THIRD-PARTY CYBER RISK FOR FINANCIAL SERVICES: BLIND SPOTS, EMERGING ISSUES & BEST PRACTICES

April 2019

BITSIGHT®
The Standard in SECURITY RATINGS

Center for Financial Professionals

CONTENTS

Introduction 3

Key Findings 4

Part 1: Growing Awareness 5

Part 2: The Disconnect 6

Part 3: Common Barriers 7

Part 4: The Way Forward 9

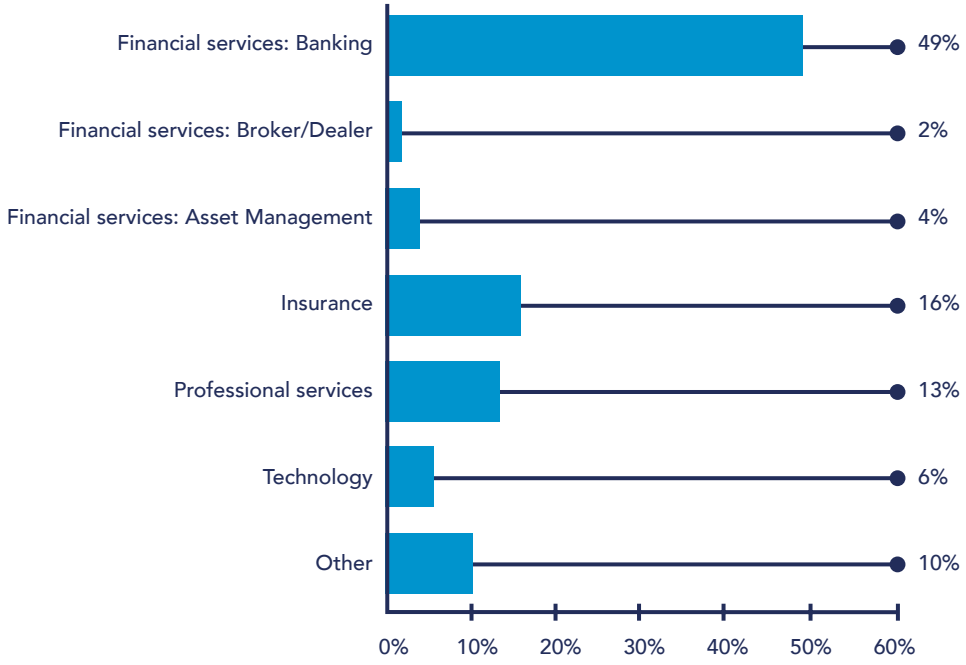
INTRODUCTION

The complexity of today's business world means that most organizations need to regularly work with hundreds – and sometimes thousands – of third parties, including service providers, vendors, suppliers, contractors, partners, and other organizations. While this collaboration is critical, the exchange of data and sensitive information involved creates a new set of security risks that must be actively managed and continuously monitored. Harmful data breaches can originate with the compromise of a key vendor or business partner; disruptions impacting a third party can cause operational impact to customers. Assessing and measuring the cyber risk posed by third parties has become a major component of an organization's ongoing security needs, driven by an increase in data breaches and the legal and financial consequences for companies involved in them.

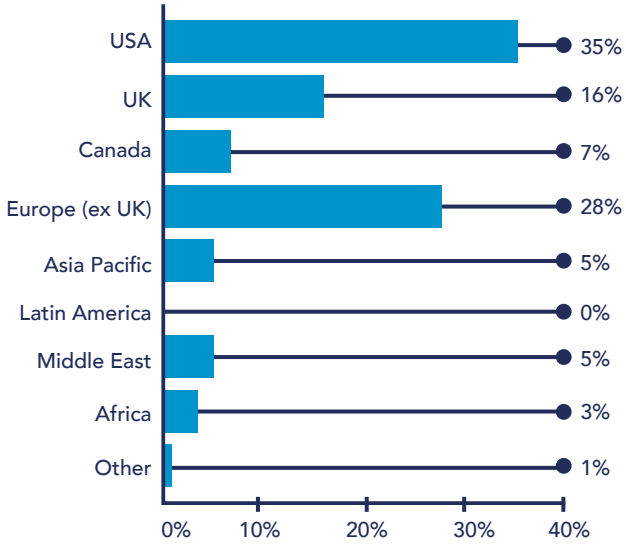
While the finance industry has historically had more robust cyber defenses compared to other industries, the many third parties involved in its massive supply chain - including legal organizations, accounting and human resources firms, management consulting and outsourcing firms, and information technology and software providers - all pose potential weak spots. This begs several important questions: How is the finance industry responding to the growing challenges associated with third-party cyber risk? How are organizations measuring and reporting on this risk? What tools are they using?

In order to assess how financial institutions are responding to growing third-party cyber risk, the Center for Financial Professionals (CeFPro) and BitSight launched a joint study: "The State of Third-Party Cyber Risk Management (TPRM) in Financial Services, 2019." The survey polled 126 financial services professionals from various industry sectors, including banking (49 percent), insurance (16 percent) and professional services (13 percent), among others. Respondents are located around the world, with the majority coming from the United States (35 percent), Europe (28 percent, not including the UK), and the United Kingdom (16 percent). The majority of respondents were at the manager level (36 percent) and the SVP/VP/Director level (30 percent), as well as the analyst (about 15 percent), C-level (about 10 percent) and board member (about 3 percent) levels.

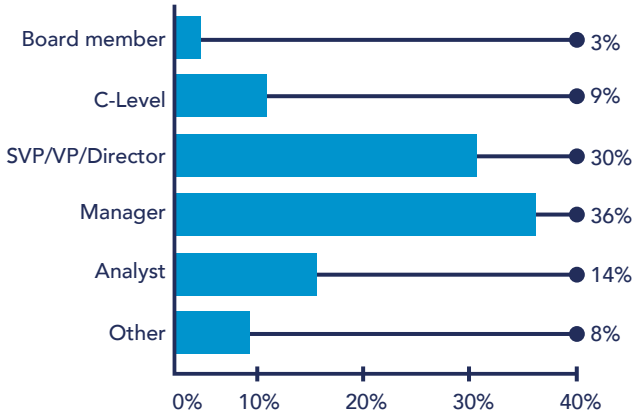
What best describes your industry?



Where is your company headquartered?



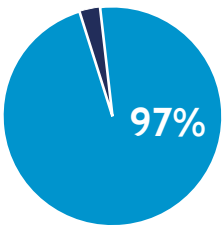
What is your job level?



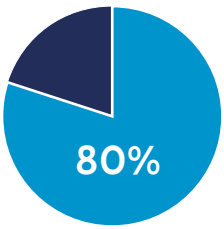
KEY FINDINGS

Results from the TPRM in Financial Services Survey shed light on the fact that many financial services organizations recognize the risk posed by third parties that they work with, which has driven a greater awareness around the need to manage these risks.

What the data also makes clear, however, is that, while many companies consider TPRM a key business issue that guides decision-making about which companies they do business with, many still struggle to measure and regularly report on this risk. Meanwhile, many organizations are not utilizing key tools like security ratings, leaving them unable to effectively and continuously monitor third-party risk.

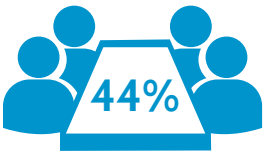


Of respondents say that cyber risk affecting third parties is a "critical" or "important" issue



Nearly 80% of financial services firms say they would decline, or already have declined, a business relationship due to a third party's cybersecurity performance

Only 22% of organizations are currently using a security ratings service to continuously monitor the cybersecurity performance of third parties

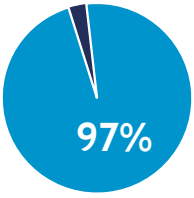


organizations are regularly reporting on TPRM to executives and boards

Looking ahead, given the criticality of the issues, organizations described their interest in creating more formal, scalable, dynamic third- and fourth-party cyber risk management programs. The data suggests that financial services organizations can learn a great deal from each other as they seek to implement sustainable programs to meet the challenges of the 21st century.

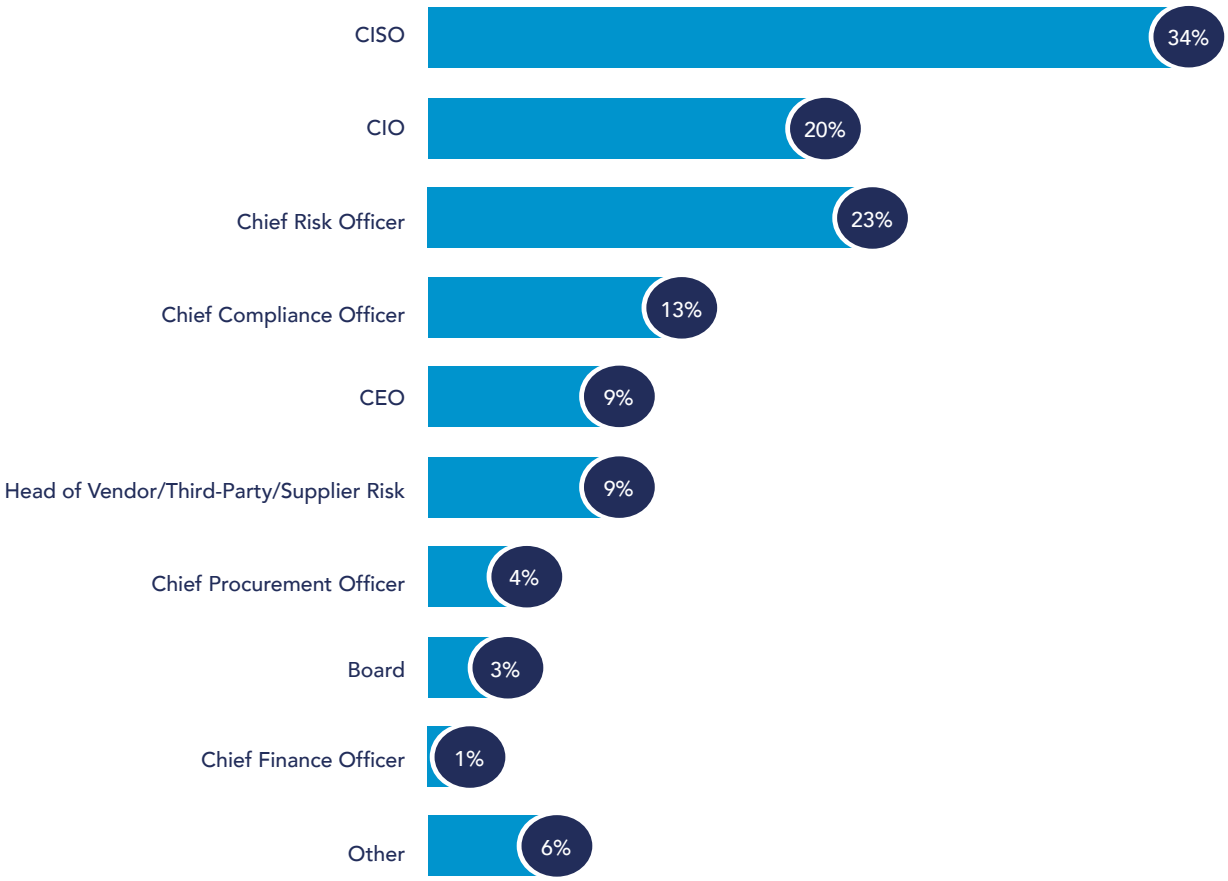
PART 1: GROWING AWARENESS OF THIRD-PARTY CYBER RISK

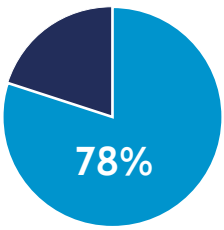
Major public security breaches are becoming commonplace in today's volatile cyber risk landscape. More and more, corporate executives and boards are being held responsible for cyber incidents. Coupled with this growing pressure are regulations like GDPR and the NYDFS, not to mention the financial consequences and major reputational fallout that can come with a breach. What's more, recent headline-grabbing third-party security breaches and heightened accountability are bringing more awareness and concern around third-party risk management.



Nearly 97 percent of respondents said that cyber risk affecting third-party vendors is a 'critical' (57 percent) or 'Important' (40 percent) issue. The C-suite is particularly aware of this issue and is taking responsibility for it in new ways. Respondents reported that CISOs, CIOs, Chief Risk Officers, Chief Compliance Officers and CEOs are primarily accountable for third-party risk within their organizations, and 1 in 10 organizations have a dedicated role for managing vendor, third-party or supplier risk.

Who has primary accountability for third-party cyber risk in your organization? (Multiple choice)



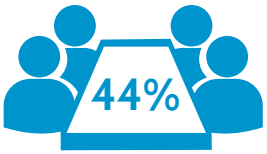


Organizations that have made third-party risk a C-level concern have firmly established cybersecurity posture as an important part of vendor selection. 41 percent of respondents said they would decline a business relationship, or terminate an existing relationship, due to a vendor's cybersecurity performance, while 37 percent say they have already done so. For this reason, demonstrating strong cybersecurity posture is now a clear imperative for organizations seeking to do business in the financial sector, as cybersecurity performance can be a business differentiator.

PART 2: THE DISCONNECT — A FALSE SENSE OF SECURITY FUELED BY A LACK OF CONSISTENT REPORTING

Despite the growing awareness of third-party cyber risk management as a business-critical practice, survey respondents suggest there are areas for improvement, particularly around measurement and risk reporting.

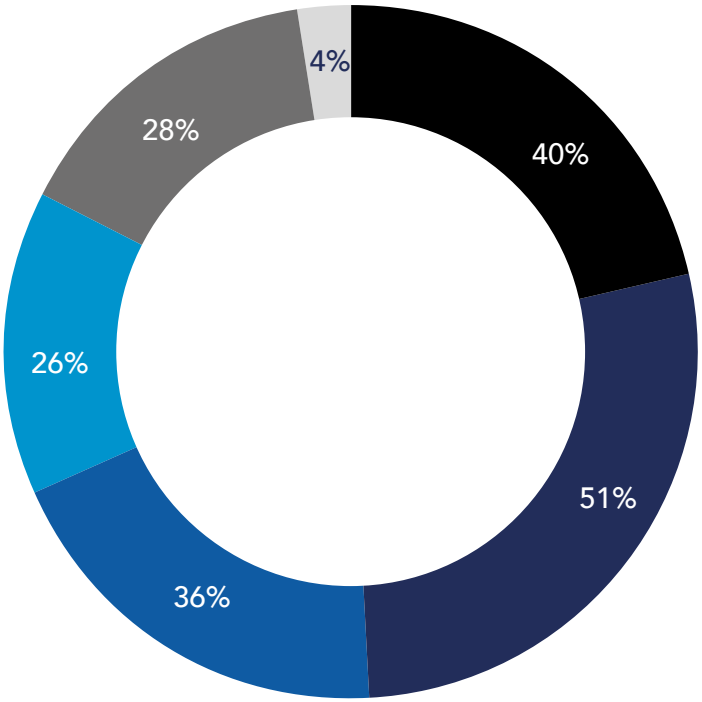
82 percent of those surveyed said that they believe executives and boards are confident in their approach to measuring and managing third-party risk, yet only around 44 percent are reporting on this risk to their executives and boards on a regular basis. How can companies expect boards to both understand and feel confident in their third-party risk management programs if they are reporting so infrequently on them? This lack of regular reporting could be the reason why **nearly 1 in 5 respondents think boards and executives are not confident or do not understand their approaches to TPRM.**



Clearly, financial services firms are still challenged to communicate and measure the effectiveness of their third-party risk management strategies to board members and to leadership. Organizations need to be thinking about what security metrics are most important, how to track them, and how to leverage them more effectively in executive communications. Beyond that, they need to consistently communicate how they are improving security and managing risk among third parties and other vendors.

Furthermore, though organizations cite fourth- and "nth"-party cyber risk as areas of concern, **more than 50 percent of respondents say that they do not have a strategy in place for fourth-party cyber risk.** As the importance of fourth-party risk management grows, we can expect that executives and boards will increasingly expect communication on these issues.

With respect to fourth party cyber risk, my firm (check all that apply)



40%	Collects information about fourth parties directly from our vendors/third parties
51%	Uses contractual language to reduce risk exposure
36%	Uses technology to assess our risk
26%	Is developing a strategy for fourth party cyber risk management
28%	Does not have a strategy for fourth party cyber risk management
4%	Other

PART 3: COMMON BARRIERS TO EFFECTIVE RISK MANAGEMENT

CeFPro and BitSight's survey also asked respondents to share the key third-party risk management challenges faced by their organizations. Many respondents reported concerns about the data gained from these risk assessments: its accuracy and quality, the actionability of the data, its timeliness, and the cost of data collection tools. Others cited the speed of the risk assessment process itself as a key challenge, as well as unclear responsibility within their organizations.

KEY CHALLENGES TO ASSESSING VENDOR CYBER RISK

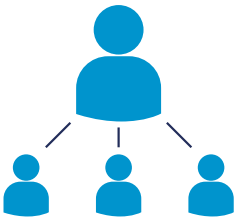
Data accuracy and quality

Actionability of data

Lack of continuous monitoring

Speed of the risk assessment process

Cost of on-site assessments



Unclear responsibility within an organization

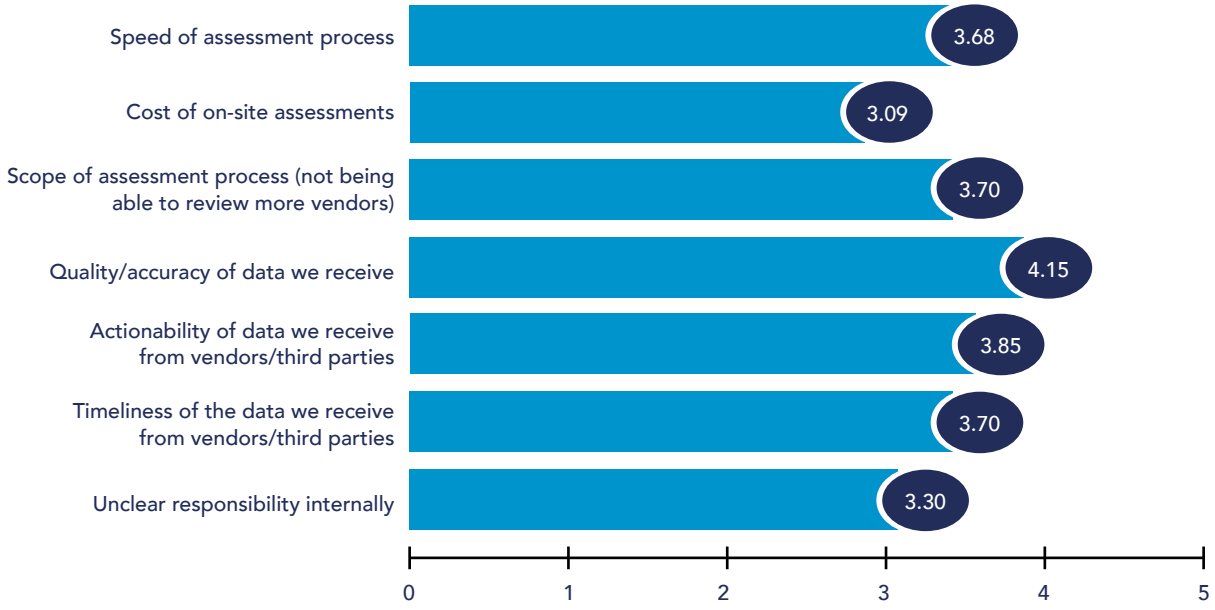
Survey respondents also called attention to key third-party risk management challenges they expect to face this year. Scaling a program to include growing numbers of third parties (including cloud service providers), creating a program responsive to the dynamic nature of the risk and business ecosystem changes, proactively sharing risk and vulnerability information, and fourth-party ("nth"-party) risk management were all cited as key issues. Meanwhile, the majority of respondents think that their firms' technology budget (55 percent) and services budget (57 percent) for third-party risk management will only increase slightly over the next three years. This means that **organizations will have to choose TPRM solutions carefully to leverage limited resources and make the most impact.**

One regulatory consultant for a European bank with greater than $100 billion assets under management (AUM) cited that "rapid changes in types of threats in combination with growing dependency on [third]-party IT infrastructures and solutions" is a major concern, which speaks to the increasingly complex landscape many financial services organizations are currently dealing with.

According to a professional at the SVP/VP/Director level of a $10-24 billion AUM bank in the UK, subcontractors and "nth"-parties will present a major challenge over the next year. This respondent posed the question, "How much further do you follow your data especially when NPI [nonpublic information] is involved?"

KEY TPRM CONCERNS

What issues related to the vendor cyber assessment process are you concerned about? Rank on a scale of 1-5, with 5 being of "higher concern"



"[Our] capacity to perform a detailed risk assessment of each third party [and] ongoing monitoring of their risk posture."

SVP/VP/Director of a bank in Africa with AUM of $50 - $100 billion

"Making all stakeholders understand the importance of this risk factor and the ensuing threats to business."

SVP/VP/Director of an Asia Pacific bank

"Having [the] ability to assess risk across the entire supply chain based on budget and resource constraints."

SVP/VP/Director at a technology company in the United States

"Identification of issues, but also forcing third parties to remediate."

SVP/VP/Director of a Canadian bank with AUM of $100+ billion

Despite these concerns and challenges, many organizations fail to utilize some of the most effective tools to assess the security of their vendors. Respondents reported that they still rely on tools like annual on-site assessments, questionnaires and facility tours to assess third-party security posture, giving them limited visibility into their third-party cyber risk. Meanwhile, only 22 percent of organizations are currently using a security ratings service to continuously monitor the cybersecurity performance of third-parties, though nearly 30 percent are currently evaluating a security ratings solution.

Security ratings are critical to effective evaluation and continuous monitoring of third-party ecosystem cyber risk, by providing an objective and comprehensive measurement of a third-party's security performance, similar to credit ratings for financial performance. Security ratings leverage terabytes of externally observable data on security behaviors in order to deliver an objective, data-driven rating. Organizations find these real-time metrics useful and cost-effective in evaluating potential partners and continuously monitoring security performance of critical third parties.

Organizations will likely look to cost-effective measures in order to maximize the value of their program. While 22 percent of organizations expect a "significant" increase in budget for third-party cyber risk management, nearly three-quarters of respondents say that their budget for third-party cyber risk will "increase slightly" or "stay the same."

A number of organizations find that technology can be useful in assessing the risk of fourth parties, bolstering data collected directly from third parties. Given the focus of many respondents on fourth- and "nth"-party risk, this is likely an area that will grow in future surveys.

PART 4: THE WAY FORWARD

New tools and best practices are becoming readily available to help organizations address some of the key challenges and concerns surrounding TPRM as uncovered by the survey. New technologies like security ratings can help organizations more consistently and effectively measure and report on third-party risk and their security management programs.

Survey respondents' concerns and priorities for the future speak to how integral these new solutions will become as cyber risks continue to evolve. Financial professionals are focused on making their security programs more formal and systematic, cost-effective, aligned with regulatory requirements, and focused on providing continuous monitoring and visibility.

Many recognized the balance needed between risk management and business needs. One U.S. banking manager described the importance of "creating a process to evaluate risks that does not slow down business."

One U.S.-based SVP/VP/Director in the transportation sector listed the most important future TPRM initiatives as "[the] collection and evaluation of TPRM documentation from vendors, development of internal documentation to show proof of program effectiveness, and compliance with emerging regulations (GDPR, [California Privacy Act], NYDFS, etc.)."

Another respondent, an analyst in the U.S. insurance sector, spoke of his organization's need to "reduce the time and burden on vendors to reply to information gathering, improve the richness of [the] data gathered, [gain] better knowledge of incidents when they happen and past incidents [and a] better knowledge of threats for the future."

In order to stay ahead of future priorities and challenges, organizations should look to the following best practices to help them measure and manage their cyber risk with third-party risk data that is accurate and actionable:

BEST PRACTICES IN TPRM

INTEGRATE & STANDARDIZE TPRM APPROACH

At a high level, it is critical for financial services companies to incorporate TPRM as a strategic part of their overall risk management program. After establishing a comprehensive list of third parties, organizations should work to standardize the risk assessment process and prioritize based on criticality. Through this standardization, organizations should map out important guidelines and processes such as the third party evaluation and assessment process, minimum security obligations and expectations (including security ratings), and steps to take to communicate in the event of a security issue or incident discovery.

USE CONTINUOUS MONITORING

Third-party risk assessment forms comprised of "yes" or "no" questions won't help financial services companies accurately understand security in an ongoing fashion – but continuous, objective, actionable data and metrics will. By using continuous monitoring tools, organizations can establish a level of trust with their third parties, but also verify their cybersecurity postures. For example, with security ratings, organizations gain real-time visibility into third- or fourth-party security vulnerabilities, allowing the issues to be addressed immediately.

ESTABLISH CONSISTENT BOARD REPORTING

Cybersecurity is increasingly becoming a board-level issue, yet communication and reporting strategies often fail to include security and risk metrics that are easily digestible for executive audiences. What's more, as our survey shows, financial services businesses are failing to report on third-party risk against any routine cadence. Security leaders can leverage data and metrics – including security ratings -- to pull together easily comprehendible reports on vendor risk and security concerns and establish a regular reporting cycle of, at minimum, once per year.

CREATE A FOURTH-PARTY RISK PROGRAM

As TPRM becomes an integral part of cybersecurity programs, organizations are paying increasing attention to fourth-party risk. Located at the outer web of a company's business ecosystem, fourth parties can also pose a considerable threat to an organization if compromised. Obtaining visibility into vendors' supply chains and contractor ecosystems through fourth-party monitoring is a critical step in maintaining good security hygiene in the financial services world.

ABOUT THE CENTER FOR FINANCIAL PROFESSIONALS (CEFPRO)

An international research organization and the focal point for financial risk professionals to advance through renowned thought-leadership, knowledge sharing, unparalleled networking, industry solutions and lead generation. CeFPro is driven by and dedicated to high quality and reliable primary market research; providing an excellent portfolio of peer-to-peer conferences and thought-leadership content.

Recently, CeFPro have launched a membership area for the industry to connect; inclusive of industry led content such as: Live interactive webinars, 50+ page quarterly magazine, filmed conference sessions, interviews, research reports, international surveys and much more. Find out more at www.cefpro.com.

BITSIGHT®
The Standard in SECURITY RATINGS

ABOUT BITSIGHT

Founded in 2011, BitSight transforms how organizations manage cyber risk. The BitSight Security Ratings Platform applies sophisticated algorithms, producing daily security ratings that range from 250 to 900, to help organizations manage their own security performance; mitigate third party risk; underwrite cyber insurance policies; conduct M&A due diligence and assess aggregate risk. With over 1,500 global customers and the largest ecosystem of users and information, BitSight is the most widely used Security Ratings Service. For more information, please visit www.bitsight.com, read our blog or follow @BitSight on Twitter.