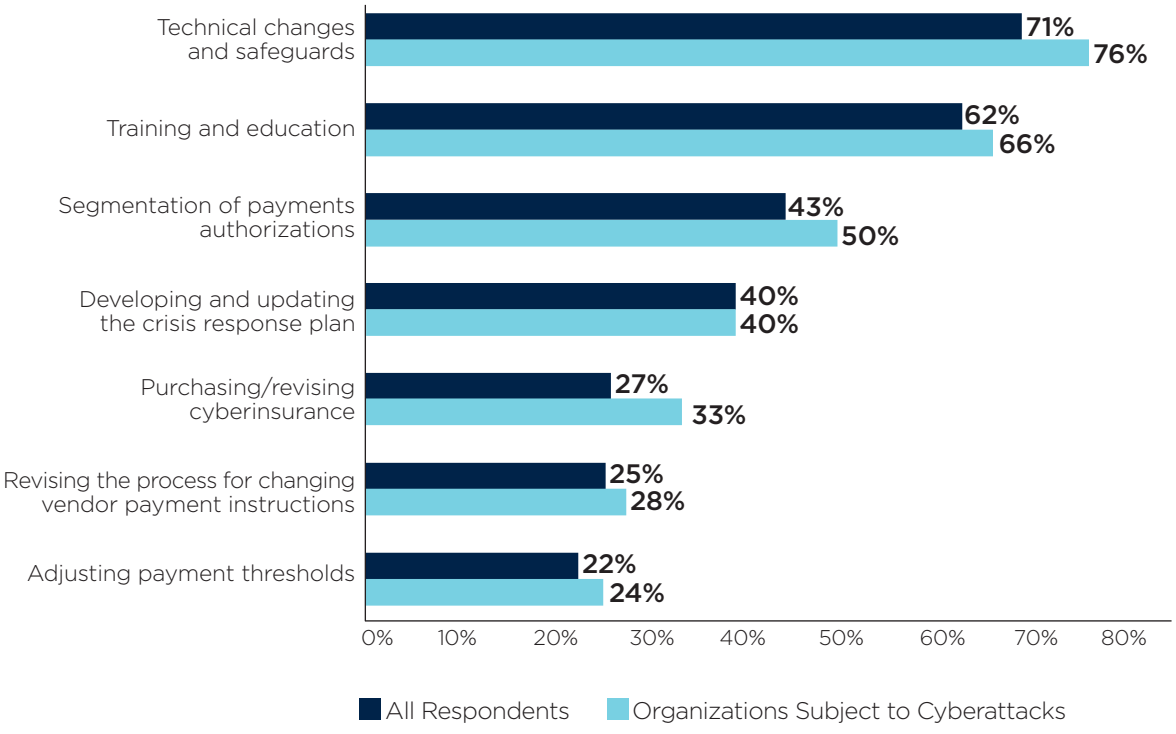
The response to the growing threat of cyberbreaches suggests that best practices for proactively managing cyberthreats are still maturing. Survey results show there is currently a strong emphasis on implementing technical safeguards to bolster defenses. Fewer companies are putting an emphasis on training, education, process revisions or developing proactive response plans.

Seventy-one percent of companies are implementing technical changes and safeguards (e.g., embedding multiple levels of systems approvals, authentication procedures, access controls) to protect themselves against potential cyberthreats as well as minimize the impact of current attacks. Companies that have actually suffered cyberattacks are slightly more likely to have adopted technical changes and safeguards (76 percent).

Sixty-two percent of survey respondents report that their organizations are adapting training to better educate staff to prepare and address potential attacks. Other actions organizations are taking to manage cyberbreaches include segmentation of payments authorization (43 percent) and developing and updating the company's crisis response plan (40 percent).

Companies are implementing technical changes and investing in training and education to protect against cyberthreats

Action Taken by Treasury and Finance to Respond to and Reduce Cyberrisk
(Percent of Organizations)

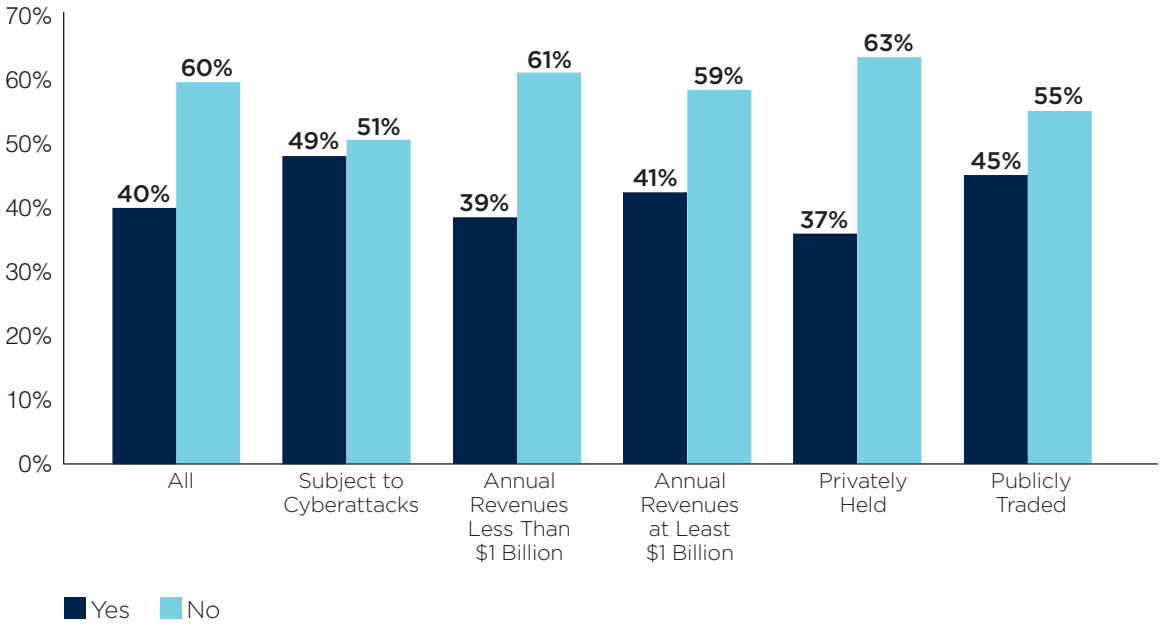


It's an almost accepted fact of life that organizations are facing the potential for an increasing number of threats to their security. The question is "when" rather than "if" a cyberattack will occur in the future.

But even as companies face an increasing number of threats to their security, most do not have a response plan to counter an inevitable attack. A majority of financial professionals (60 percent) indicate that their company does not have a clear, documented mechanism to respond to a cyberbreach event. Perhaps more surprising is that just over half of organizations that have been subject to a cyberattack still do not have a plan in place respond to a future attack.

60% of companies do not have a response plan for a cyberbreach

Presence of Clearly Documented Mechanism to Initiate Response in the Event of a Cyberattack
(Percent of Organizations)



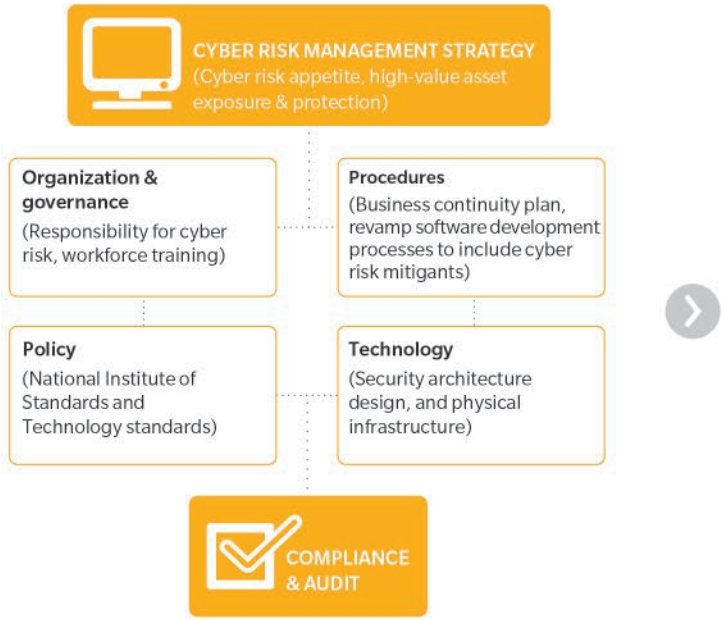
So, what can organizations do to better prepare themselves to defend against or deal with an inevitable cyberattack? Most importantly, they can realize that there is a myriad of interconnected factors that are causing these attacks; if and when there is a crisis, it will be multi-dimensional.

Additionally, organizations should keep their internal and external stakeholders engaged so that they are able to react instantly to a crisis. To get to the root of the attack, organizations will have to be able to gather the facts as quickly as possible and therefore should have a plan in place so there is no delay once they have been attacked.

The survey results suggest that organizations are still struggling to develop strategies and tactics to respond to cyberrisks, and still overly rely on technology solutions. Such a view—that dealing with cyberrisks is the responsibility of and thus can be managed wholly within an organization's IT function—represents a failure to adopt a holistic enterprise approach.

Even though key areas of a treasury function's responsibility are not involved in every cyberattack situation, Treasury does hold or manage much of the data that is often the target of cyberattacks (e.g., payment or credit card information.) In fact, Treasury may be the area to actually discover any breach, and thus could be the first line of defense. As such, an organization's treasury team should be a key player in any overall enterprise approach to cyberrisk management (see below).

An Enterprise-wide Cyberrisk Management Framework



- An overarching **cyber risk strategy** is created, based on risk appetite, environment, and capabilities
- **Governance** structures are installed to control cyber risk and security throughout the organization
- **Security policies** are derived to bring the cyber risk strategy and compliance up to industry standards (PCI, ISO, FISMA)
- **Suitable personnel** are selected and trained. Risk culture is established
- **Security processes** are aligned to the cybersecurity strategy and security policies (war gaming, threat modeling, access control, background screening, secure development, pen testing, business continuity)
- **Technology infrastructure** is deployed to support security processes (information security architecture, systems integrity, monitoring/detection tools, network redundancy)
- **Physical infrastructure** is designed and installed with access controls, surveillance, and crisis management to provide a secure foundation for processes and IT infrastructure
- **Regular audits** are conducted to ensure compliance and performance with defined processes

Source: Combating Cyber Risk: How to Attack a Growing Threat, Oliver Wyman Risk Journal, Vol. 4

Cyberrisk poses entirely new challenges to many firms. It involves a level of complexity and a rate of change that exceed most other operational risks. Most importantly, managing cyberrisk requires an enterprise-wide approach, starting with leadership from the senior management team.

But as suggested by the survey data, few firms have yet to establish an enterprise-wide framework for managing cyberrisk. The key to managing cyberrisk is recognizing that it is a new variant of a familiar problem and an ongoing operational risk. The approaches to measuring and managing operational risk that have been developed over recent decades can be applied to cybersecurity. As a result, new skills and dedicated staff are required.

It is also crucial that Treasury be intimately involved. Within a cyberrisk management framework, Treasury staff need to be educated about the risks and have processes in place to help a company respond to a cyberattack. Such processes would include a cyberrisk response plan that could either be one element of an overall treasury function business continuity plan or a stand-alone plan. The treasury/ finance function can also examine existing processes (vendor payments, payment thresholds, etc.) to determine how it can proactively strengthen a company's resilience to cyberattacks when they occur.

Meeting Challenges that Result from Safeguarding Organizations

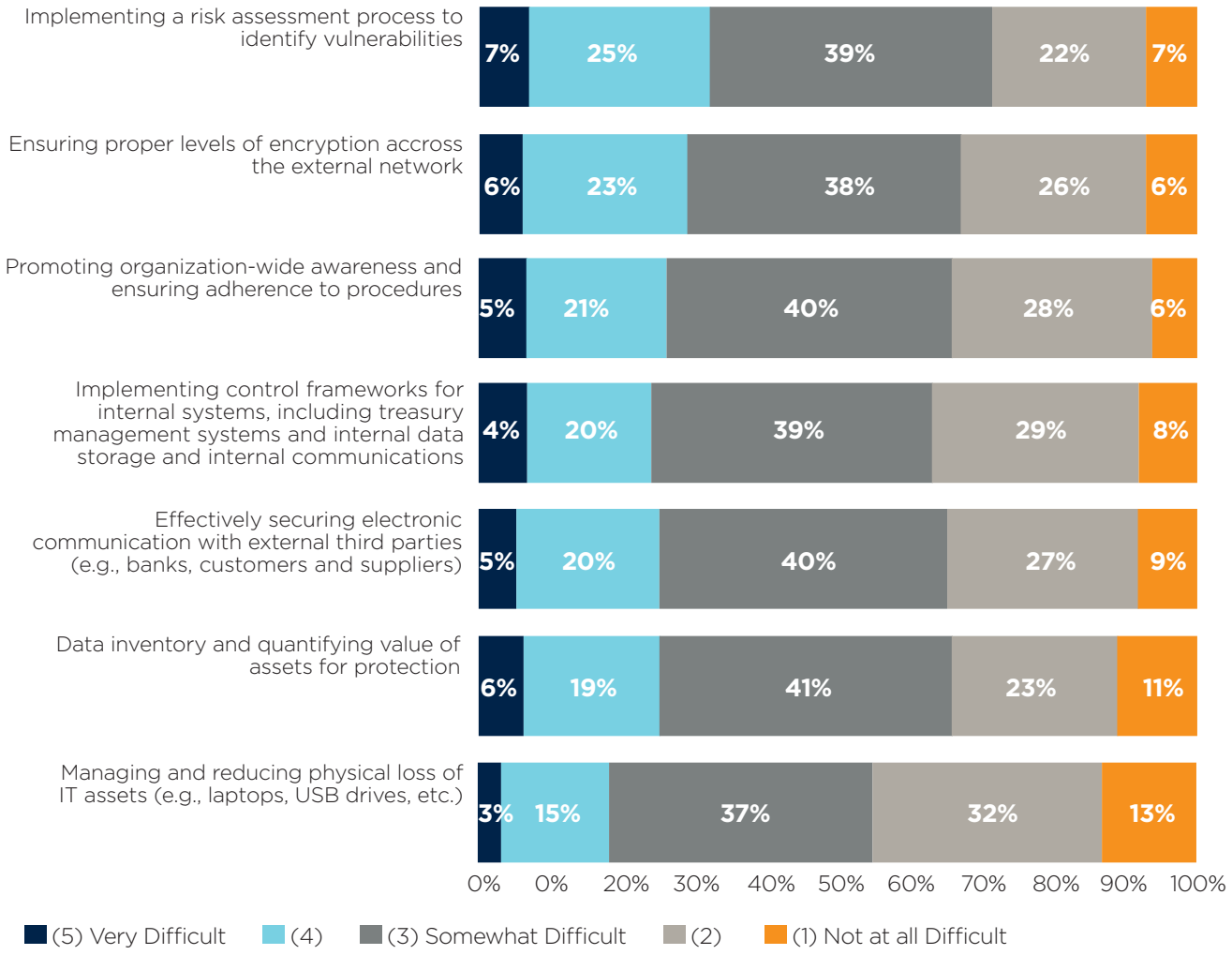
Adopting an enterprise-wide approach to cyberrisk management is challenging. The majority of financial professionals report some level of difficulty in meeting these challenges—primarily the implementation of a risk assessment process to identify their organizations' vulnerabilities (cited by 71 percent of survey respondents) and ensuring proper levels of encryption across external networks (67 percent). Additional challenges recognized by financial professionals include data inventory and quantifying value of assets for protection and promoting organization-wide awareness and ensuring adherence to procedures (each cited by 66 percent of survey respondents).

Other challenges noted by financial professionals include:

- Effectively securing electronic communication with external third parties (cited by 65 percent of survey respondents)
- Implementing control frameworks for internal systems, including treasury management systems and internal data storage and internal communications (63 percent)
- Managing and reducing physical loss of IT assets (e.g., laptops, USB drives, etc.) (55 percent)

Difficulty in Meeting Challenges to Reduce Organization's Vulnerability to Cyberrisks

(Percentage Distribution of Organizations)



Conclusion

Although there has been some decline in the perceived exposure to earnings uncertainty in the last three years, a large majority of financial professionals continue to believe their organizations are exposed to the same or greater level of earnings uncertainty compared to three years ago. Forecasting appears to be as challenging now as it was in 2011, and most financial professionals do not expect this task to become easier in the next three years.

Additionally, the risk landscape is being complicated further by the growing risk of cyberattacks. Cyberbreaches are extensive with rampant malicious hackers successfully outsmarting even large and high-profile organizations equipped with robust risk management capabilities. In spite of high awareness, media frenzy and great concern regarding potential cyberattacks, financial professionals report that their organizations are not yet taking adequate steps to implement necessary actions to protect organizations or prepare their staffs to respond promptly.

Results from the *2015 AFP Risk Survey* reveal a number of key messages in the area of risk management. Notable conclusions from the report include:

Uncertainty continues to prevail in the business environment. Eighty-six percent of respondents report their organizations are exposed to the same or more uncertainty currently than they were three years earlier. Nearly half the respondents anticipate it will be more difficult to forecast risk three years from now.

Political/regulatory uncertainty, tougher competition and customer satisfaction/retention remain top risks to earnings over the next three years. In response companies are focusing on their product lines and supply chain management and capital expenditures to shore up their ability to respond.

Only one out of three organizations has been subject to a cyberattack over the past 18 months. But a combination of underreporting and lack of awareness suggest that cyberattacks are more frequent.

Financial professionals are greatly concerned about possible reputational damage to their organizations in the event of a cyberattack. Sixty percent of financial professionals are most concerned about reputational damage from cyberattacks. Additionally, nearly half (45 percent) note that in the wake of a cyberbreach, the most severe impact would be damage to the company's reputation.

Organizations must move beyond technical safeguards to protect themselves from these attacks. Technical changes are the actions most often being adopted by treasury functions to assist organizations in reducing and responding to potential attacks.

Organizations are not adequately prepared to respond to a cyberattack. Sixty percent of financial professionals noted that in the event of a cyberattack, their treasury group does not have a clearly documented mechanism in place to initiate a response process.

About the Survey

In October 2014, the Research Department of the Association for Financial Professionals® (AFP) surveyed its senior level corporate practitioner membership about uncertainty and how their organizations manage risk. The survey was sent to AFP members and prospects who held job titles of CFO, Treasurer, Controller, Vice President of Finance and Assistant Treasurer. Responses from 509 professionals form the basis of this report. The respondent demographic profile closely models that of AFP's membership and is presented below.

AFP thanks Oliver Wyman with the support of the Marsh & McLennan Companies Global Risk Center, for being a valued partner on the AFP Risk Survey series, including sharing subject matter expertise for the design of the questionnaire and for the final report. The Research Department of the Association for Financial Professionals is solely responsible for the content of this report.

Annual Revenues (USD)

(Percentage Distribution of Organizations)

Under $50 million	19%
$50-99.9 million	8
$100-249.9 million	9
$250-499.9 million	10
$500-999.9 million	11
$1-4.9 billion	26
$5-9.9 billion	8
$10-20 billion	4
Over $20 billion	5

Ownership Type

(Percentage Distribution of Organizations)

Publicly Traded	35%
Privately Held	44
Non-profit (not-for-profit)	11
Government (or government-owned entity)	9

Industry Classification

(Percentage Distribution of Organizations)

Financial Services (Banking, Investment, Brokerage, Insurance, etc.)	18%
Government/Not for Profit	10
Consumer Products (Manufacturing, Sales, Distribution, etc.)	7
Retail	7
Technology (Development, Manufacturing, Sales, Distribution, etc.)	7
Energy (Utilities, Oil, etc.)	6
All other Manufacturing (excluding Consumer Products, Pharmaceuticals, Technology)	6
Media/Professional Services	4
Healthcare Provider	3
Mining and Metals	3
Chemicals	2
Communications	2
Pharmaceuticals/Biotechnology (Development, Manufacturing, Sales, Distribution, etc.)	2
Surface Transport (Maritime, Motor Transport, Rail)	2
Agriculture	1
Automotive	1
Other	19

Appendix: Survey Data Tables

Table 1: Change in Exposure to Earnings Uncertainty Relative to Three Years Ago

(Percentage Distribution of Organizations)

	All	Subject to Cyberattacks	Annual Revenues Less Than $1 Billion	Annual Revenues At Least $1 Billion	Privately Held	Publicly Traded
Exposed to more	43%	46%	38%	49%	38%	47%
Exposed to the same level	43	41	44	40	44	42
Exposed to less	14	13	18	10	18	12

Table 2: Primary Drivers of Increase in Exposure to Earnings Uncertainty

(Percentage Distribution of Organizations That Have Experienced Greater Earnings Uncertainty)

	All	Subject to Cyberattacks	Annual Revenues Less Than $1 Billion	Annual Revenues At Least $1 Billion	Privately Held	Publicly Traded
Business/Operations (e.g., supply-chain disruptions, production interruptions, litigation, labor, outsourcing, IT, cyber)	25%	23%	26%	24%	24%	28%
Financial (e.g., credit, liquidity, interest rate, currency/FX)	24	31	22	27	19	29
External (e.g., country risk, regulatory, natural disaster)	20	21	23	17	20	15
Macroeconomic (e.g., GDP growth, inflation, consumer price index (CPI)	20	15	21	20	24	17
Commodities (e.g., energy, agricultural, basic resources)	11	10	8	12	12	11

Table 3: Difficulty of Forecasting Risk Today Relative to Three Years Ago (2011)
(Percentage Distribution of Respondents)

	All	Annual Revenues Less Than $1 Billion	Annual Revenues At Least $1 Billion	Privately Held	Publicly Traded
Easier	23%	25%	19%	26%	22%
Same	47	49	43	44	46
More Difficult	31	27	38	30	33

Table 4: Anticipated Difficulty of Forecasting Risk Today Versus Three Years from Now (2017)
(Percentage Distribution of Respondents)

	All	Annual Revenues Less Than $1 Billion	Annual Revenues At Least $1 Billion	Privately Held	Publicly Traded
Easier	16%	14%	19%	19%	16%
Same	38	38	37	37	36
More Difficult	46	48	44	45	48

Table 5: Key Risk Factors which will have the Greatest Impact on Organizations' Earnings in the Next Three Years
(Percent of Respondents)

	All	Subject to Cyberattacks	Annual Revenues Less Than $1 Billion	Annual Revenues At Least $1 Billion	Privately Held	Publicly Traded
Political and regulatory uncertainty	44%	51%	46%	43%	35%	44%
Tougher competition	38	28	38	38	43	41
Customer satisfaction/retention	37	35	39	36	43	33
Product innovation	23	23	21	26	20	33
Interest rates	23	26	23	24	24	21
Country risk/geopolitical challenges	21	23	17	27	20	27
GDP growth	20	24	19	23	16	27
Cyberrisk	19	23	20	18	17	18
Energy price volatility	17	21	14	23	15	19
Information technology risk (e.g., systems failure)	17	20	19	16	16	15
Liquidity	16	14	15	18	17	18
Currency volatility	16	14	13	21	18	20
Labor and HR issues	15	10	17	12	18	9
Inflation	14	17	18	9	13	12
Commodity (non-energy) price volatility	14	10	13	17	19	15
Credit	13	15	14	13	14	15
Supply chain disruptions	9	6	9	11	13	7
Infrastructure failure/breakdown	9	10	11	8	10	7
Tax risk	8	8	7	8	7	9
Natural catastrophe	7	5	5	9	5	10

Table 6: Revisions to Mitigate Risk in Direct Response to Current and Emerging Threats
(Percentage Distribution of Organizations)

	All	Subject to Cyberattacks	Annual Revenues Less Than $1 Billion	Annual Revenues At Least $1 Billion	Privately Held	Publicly Traded
Yes	65%	68%	62%	70%	64%	65%
No	35	32	38	30	36	35

Table 7: Actions Taken in Response to Current and Emerging Business Risks
(Percent of Organizations)

	Increased	Same	Decreased
Adjusting product lines/offerings	69%	26%	5%
Making capital expenditures	59	28	12
Re-sizing organization workforce	59	28	13
Creating new partnerships in the supply chain	62	33	5
Re-prioritizing geographic markets served	59	36	5
Increase/decrease insurance coverage	46	49	5
Undertaking M&A activity	50	45	6
Entering joint ventures/securing external equity investment	50	42	8
Divesting businesses and assets	43	48	10
Developing new legal entities	46	45	8

Table 8: Effective Integration of Risk Data and Analytics in the Organization
(Percent of Organizations)

	All	Subject to Cyberattacks	Annual Revenues Less Than $1 Billion	Annual Revenues At Least $1 Billion	Privately Held	Publicly Traded
Improving risk identification	38%	42%	42%	35%	36%	42%
Informing the overall business strategy	35	32	40	30	39	32
Enhancing risk mitigation	31	32	30	32	31	31
Improving risk quantification	30	27	25	37	26	35
Understanding organization's risk-bearing capacity	27	27	28	27	28	27
Informing decisions on specific risks	27	29	29	26	26	22
Facilitating risk reporting to board and other stakeholders	26	29	26	26	19	29
Supporting decisions on major transactions	26	27	23	32	25	29
Optimizing risk finance	16	11	13	18	18	17
Optimizing insurance programs	15	15	13	16	17	11

Table 9: Organization a Target of Cyberattacks in the Past 18 Months
(Percentage Distribution of Organizations)

	All	Subject to Cyberattacks	Annual Revenues Less Than $1 Billion	Annual Revenues At Least $1 Billion	Privately Held	Publicly Traded
Yes	34%	100%	30%	43%	24%	43%
No	66	–	70	57	76	57

Table 10: Key Areas for Concern with Regards to Cyberrisks
(Percent of Organizations)

	All	Subject to Cyberattacks	Annual Revenues Less Than $1 Billion	Annual Revenues At Least $1 Billion	Privately Held	Publicly Traded
Reputational damage with customers and vendors	60%	63%	59%	66%	56%	60%
Loss of customer data	48	49	48	49	53	43
Loss of confidential personnel data	41	50	42	39	37	36
Loss of banking data (including compromised credentials)	31	28	34	26	35	27
Operations sabotage	26	29	26	25	26	27
Theft of intellectual capital/intellectual property	25	30	26	26	23	34
Loss of payment information	17	12	19	16	15	19
Leakage of financial reports, meeting minutes, etc.	16	14	15	17	15	20
Supply chain and counterparty risks	12	6	10	14	13	14

Table 11: Actions Taken by Treasury and Finance to Respond to and Reduce Cyberrisk
(Percent of Organizations)

	All	Subject to Cyberattacks	Annual Revenues Less Than $1 Billion	Annual Revenues At Least $1 Billion	Privately Held	Publicly Traded
Technical changes and safeguards (e.g., embedding multiple levels of systems approvals, authentication, procedures, access controls)	71%	76%	72%	71%	74%	68%
Training and education	62	66	60	65	57	62
Segmentation of payments authorizations	43	50	38	51	41	49
Developing and updating the crisis response plan	40	40	38	42	37	43
Purchasing/revising cyber insurance	27	33	28	26	24	25
Revising the process for changing vendor payment instructions	25	28	23	28	28	28
Adjusting payment thresholds	22	24	21	24	26	24

Table 12: Presence of Clearly Documented Mechanism to Initiate Response in the Event of a Cyberattack
(Percentage Distribution of Organizations)

	All	Subject to Cyberattacks	Annual Revenues Less Than $1 Billion	Annual Revenues At Least $1 Billion	Privately Held	Publicly Traded
Yes	40%	49%	39%	41%	37%	45%
No	60	51	61	59	63	55

Table 13: Most Severe Impact on Organizations Resulting from a Cyberattack
(Percentage Distribution of Organizations)

	All	Subject to Cyberattacks	Annual Revenues Less Than $1 Billion	Annual Revenues At Least $1 Billion	Privately Held	Publicly Traded
Strong hit to corporate reputation	45%	51%	37%	55%	40%	45%
Financial liability	29	27	29	30	35	30
Direct revenue loss	14	12	17	9	13	18
Regulatory investigations	10	8	14	4	10	6
Fines	2	2	2	2	2	1

AFP Research

AFP Research provides financial professionals with proprietary and timely research that drives business performance. AFP Research is led by Managing Director, Research and Strategic Analysis, Kevin A. Roth, PhD and is joined by a team of research analysts.

AFP Research draws on the knowledge of the Association's members and its subject matter experts in areas that include bank relationship management, risk management, payments, and financial accounting and reporting. AFP Research also produces *AFP EconWatch*, a weekly economic newsletter. Study reports on a variety of topics, including AFP's annual compensation survey, and *AFP EconWatch* are available online at www.AFPonline.org/research.

About the Association for Financial Professionals

Headquartered outside Washington, D.C., the Association for Financial Professionals (AFP) is the professional society that represents finance executives globally. AFP established and administers the Certified Treasury Professional™ and Certified Corporate FP&A Professional™ credentials, which set standards of excellence in finance. The quarterly AFP Corporate Cash Indicators™ serve as a bellwether of economic growth. The AFP Annual Conference is the largest networking event for corporate finance professionals in the world.

AFP, Association for Financial Professionals, Certified Treasury Professional, and Certified Corporate Financial Planning & Analysis Professional are registered trademarks of the Association for Financial Professionals.

General Inquiries	AFP@AFPonline.org
Web Site	www.AFPonline.org
Phone	301.907.2862

MARSH & McLENNAN COMPANIES

WHAT'S THE RIGHT WAY TO MANAGE RISK? THE SMARTEST PATH TO GROWTH? THE BEST WAY TO ENGAGE YOUR PEOPLE?

When it comes to risk, strategy, and human capital, clients in more than 130 countries depend on us to help them answer the hard questions. Together, we work to solve complex problems, seize opportunities, and drive growth.

We are Marsh & McLennan Companies, a global professional services firm whose deep expertise and commitment to lasting partnerships protect and advance our clients' vital assets: their people, their capital, their strategy.

To learn more about us and our market-leading brands, visit MMC.com.

MARSH GUY CARPENTER MERCER OLIVER WYMAN