TREASURY FRAUD & CONTROLS

2016 SURVEY REPORT

Performed & Analyzed by

STRATEGIC TREASURER

Underwritten by

Bottomline Technologies

TABLE OF CONTENTS

The table of contents shown on the right includes 10 logical sections, which can be used to explore the various survey results and commentary we have provided. In addition, we have included details on why those sections were selected, along with a high level overview of what they cover.

EXECUTIVE SUMMARY

INTRODUCTION

- ❑ HISTORY & NEED
- ❑ PARTICIPANT DEMOGRAPHICS

SUMMARY REPORT

INFOGRAPHIC

DETAILED FINDINGS

1) BANKING STRUCTURE, PRACTICES & CONTROLS
2) VISIBILITY & RECONCILIATION
3) SPEED OF DETECTION
4) BRIBERY & FRAUD REPORTING
5) ACCESS: SYSTEM & EMPLOYEE MONITORING
6) SANCTIONED PARTIES
7) FRAUD: SOURCES & EXPERIENCE
8) CYBER FRAUD RISKS & CONTROLS
9) CONTROLS: PREVENTION & DETECTION
10) SPENDING ON FRAUD MANAGEMENT

CONTACT INFORMATION

DETAILED FINDINGS: SECTION SUMMARIES

1. **Banking Structure & Control Framework.** These survey questions explore the practices and intentional control efforts as reflected in the banking structure and whether there is a formal control framework at the corporate and treasury levels that guide various practices and activities.

2. **Visibility & Reconciliation.** Visibility and reconciliation represent elements of rapid detective control methods. Lower visibility and slower reconciliations both create friction in early fraud detection. In many cases, both of these functions can stop fraud losses if they are timely and complete.

3. **Speed of Detection.** An organization's ability to detect fraud is vital as it often can prevent or minimize losses. These responses self-identify their organization's ability to detect fraud against different dimensions of value, time and type of fraud.

4. **Bribery & Fraud Reporting.** We wanted to understand what cultural defenses and practical steps were available to combat underlying issues that lead to fraud and that could act as preventative protection against future fraud attempts and losses.

5. **Access: System & Employee Monitoring.** This section of the survey explores practices used to defend system access (entry and removal of users), perform employee background checks, and maximize the effectiveness of segregation of duty protocols.

6. **Sanctioned Parties.** With increased requirements being placed upon corporations to screen for sanctioned parties, we knew many organizations were behind the curve. The intent of this section was to see the current state of affairs with regard to filtering activity and incidence of violations for these requirements.

7. **Fraud: Sources & Experience.** What have organizations been experiencing with regard to various types of fraud attempts and actual losses? Where have these attempts originated from (when known)?

8. **Cyber Fraud Risks & Controls.** Cyber fraud is a trending issue and regularly makes headlines as major incidents continue to occur. In this section, we explore a range of topics including: cyber fraud experiences, insurance coverage, and coverage trajectory.

9. **Controls: Prevention & Detection.** We wanted to assess the control practices of organizations against several different areas and differentiate between preventative controls, that prevent fraudulent actions from occurring, and detective controls that enable organizations to quickly detect if fraudulent actions are being attempted.

10. **Spending on Fraud Management.** It seems that in recent years, fraud has been paying for criminals. They seem to be increasingly focused on fraudulent activities, and their ROI for such activities has subsequently improved. There has been strong industry discussion about fraud, and it seemed prudent to identify the areas in which organizations plan to direct significant spend towards managing their exposure.

EXECUTIVE SUMMARY

Treasury professionals view fraud, cyber-fraud and the necessary controls as highly important issues. This concern and attention is true whether they are in global multinational corporations, bank treasuries, government or not-for-profit entities. This heightened attention comes from very public incidents of data breaches as well as hard dollar losses from the cyber/social engineered theft via man-in-the-email schemes.

Treasuries are paying more attention to these concerns, as is executive management. Organizations are also adding better controls and have plans to spend significantly more on better technology and improved processes. The investment is worthwhile, given the attempts and successes of the various criminals who pursue organizational assets.

This survey by Strategic Treasurer with Bottomline Technologies will be repeated annually to help determine various trends in practices and developments of all types of fraud activities that occupy the minds of treasurers.

Seeing what your peers are experiencing and doing to prevent and detect fraud is a good start. It is not the end. Determining what your organizational priorities are for security and controls and what steps, system changes and processes are necessary is next.

You will find some data confirms what you already know. Other elements should be quite eye-opening as to the extent of fraud attempts / successes and some of the practices of your peers. In many areas there is a great divide between excellent practices and ones below the standard of good corporate conduct.

We invite you to stay in touch with both Strategic Treasurer and Bottomline Technologies for receiving additional information and analysis on this and other Treasury Fraud & Control topics.

THANK YOU TO ALL WHO PARTICIPATED IN THE SURVEY!

Enjoy,

Craig Jeffery, *Managing Director*, Strategic Treasurer
Gareth Priest, *VP of Business Solutions*, Bottomline Technologies

Editors Note: *The following index of survey data does not contain every question asked as part of the Treasury Fraud & Controls Survey; it is a selection of many noteworthy responses. As part of an effort to limit the size of the report, certain questions and responses were redacted.*

INTRODUCTION

STRATEGIC TREASURER AND BOTTOMLINE TECHNOLOGIES ARE DELIGHTED TO BRING YOU THIS SUMMARY REPORT OF THE 2016 SURVEY ON TREASURY FRAUD & CONTROLS.

We sought to cover a broad range of current practices, to determine future methods of preventing fraud and implementing a strong controls system for treasury. This survey pulled together essential information from a variety of corporations with the goal of aiding in the elimination and prevention of fraud, recognizing weak areas within business practices and identifying areas where organizations are improving their control framework to address emerging and future threats.

The survey began in the fall of 2015 and was completed on January 2, 2016. More than 300 global respondents took part in this comprehensive survey. Over 60% of the respondents came from North America and over 25% were from EMEA. The remainder were from the Asia-Pacific region.

The genesis for this extensive survey came from our own efforts to answer questions about fraud and controls in Treasury departments. Instead of relying on various bits of anecdotal data, we searched for statistically relevant information. We found that, while there were several decent annual or bi-annual surveys that covered some aspects of payment fraud or types of control practices, there were far too many important questions and entire categories not covered. Additionally, some surveys researched only one country or a single region.

It was clear that the industry needed more information on a variety of topics with better global representation. To that end, we crafted the survey over a number of months and then released it to the treasury world. It is important to note that we were advised that treasury professionals would have neither the patience nor the time to complete a comprehensive fraud and controls survey. The fear of survey-length fatigue is real, but we found that by being up front about the amount of time the survey would require, we were able to get many responses.

We are grateful for the hundreds of people who took the time to add their contribution to this data by investing, in aggregate, many dozens of hours into this endeavor. Since there were numerous demographic questions and multiple regions of the world with significant numbers of respondents, we are able to stratify the data in statistically relevant ways. This stratification is useful for determining the differing practices and experiences across size, geography and industry sectors.

CURRENT STATE OF TREASURY FRAUD & CONTROLS

CRIME DOES PAY!

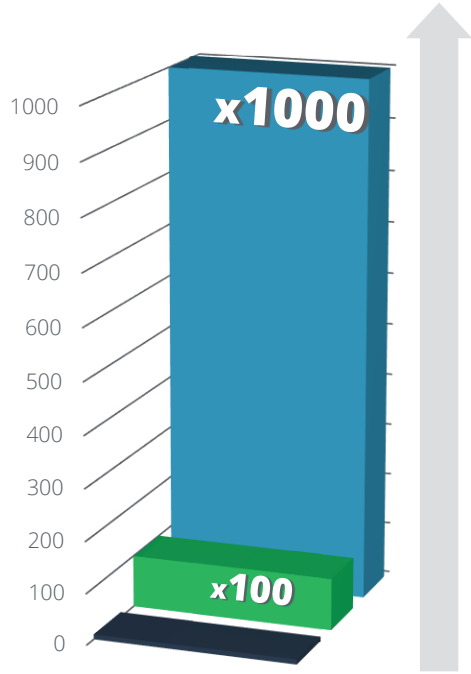
What must be done to change the risk/reward calculus?

WE HAVE LONG HEARD THAT CRIME DOESN'T PAY. AND, ULTIMATELY, IT DOESN'T. HOWEVER, WHAT HAS TRANSPIRED OVER THE PAST 24-36 MONTHS HAS SHOWN THAT THE RISK/REWARD CALCULATIONS FOR CRIMINALS PERPETRATING FRAUD HAVE MOVED DRAMATICALLY IN THEIR FAVOR.

In this battle, there has been a significant momentum shift in favor of the offense. Defense now needs revamp their efforts in order to change the calculus or risk/reward for the criminals.

While we may care about the security of the industry as a whole generally, the specific responsibility we have to the organizations we are a part of requires adjustments in order to move off of being one of the easier targets. What was a leading practice several years ago can quickly become the minimum standard (the standard of good corporate conduct) and, in some situations, completely inadequate.

Change is happening quickly in the area of fraud, and the controls we use to combat the criminals and protect our organizations must evolve in concordance with new threats that are identified.



SYSTEM FRAUD
Typical Payout Range:
$1M-10M+

WIRE (BEC) FRAUD
Typical Payout Range:
$130K+

CHECK FRAUD
Typical Payout Range:
$1K-2K

The above values are taken from calculations off of FBI, Banking Data and Strategic Treasurer estimates.

The risk/reward calculus for criminals has changed as the potential payouts are larger than ever. While many corporates are on the watch for check fraud, the larger targets remain unplanned for and vulnerable to attack.

FROM CHECK FRAUD TO ELECTRONIC (WIRE) FRAUD

MATURITY OF CHECK FRAUD

Check fraud has been supremely easy to perpetrate, especially in technology-ready and check-heavy countries like the United States. The criminals can be independent or part of crime syndicates. Those washing, printing and presenting fraudulent checks have been developing numerous schemes and variations in order to bilk organizations and banks of their funds. Defensive maneuvers and fraud detection services have continued to grow to keep the risk/reward ratio relatively low.

Based on data from the American Banking Association over the years, we see average losses based off total cases in the US typically averaging between $1,000 and $2,000. Services like positive payment, payee match positive payment and bank fraud detection algorithms and processes have limited the effective yield for these.

NEW TARGET: WIRE FRAUD

The calculus is dramatically different for wire related fraud versus check fraud by two orders of magnitude, on average, with much larger paydays possible. Check fraud losses average out in the $1K-$2K range (based upon ABA reported numbers), while wire fraud losses are averaging over $130K (derived from FBI data).

THE LARGER PAYOFF, WITH NO ADDITIONAL RISK, SUPPORTS THE ADDITIONAL ATTEMPTS AND PATIENCE OF THE CRIMINALS. OUR SURVEY DATA REFLECTS THIS CALCULUS: 77% OF FIRMS HAVE HAD IMPOSTER FRAUD ATTEMPTS ALONE IN THE PAST TWO YEARS. AND, OVER 10% OF THOSE ORGANIZATIONS TARGETED HAVE SUFFERED A LOSS.

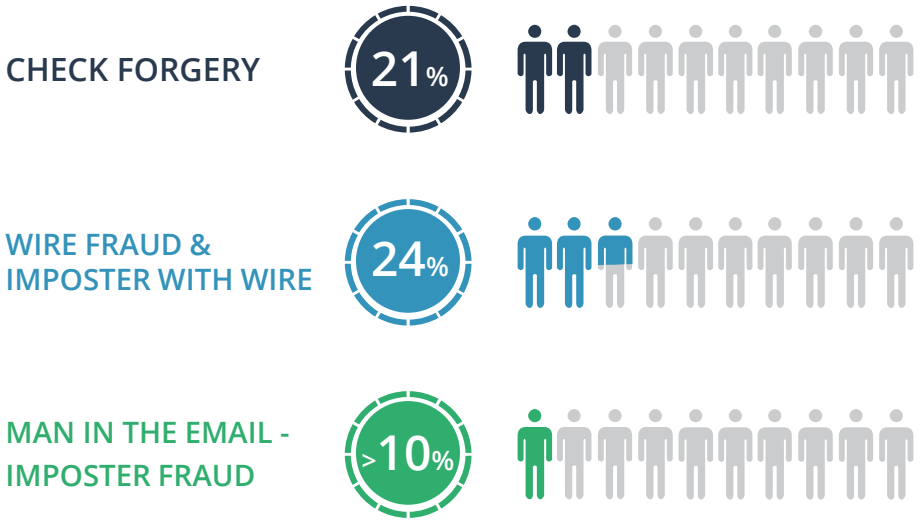
Dramatically higher yields, coupled with a higher success rate with wire fraud over against check fraud, represent an enormous opportunity for criminals. They understand arbitrage and have been busy shifting to electronic methods of perpetration. Too many organizations have not been equally busy or cognizant of the changing threat. It is time to recognize how the game has changed and what is necessary to stay ahead of criminals.

RISING ATTEMPTS WITH SIGNIFICANT LOSSES

ATTEMPTS AT FRAUD

While there has been a rise in wire and impostor fraud attempts and success, survey data indicates that traditional check forgeries still remain at the top of the list of attempts. The top fraud attempts in our survey were:

1. Check Forgery 39%
2. Wire Fraud/Impostor Fraud 31%
3. ACH Fraud 25%
4. Check Conversion Fraud 23%



SUCCESS RATES

Like the disparity in yields of different fraud types, successful rates for fraud differ too. Please note that the rates that are reported are aggregated and calculated by company rather than attempt. Some companies indicate they are experiencing more than four or five payment fraud attempts every day. Others find, after the fact, that the criminals targeting them were very methodical and patient in their approach.

Rather than undergo multiple attempts, these criminals waited for the opportune moment to make their move and came away with a very healthy payoff. The survey provides some interesting percentages of success versus attempt or attempts over several years.

- **10% Man in the Email/Impostor Fraud.** These large-amount fraud attempts resulted in 8% of survey respondents suffering a loss. Additionally, more than one in ten companies that were targeted suffered a loss in the past two years.
- **24% Wire Fraud and Impostor Fraud with Wire.** Nearly one in four firms that were targeted for this type of fraud experienced some loss over a two-year period.
- **21% Check Forgery.** Over one in five firms that were targeted for check forgery suffered a loss in the past two years.

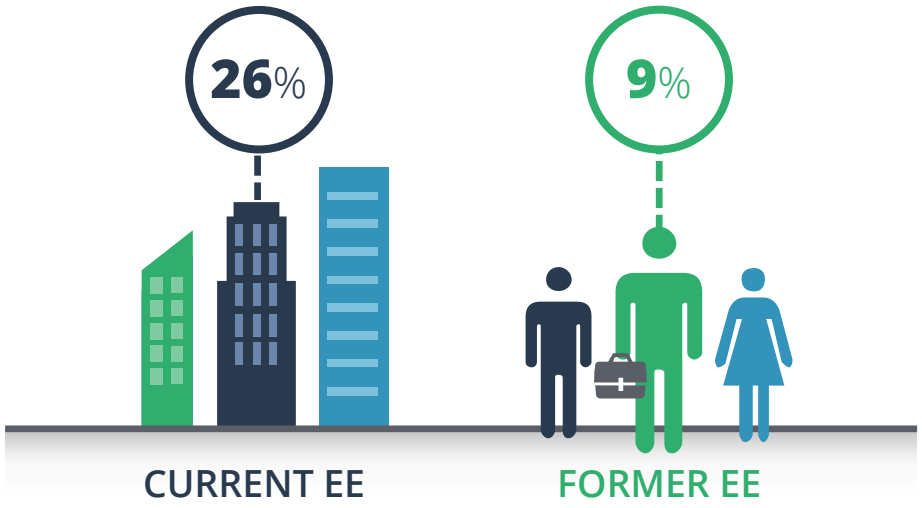
ATTACKS COME FROM CLOSER THAN YOU THINK

SOURCES OF FRAUD

Identifying the source of fraud is useful if you are interested in finding appropriate ways of deterring or stopping it. Here is what we found (more than one type of fraud was possible):

EMPLOYEES WERE IDENTIFIED AS THE SOURCE OF FRAUD IN OVER ONE THIRD OF THE CASES REPORTED.

- **Employees (EE)** **36%**
  - *Current EEs* *26%*
  - *Former EEs* *9%*
- **Non-Employees** **59%**
- **Unknown and Other Sources** **11%**

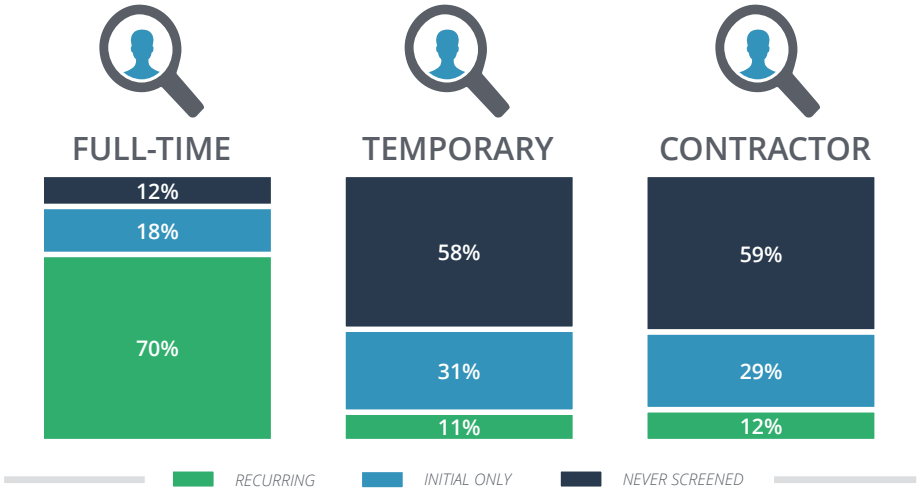


EE AND WORKER SCREENING

Despite the fact that more than 1/3rd of organizations have experienced recent fraud from current and former employees, background checks are not as prevalent as we expected.

Since EEs were identified as the source of fraud at 36% of organizations, background checks would seem like a logical method of combatancy. And, not just for employees. However, the results show there is a significant personnel gap.

- **12%** of EEs were Not Checked Ever
- **58%** of Temporary Workers were Not Checked Ever
- **69%** of Contractors were Not Checked Ever



CORPORATE TREASURY FALLING BEHIND ON SECURITY

AREAS IN NEED OF SIGNIFICANT IMPROVEMENT

THERE ARE A NUMBER OF FINDINGS THAT REPRESENT CRITICAL AREAS OF EXPOSURE FOR FAR TOO MANY ORGANIZATIONS.

A few items that you'll want to read more closely within the report include:

- 57% of firms have NO control framework. None. Nothing in treasury. Nothing at the corporate level. Given what we have seen with regard to fraud over the past few years, this is deeply disturbing. (see slide 17)
- Only 42% of firms have formally assigned fraud monitoring roles and responsibilities. (see slide 19)
- Control Design: 25% have a banking structure that either does not reflect any control design (10%) or only partially reflects a control design (15%). (see slide 15)
- 35% of organizations do NOT screen for sanctioned parties at any time in their processes. They instead rely on banks to, hopefully, catch the problem. By then it is a reportable event. (see slide 31)

CONTROL FRAMEWORK

57% of firms have no control framework. None. Nothing in treasury or at the company level.

57%

CONTROL DESIGN

25% of firms have banking structures that do not (10%) or only partially (15%) reflect a control design.

25%

FRAUD MONITORING

Only 42% of firms have formally assigned fraud monitoring roles and responsibilities.

42%

SANCTION SCREENING

35% of firms do NOT screen for sanctioned parties at any time in their processes, relying solely on banks.

35%

STRENGTHS IN CURRENT STATE OF CONTROLS

AREAS OF POSITIVE PROGRESS

There are organizations who are constantly working to improve their controls and processes. These controls can be preventative (stopping fraud from occurring) or detective (the ability to identify that fraud has happened – or that there is some problem).

Detective controls, if performed quickly and automatically, have the ability to prevent future losses and in some cases block an attempt that is transpiring. Visibility and Reconciliation are two interesting examples.

- 24% of firms in the survey indicated that they reconciled 100% of their bank accounts on a daily basis. And, 45% reconcile 90% or more of their accounts on a daily basis (see slide 23).
  - 27% of small companies reconcile 100% of their accounts daily while only 21% of larger firms do.
  - 29% of EMEA firms reconcile 100% of their accounts on a daily basis versus only 22% of firms in the Americas.
- High Visibility. 70% of firms can see 90-100% of their bank account balances and activity on a daily basis (see slide 22).
- Anti-Bribery/Corruption. 70% of respondents indicate their firm had a policy on ABAC. 16% were uncertain of whether they had a policy or not (see slide 27).

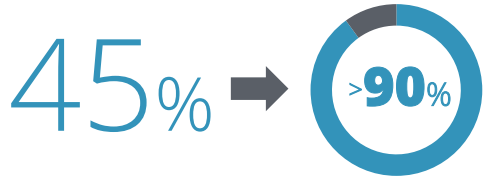
SYSTEM ACCESS

For all the talk about bring-your-own-device (BYOD), organizations are being very cautious about the use of certain technologies for initiating transactions. These are the numbers where companies say NO to using them for transaction initiation (see slides 29-30):

- **BYOD.** 90% do not allow employees to use their own device for initiating transactions
- **Mobile.** 88% do not allow mobile devices to be used to initiate transactions

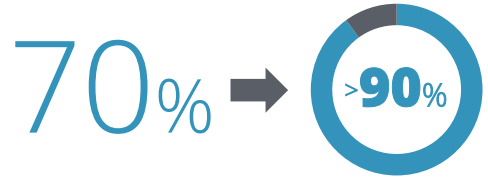
RECONCILIATIONS

45% of firms reconcile 90% or more of their bank accounts daily. 24% of firms reconcile 100% of their accounts daily.



VISIBILITY

70% of firms can see 90-100% of their bank account balances and activity on a daily basis.



A.B.A.C. POLICY

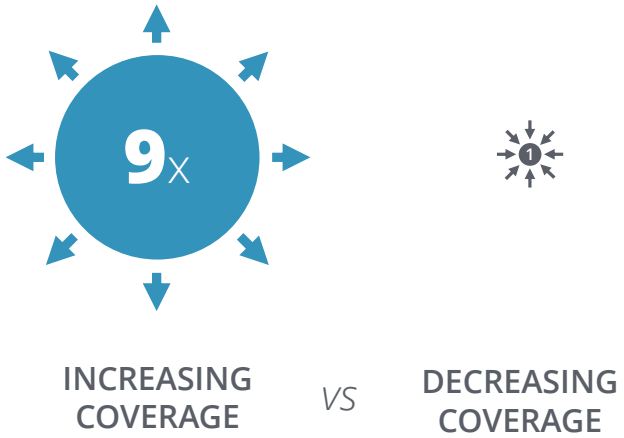
70% of respondents indicated their firm had an Anti-Bribery/Anti-Corruption policy on file. 16% were uncertain.

TACTICS FOR LESS EXPOSURE & MORE PROTECTION

PROTECTING OURSELVES

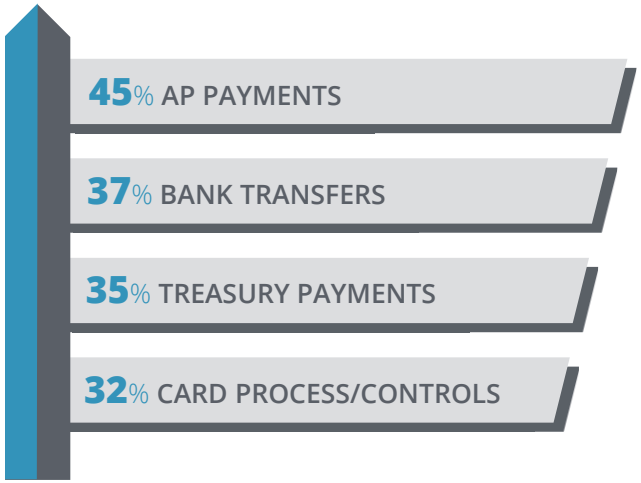
THERE ARE TWO MAIN STEPS BEING TAKEN BY ORGANIZATIONS TO REDUCE THEIR EXPOSURE TO FRAUD AND LOSSES – PURCHASING CYBER FRAUD INSURANCE AND SIGNIFICANTLY INCREASING THEIR TECHNOLOGY SPEND.

Cyberfraud Insurance. For those that increased the amount of cyber fraud insurance coverage they had versus those that decreased their coverage, the ratio was 9 to 1. In raw numbers, 27% of firms increased their cyber fraud coverage over the previous year. (see slide 42)



Technology Spend. Plans to spend and actual spending are two key measures of how important something is to an organization. The areas of planned significant spend to combat fraud and increase controls are as follows (see slide 43):

- AP Payments 45%
- Bank Transfers 37%
- Treasury Payments 35%
- Card Process/Controls 32%



FINAL THOUGHTS

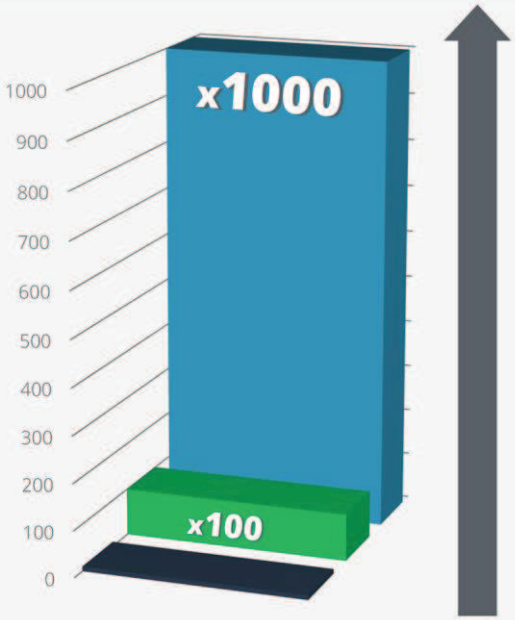
AS WE STATED EARLIER, CRIMINALS HAVE ENHANCED THEIR TECHNIQUES FOR TARGETING CORPORATIONS. A PROPER RESPONSE AND FRAMEWORK IS REQUIRED TO MEET THIS ONGOING CHALLENGE.

We hope you enjoy reading this document and learning what your peers think, what they have experienced and their plans to meet these threats.

Strategic Treasurer and Bottomline Technologies invite you to enjoy the material and then take the necessary steps to ensure your organization is appropriately protected.

Let us know if we can be of assistance in any way.

CRIME DOES PAY!



SYSTEM FRAUD
Typical Payout Range:
$1M-10M+

WIRE (BEC) FRAUD
Typical Payout Range:
$130K+

CHECK FRAUD
Typical Payout Range:
$1K-2K

The above values are taken from calculations off of FBI, Banking Data and Strategic Treasurer estimates.

The risk/reward calculus for criminals has changed as the potential payouts are larger than ever. While many corporates are on the watch for check fraud, **the larger targets remain unplanned for and vulnerable to attack**.

...& IT'S ON THE RISE

TOP FOUR TYPES OF FRAUD ATTEMPTS

1. CHECK FORGERY
2. WIRE / IMPOSTER FRAUD
3. ACH FRAUD
4. CHECK CONVERSION

While there has been a rise in wire and imposter fraud, survey data indicates that traditional check forgeries still remain on top of the list of attempts.

On the whole there has been a progressive increase in both fraud attempts and successes on multiple fronts.

REAL RATES OF LOSS

CHECK FORGERY

More than one in five firms that were targeted for check forgery suffered a loss in the past two years.

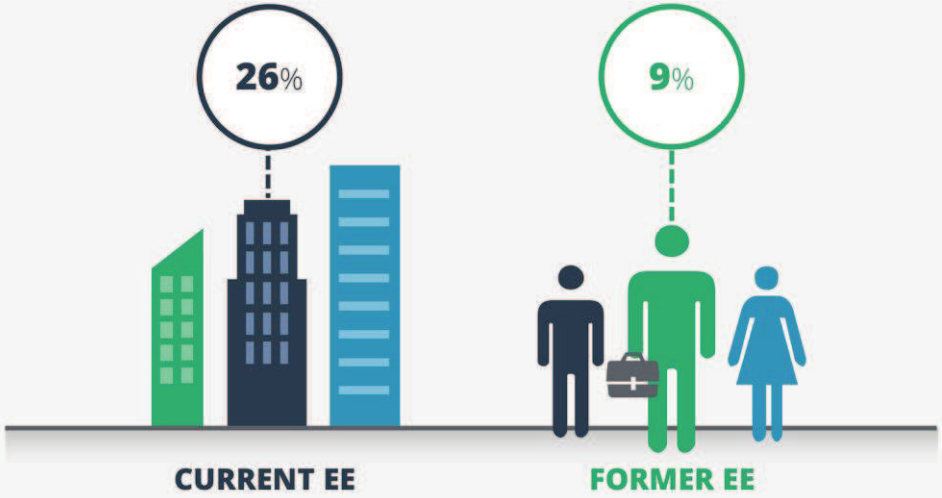
WIRE FRAUD & IMPOSTER WITH WIRE

Nearly one in four firms targeted for this type of fraud experienced some loss over a 2-year period.

MAN IN THE EMAIL/IMPOSTER FRAUD

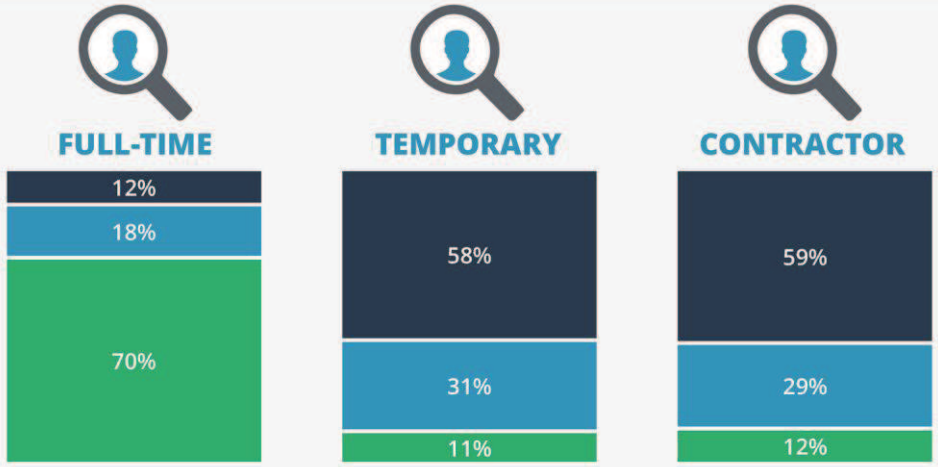
These large-sum fraud attempts resulted in 8% of firms overall suffering a loss (>10% who were targeted).

FROM INSIDE & OUT



Over 1/3 of respondents identified their corporation's employee (EE) roster (current + former) as a source of fraud for their firm. 59% of firms also claimed non-EE as a source and 11% claimed unknown and/or other sources as well.

EE SCREENING...



Limited or no background checks have left many corporations vulnerable to attack. But employee screening is only the start. There are a number of critical areas of exposure threatening many organizations.

AREAS OF HIGH RISK!

57%

CONTROL FRAMEWORK

57% of firms have no control framework. None. Nothing in treasury. Nothing at the company level.

42%

FRAUD MONITORING

Only 42% of firms have formally assigned fraud monitoring roles and responsibilities.

25%

CONTROL DESIGN

25% of firms have banking structures that do not (10%) or only partially (15%) reflect a control design.

35%

SANCTION SCREENING

35% of firms do NOT screen for sanctioned parties at any time in their processes, relying solely on banks.

POSITIVE PROGRESS...

45% → >90%

RECONCILIATIONS

45% of firms reconcile 90% or more of their bank accounts daily. 24% of firms reconcile 100% of their accounts daily.

70%

A.B.A.C. POLICY

70% of respondents indicated their firm had an Anti-Bribery/Anti-Corruption policy on file. 16% were uncertain.

70% → >90%

VISIBILITY

70% of firms can see 90-100% of their bank account balances and activity on a daily basis.

LIMITED SYSTEM ACCESS PROVIDES ADDED PROTECTION

88%

MOBILE INITIATION

Do not allow mobile transaction initiation

90%

B.Y.O.D. POLICY

No transaction initiation from personal devices

PROTECTIVE TACTICS

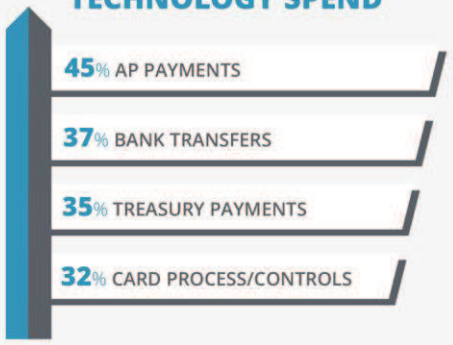
TOP 2 TACTICS USED TO REDUCE EXPOSURE & INCREASE PROTECTION FROM LOSS

CYBERFRAUD INSURANCE

INCREASING COVERAGE *VS* DECREASING COVERAGE

The ratio of firms change in coverage year to year was 9:1 in favor of more protection.

TECHNOLOGY SPEND



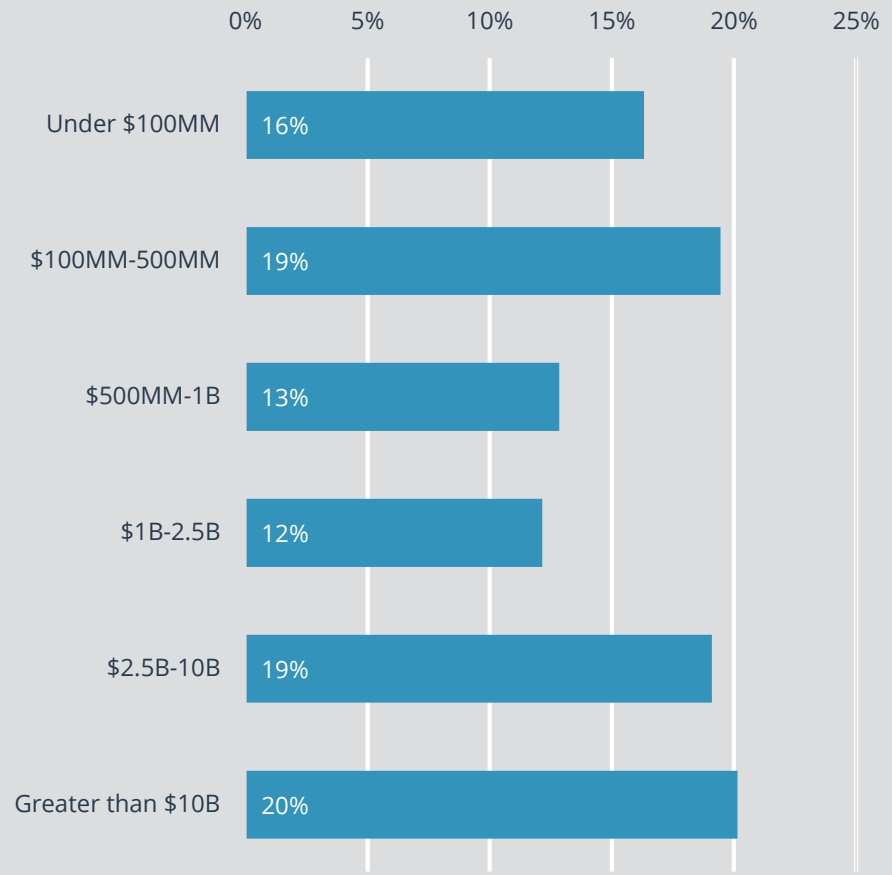
The top 4 areas of planned significant spend to combat fraud and increase controls.

SURVEY APPENDIX

DETAILED FINDINGS *FROM SELECT SURVEY* QUESTIONS & RESPONSES

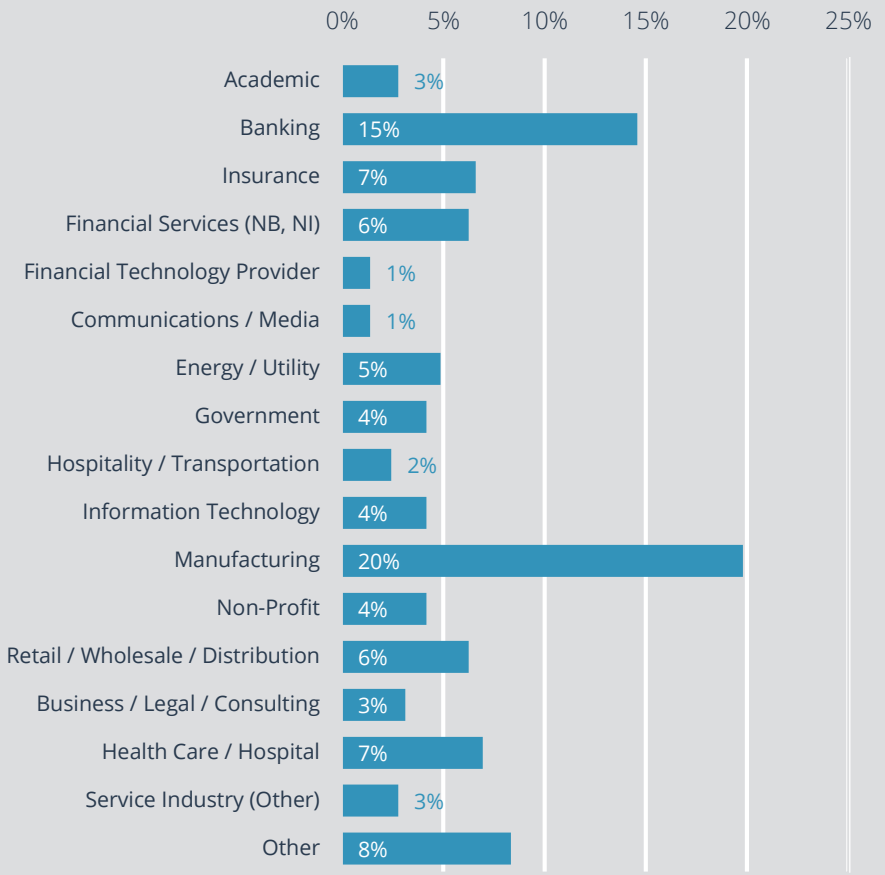
The following index of survey data does not contain every question asked as part of the 2016 Treasury Fraud & Controls Survey. It is a selection of many critical and noteworthy responses. As part of an effort to limit the size of this report, certain questions and responses were redacted.

What is your company's annual revenue?



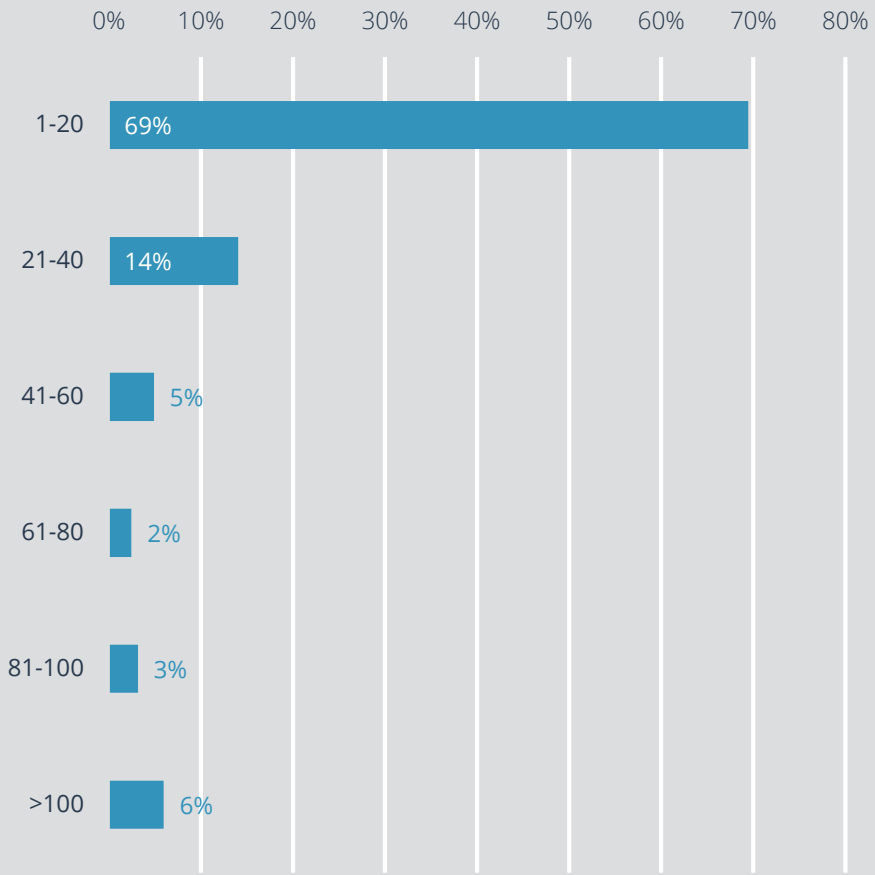
Revenue Size. 51% $1B plus in annual revenue. Approximately 1/5th in the $2.5--10B range and in the $10B+ range. The revenue size represented in this survey is well distributed which should allow for effective analysis by organizational size.

What is your organization's industry?

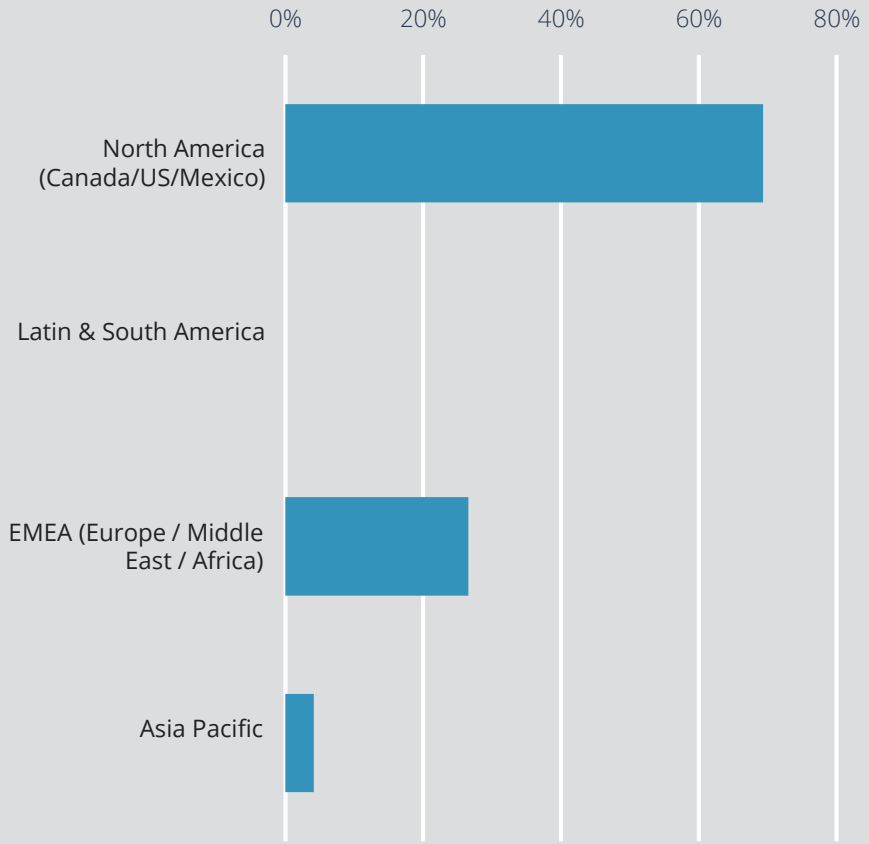


Industry. Manufacturing and banking led all other industries by a substantial margin.

Our business operates in this many countries:



In what region is your organization headquartered?

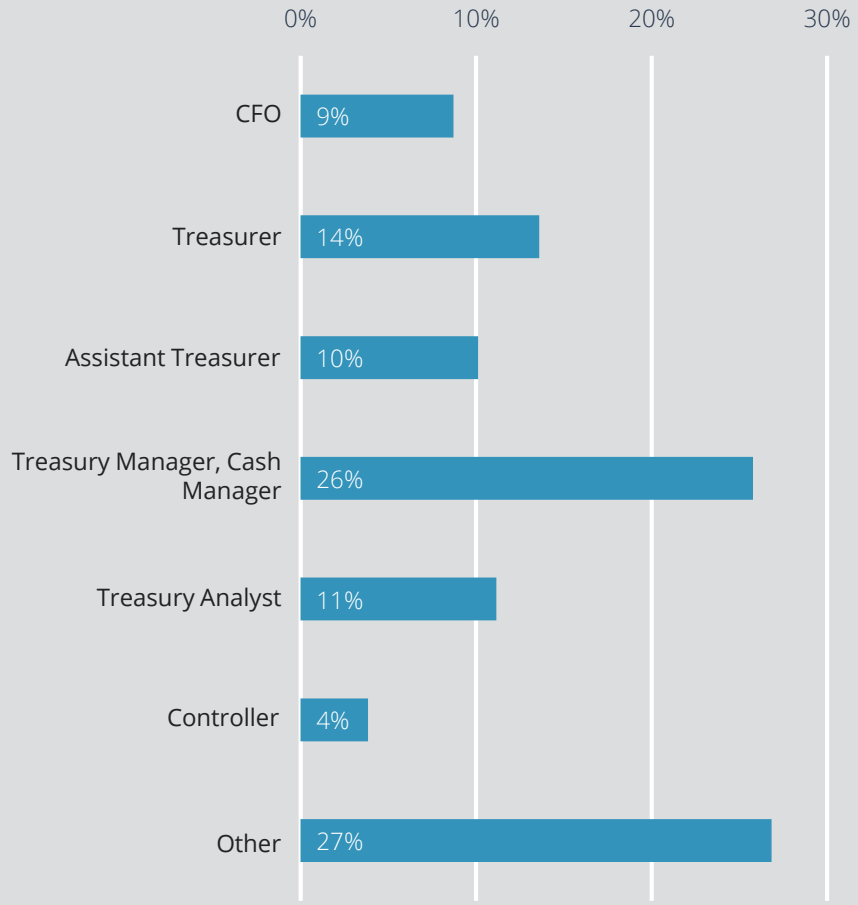


Geographic Complexity. For this measure, we used the number of countries as one proxy for geographic complexity. More operating countries increases treasury intensity.

a. 6% of firms operate in over 100 countries.
b. 31% are in 21 or more countries.

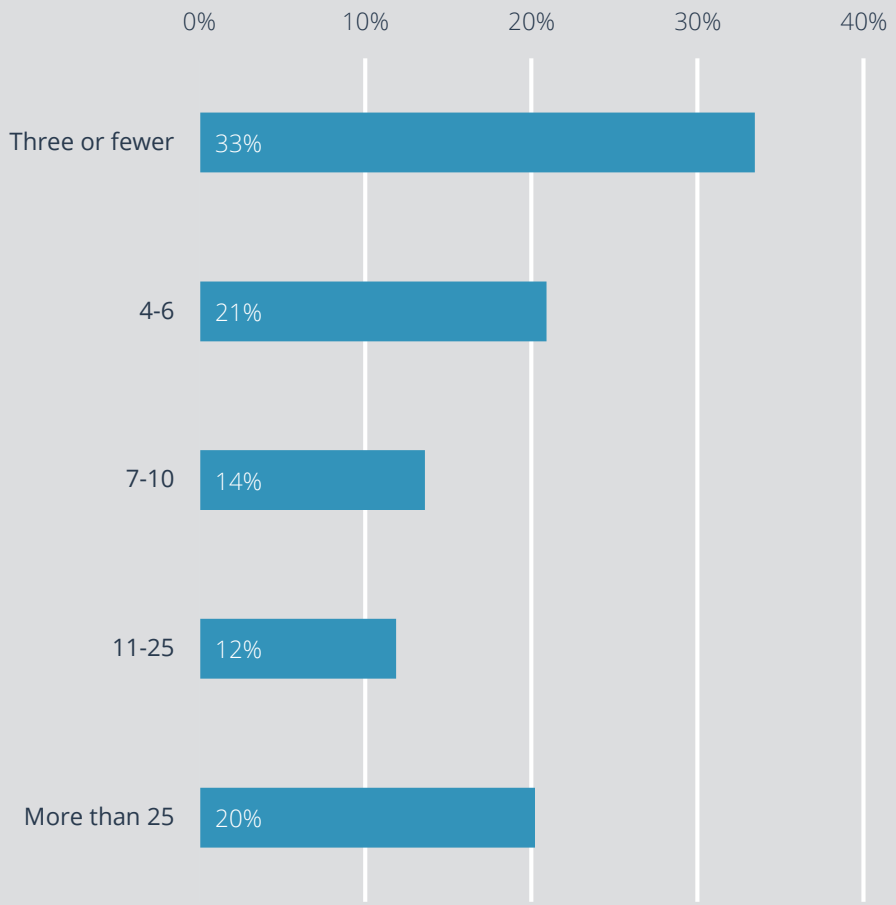
Distribution. North American concentration (>60%). EMEA (>25%). This allows for some excellent stratification by region.

What is your role?



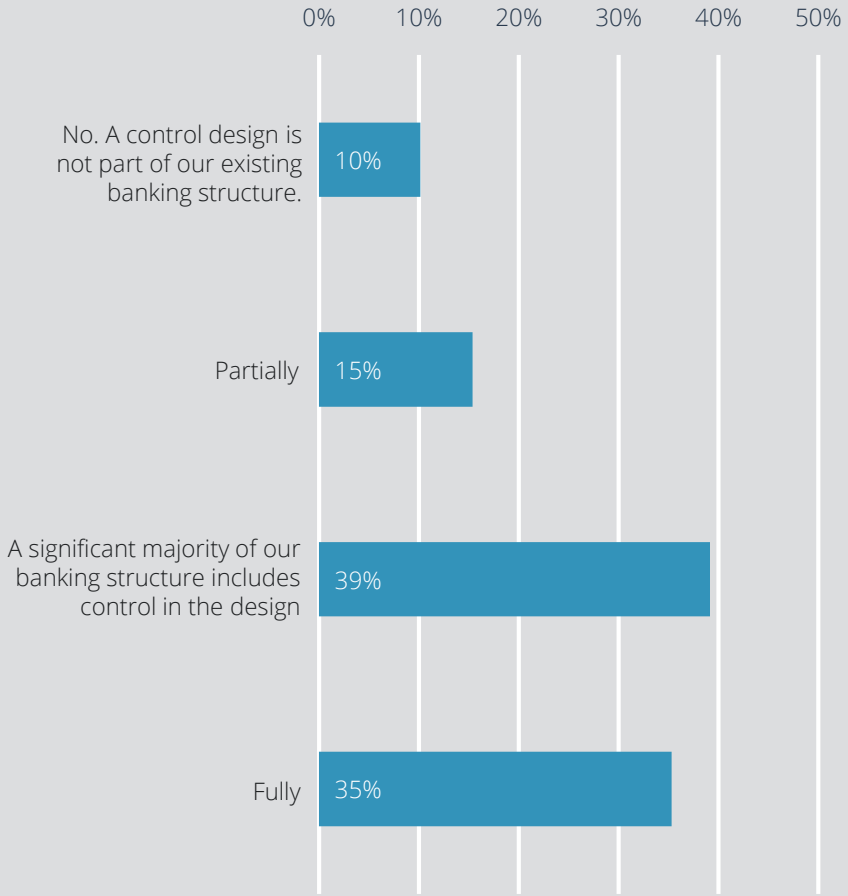
Roles. Executive level participation in the survey was high as 1/3rd of participants were CFO, Treasurer or Assistant Treasurer. Various manager level functions (Treasury Manager, Cash Manager) took up a full 1/4th of the roster (26%). Other various roles in finance reported participation by the1/4th of the respondents (27%) who selected the "Other" option.

How large is your global treasury organization, including analysts?



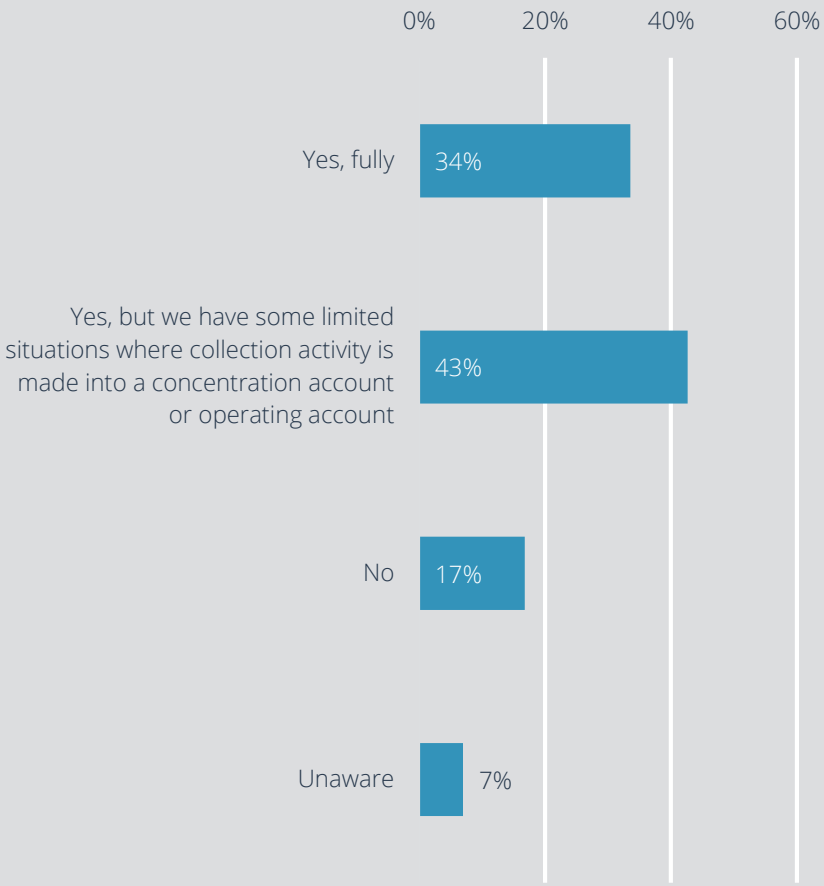
Size of Treasury. 1/3rd of respondents had a staff of three or less. 32% had 11 or more with 1/5th of organizations having more than 25 staff in treasury.

Does your banking structure intentionally reflect a control design?



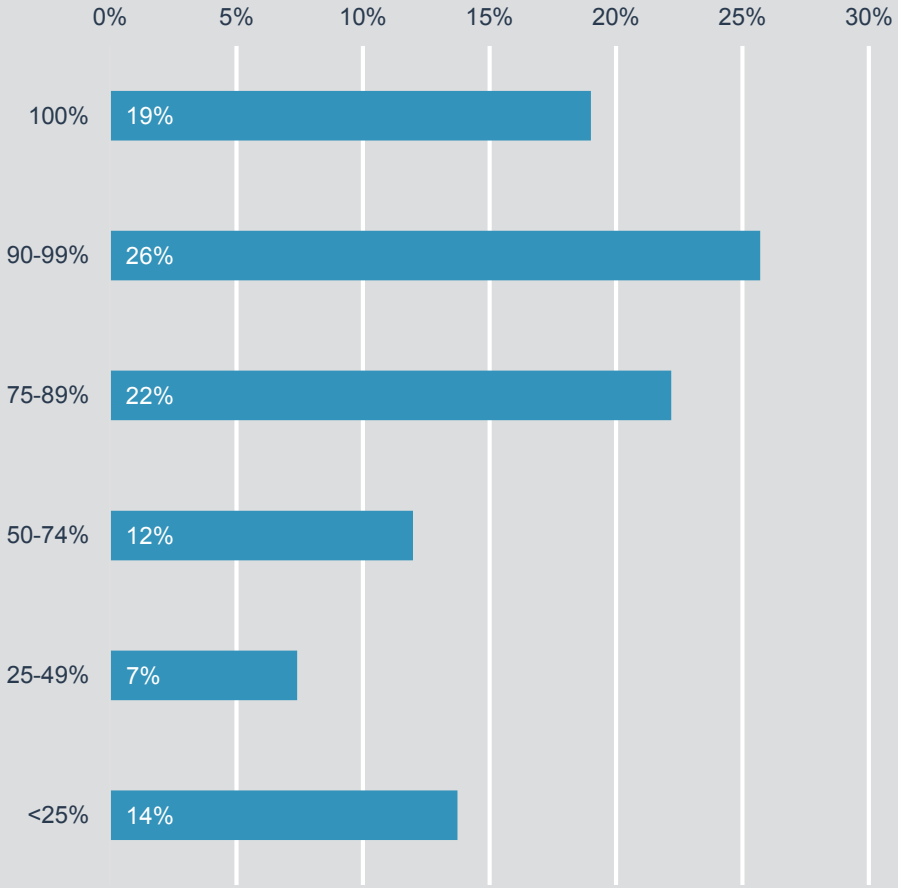
Banking Structure. Intentional Control Design. Happily, just over 1/3rd indicate their banking structure fully represents a control design. Another 39% indicate that a majority of their banking structure reflects this control design. Only 1/4th of the respondents indicate no control design or a partial control design.

We use certain bank accounts for collection activity and drive all receipts towards those accounts?



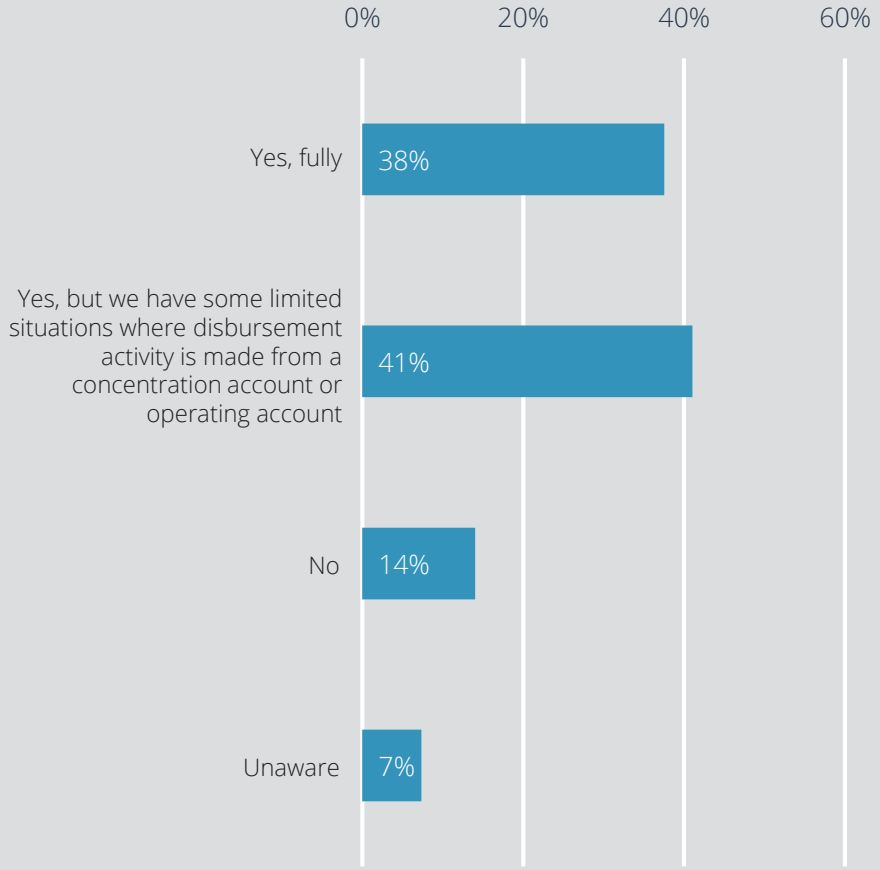
Collection Activity. Bank Accounts and Receipts. 1/6th do not use certain bank accounts for collection activity. (1/14th were unaware what their situation was). And, just over 1/3rd were fully engaged with the practice of using certain accounts for collection activity and driving receipts in that direction.

What percentage of your bank accounts are connected to your core concentration bank account structure (via standing wire transfer, ZBA, pooling)?



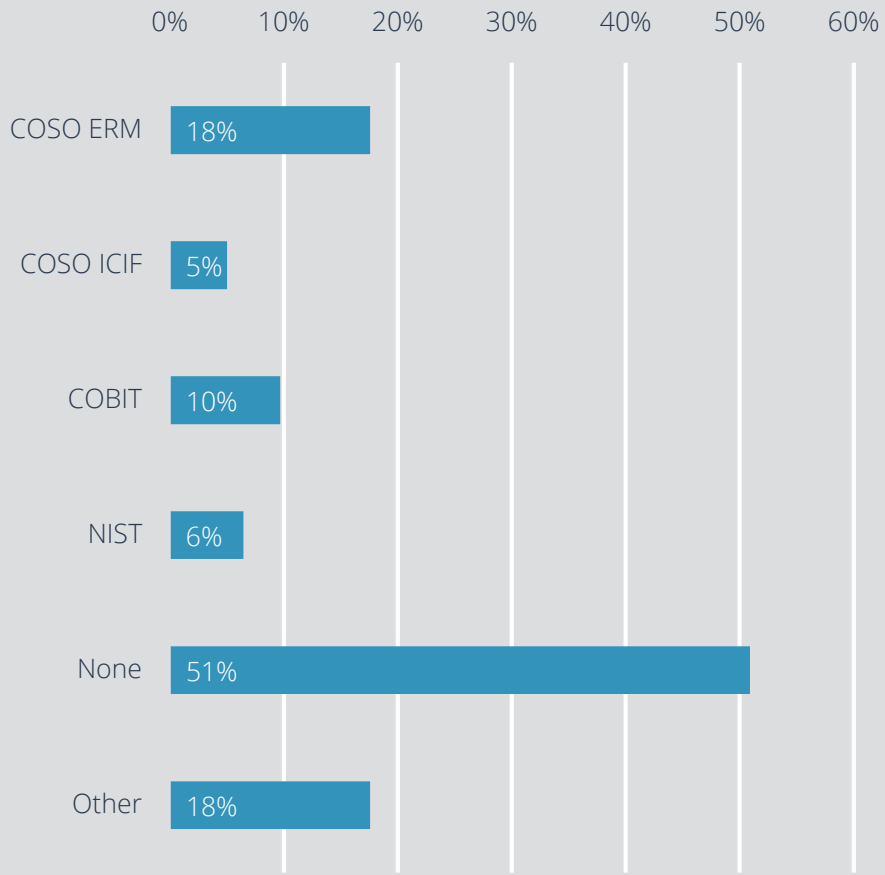
Connected Bank Accounts. Almost 1/5th of firms have 100% of their accounts connected via automated means (AST, ZBA, Pooling). 21% have less than one half of their accounts connected via one of these methods.

We use certain bank accounts for disbursement activity and make all non-treasury disbursements from those accounts?



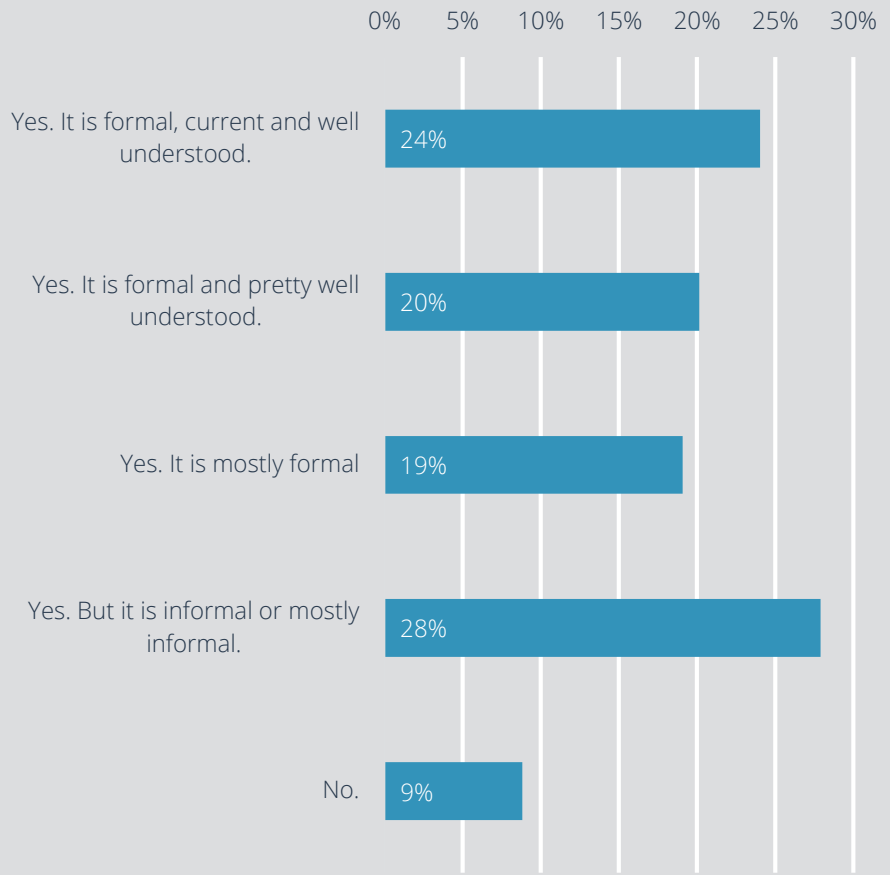
Disbursement Activity. Bank Accounts and Disbursements. 1/7th do not use this practice. Just over 1/14th were unaware and 38% fully deployed this method of disbursement control via account.

We use the following control or IT control framework(s) (check all that apply).



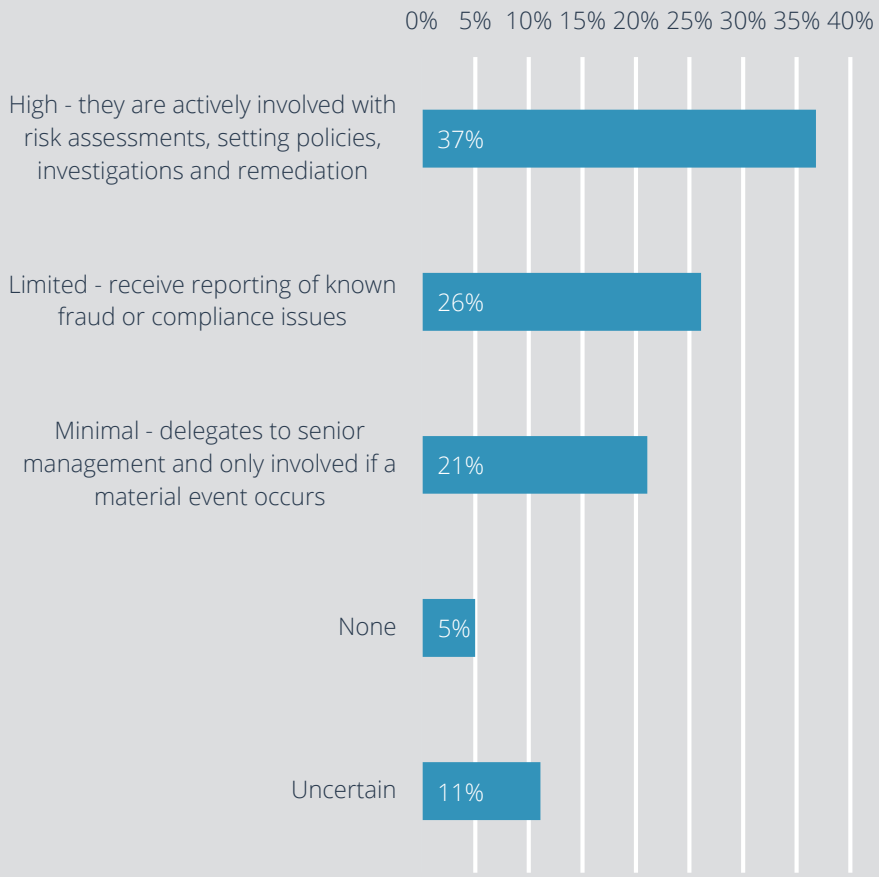
Control Framework (IT or otherwise). A big surprise was that just over half had no control framework and another 18% didn't know or weren't sure (a total of 69%). This represents, in our view, a significant gap in controls especially considering the size of the organizations participating in this survey. Those with a control framework included: Committee of Sponsoring Organizations Enterprise Risk Management (COSO ERM) which led the way with 18% of respondents. Control Objectives for Information and Related Technology had 10%, National Institute of Standards & Technology was third with 6% and Committee of Sponsoring Organizations Internal Control Integrated Framework (COSO ICIF) placed fourth at 5%.

Do you have a treasury fraud and controls framework?



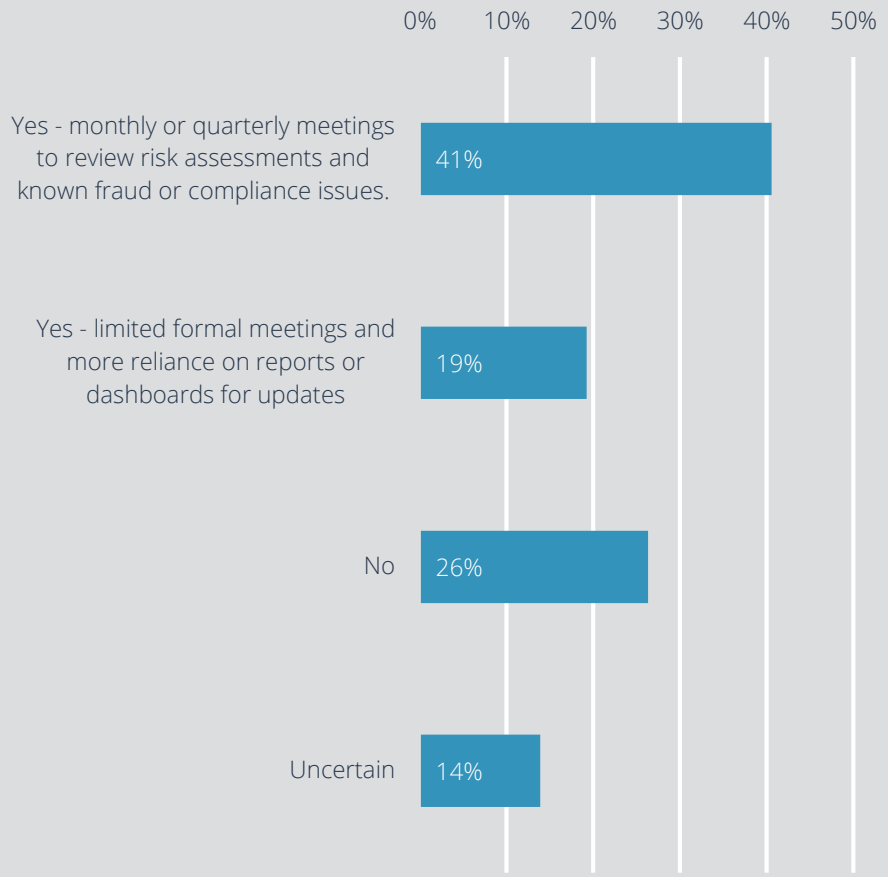
Treasury Control Framework. The most prepared (current, formal and well-understood) represent just under one in four (24% of the respondents). One in eleven (9%) did not have any type of control framework (formal or informal). 37% had either no framework or one that was informal. For context, this shows that treasury is more apt to have some form of control framework than the organization at large. 1/9th of treasury groups and one half of organizations had none. This also seems to indicate that the need is greater within treasury than for the organizations at large.

What level of engagement does the Board of Directors have in risk, fraud & compliance allegations or investigations?



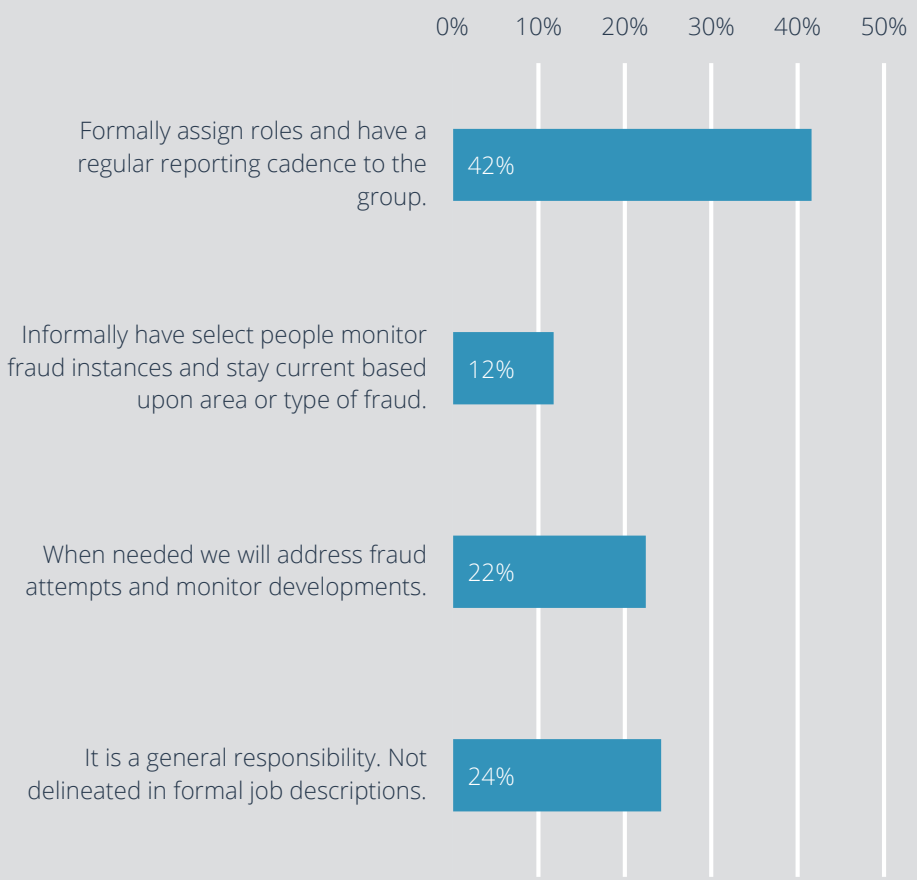
BOD Engagement in Fraud. Over 1/3rd of organizations (37%) have high involvement with risk assessments, setting policies and managing remediation.

Does your organization have a risk/fraud management committee which meets on a regular basis?

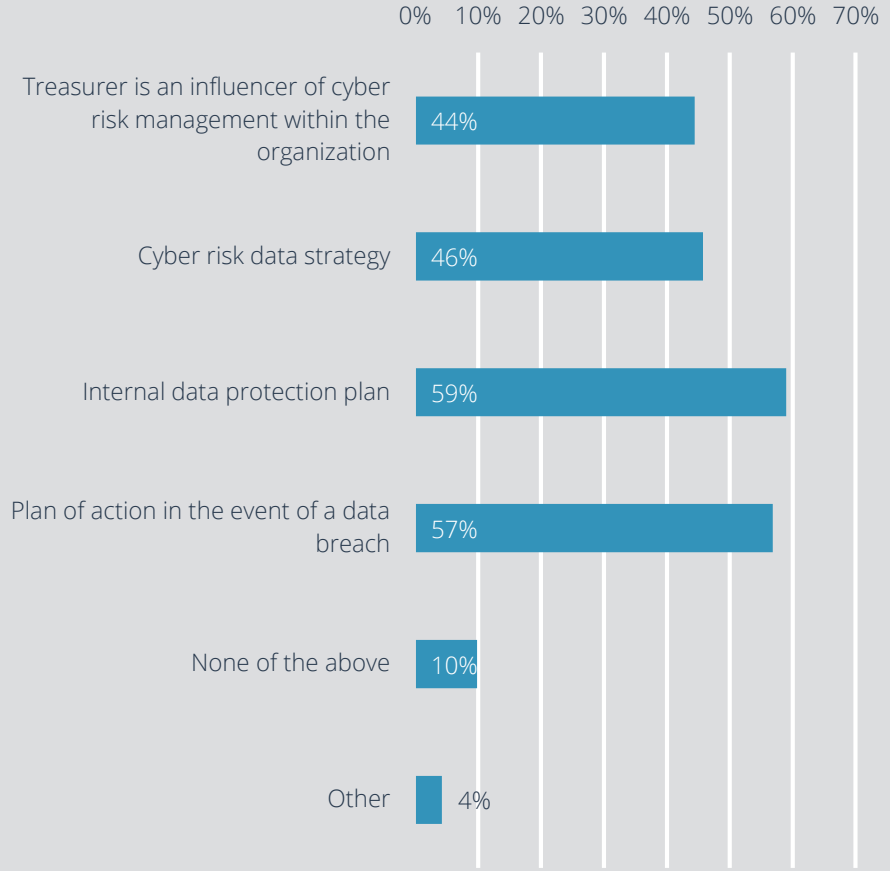


Fraud/Risk Management Committee Meetings. 4 out of 10 have monthly or quarterly meetings to review.

For assigning responsibility to track fraud and stay current on development, we:



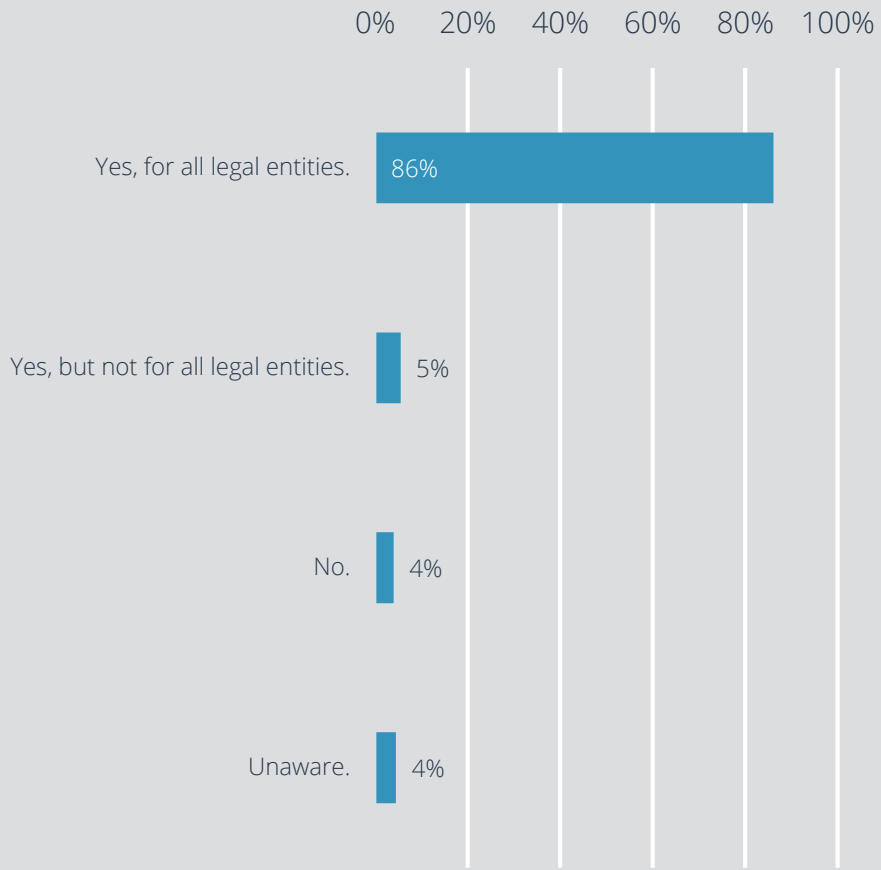
Does your organization have the following? (Check all that apply)



Monitoring Fraud. Formally assigning responsibility to stay current on fraud seems to be a clear leading practice that most (58%) are not following. Even accounting for the 12% who have an informal assignment, we are still left with almost half (46%) with no direct assignment of this important role.

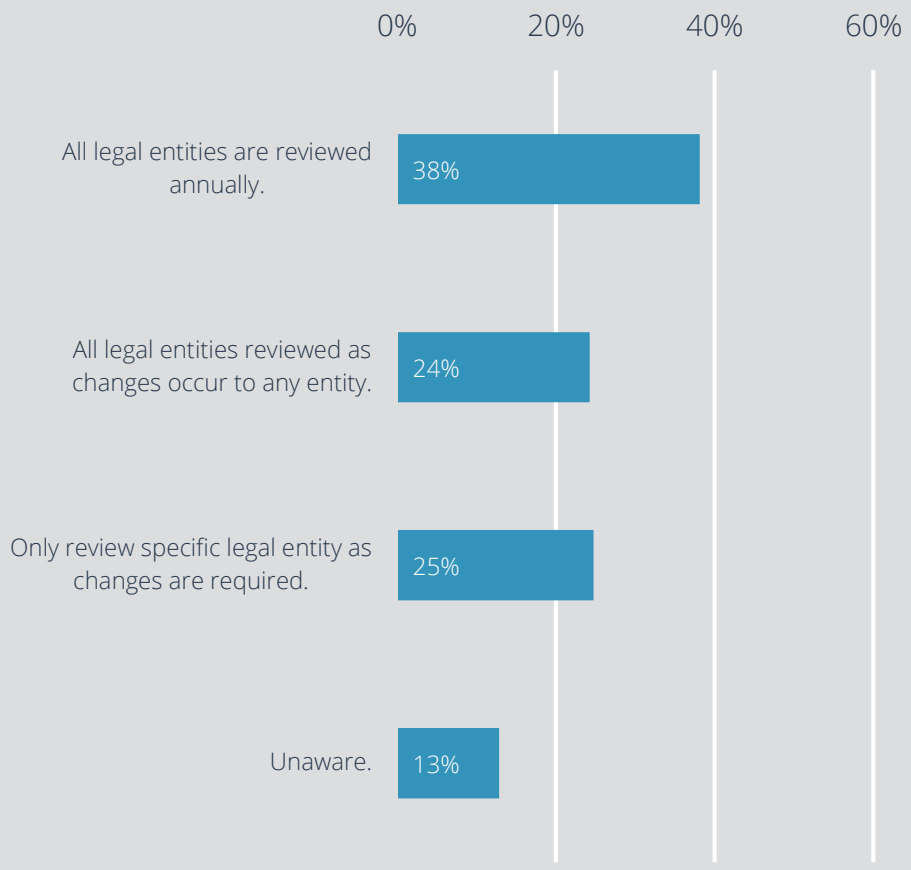
Probe of Involvement, Policy. Since the amount of focus on cyber threats has increased significantly in recent years, we sought to gauge the level of organizational involvement, including Treasury, in managing cyber threats in some different areas. Nearly all play some role (90%) in cyber risk management. Treasury is an influencer on cyber risk in 44% of firms. Only 59% have an internal data protection plan and 2% less (57%) have a plan of action in the event of a data breach. Less than half (46%) have a cyber risk data strategy. Given the threat level and the impact potential of those threats, it would be surprising not to see strong progress on these items over the next year.

Does your organization have formalized banking resolutions defining who has signatory authority and how many signatories must be represented to open and close bank accounts?



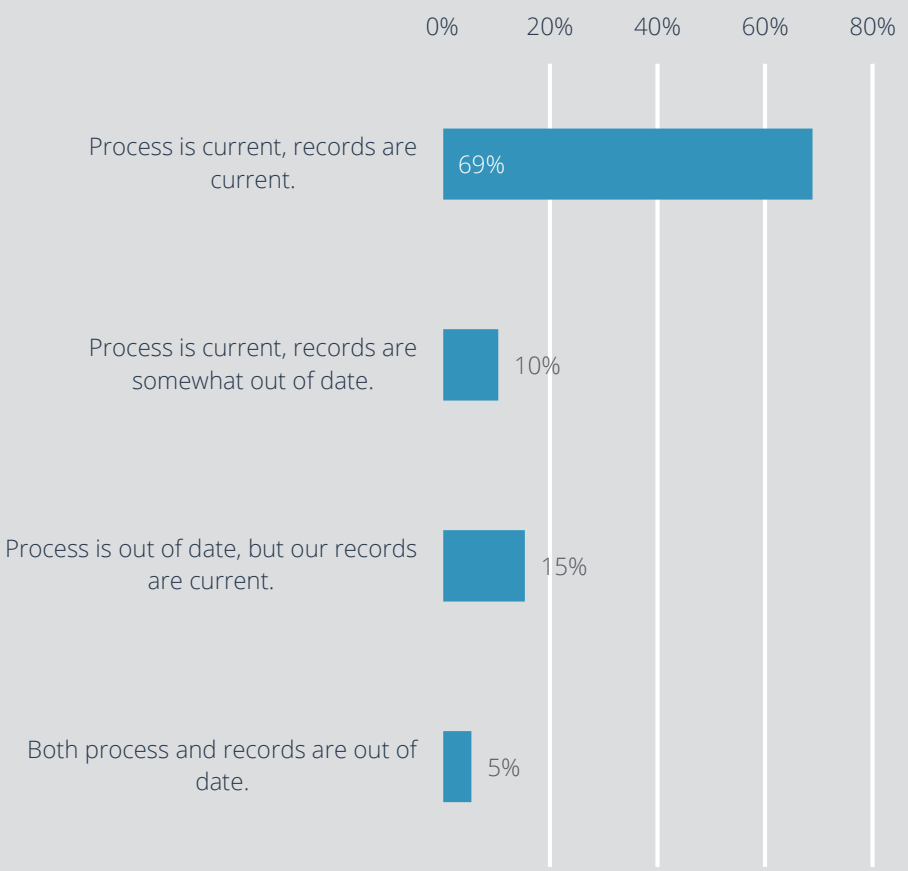
Formalized Banking Resolutions. This question is intended to capture the signer controls designated within the banking resolutions.

How often are your banking resolutions reviewed/updated?



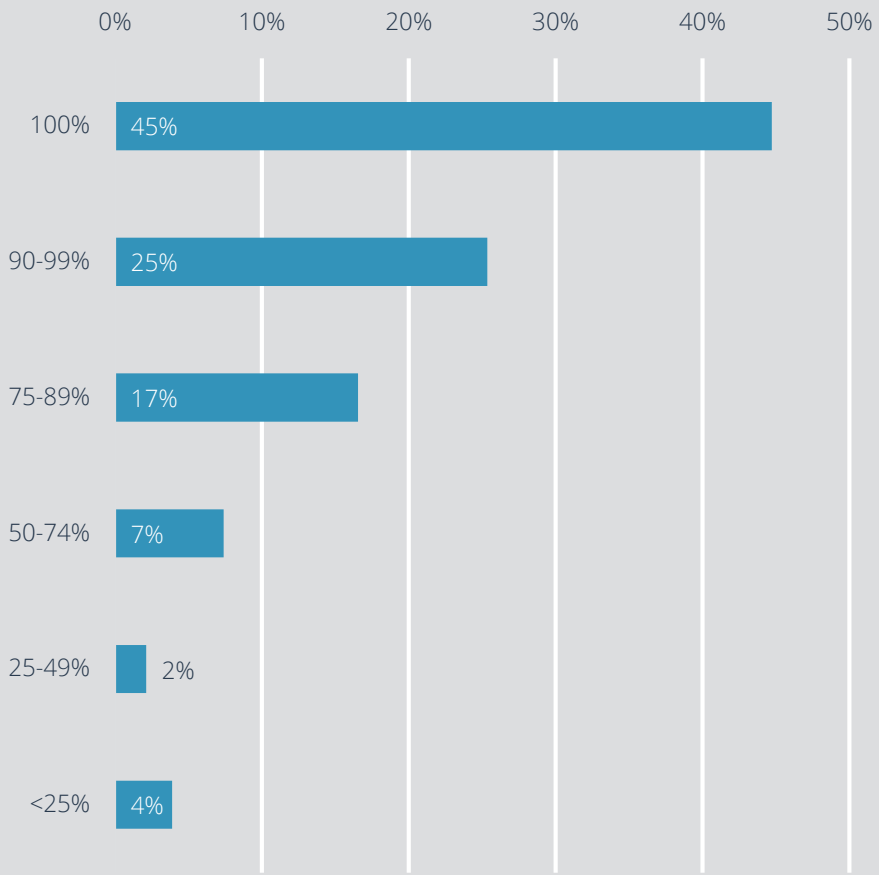
Banking Resolution Review. 38% of firms review their banking resolutions on a systematic and annual basis. 24% review all banking resolutions when changes occur to one legal entity. 25% will review all banking resolutions for that particular entity when there is a change. 13% were unaware of the process used for reviewing banking resolution data.

BAM Status. Our Bank Account Management process and records:



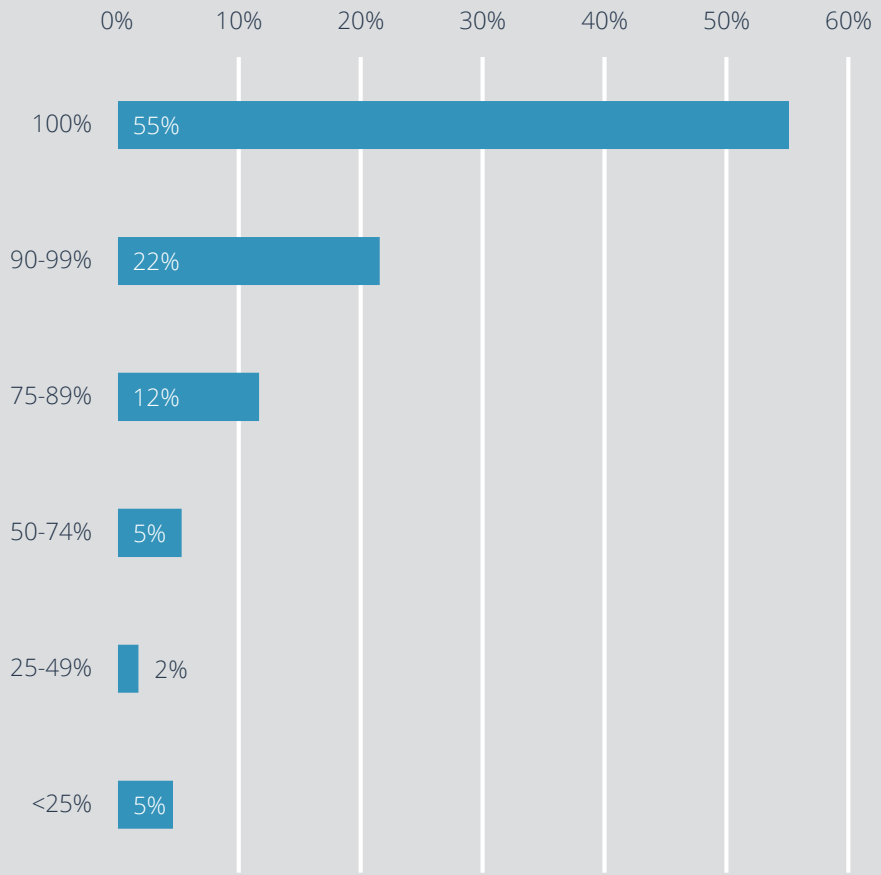
Bank Account Management (BAM). If each account and signer represents a point of cost and exposure to the organization, determining how well these records are maintained and how well the process is managed is important. Nearly 70% of firms felt that both processes and records are current. 15% of firms indicated that their records are out of date and 79% of firms say their BAM process is current.

What percentage of your bank accounts do you have visibility to on a DAILY basis (information reporting)?



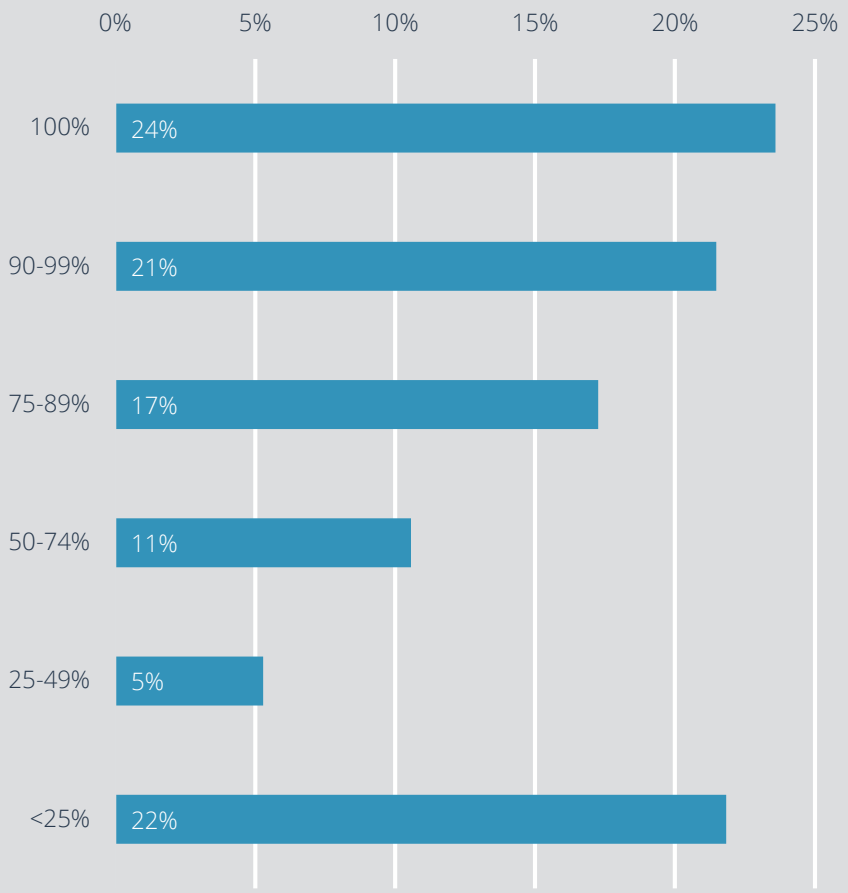
Visibility – Daily Basis. 45% have total visibility (100% of their bank accounts) daily. Another 25% have visibility to 90-99% of their accounts for a total of 70% of firms that can see 90-100% of their accounts on a daily basis. 13% of organizations see less than 75% of their accounts (6% see less than one half of their accounts on a daily basis). This question covers total accounts and not total value of cash flows. Most organizations prioritize their accounts for visibility based upon cash flow and overall impact.

What percentage of your accounts do you have visibility to on a WEEKLY or more frequent basis?



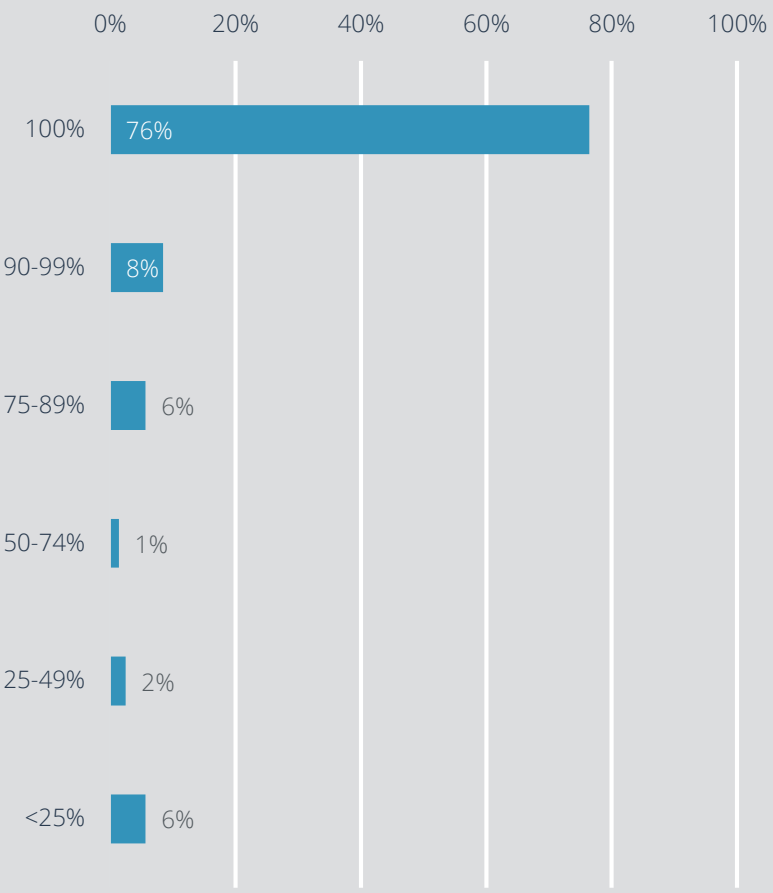
Visibility – Weekly Basis. 55% have total visibility (100% of their bank accounts) on a weekly basis (versus the 45% that have total visibility on a daily basis). 77% have weekly visibility to 90-100% of their accounts (77% vs 70% on a daily basis).

What percentage of your bank accounts are reconciled on a DAILY basis?



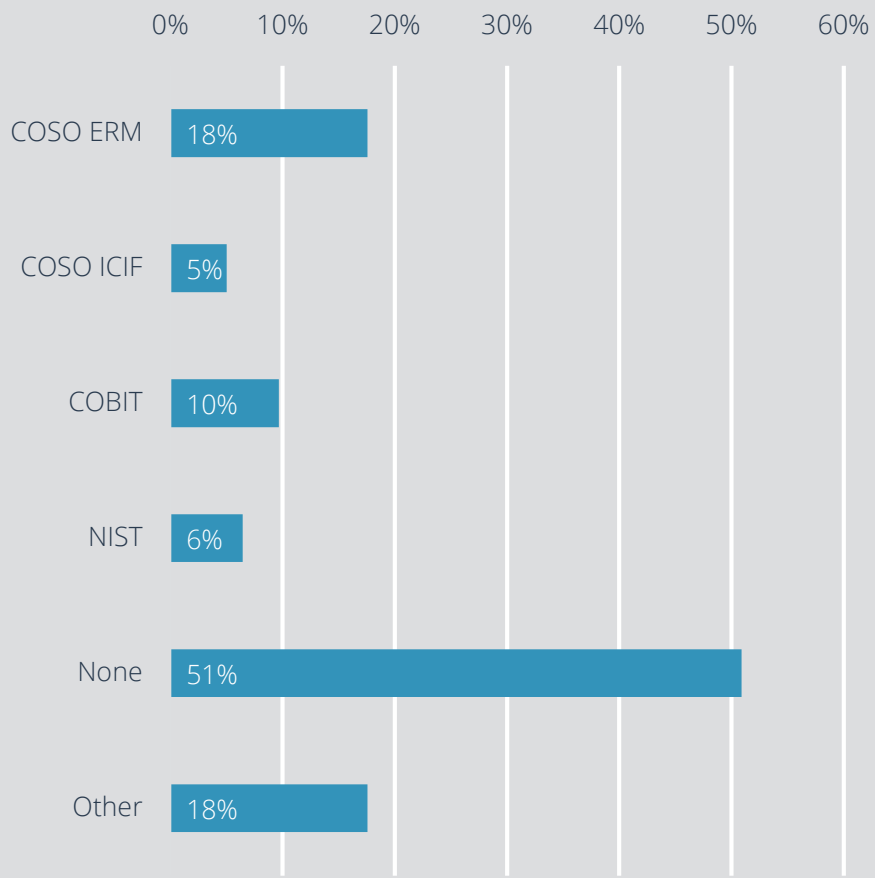
Bank Account Reconciliation – Daily. Almost 1/4th of respondents reconcile all bank accounts on a daily basis! And, a total of 45% of firms reconcile 90% or more of their bank accounts every day. Just 22% reconcile less than 25% of their accounts on a daily basis.

What percentage of your accounts are reconciled on a MONTHLY or more frequent basis?



Bank Account Reconciliation – Monthly. Just over 3/4ths of firms reconcile all bank accounts on a monthly basis. 84% of firms reconcile at least 90% of their accounts monthly.

Reconciliation. Reconciliation activities performed in our organization include (Check all that apply):



Reconciliation: Type & Description

Bank Reconciliation
The reconciliation, or comparison through resolution, of the bank statement activity to the cash books of the firm. AKA Bank-to-Book Reconciliation

GL Reconciliation
The reconciliation, or validation of the match, between the sub-ledger accounts and the control accounts on the general ledger.

Treasury Proof
The process of validating material differences between what was expected from the prior day's cash positioning activity with the reality of what was in the account at the start of the day.

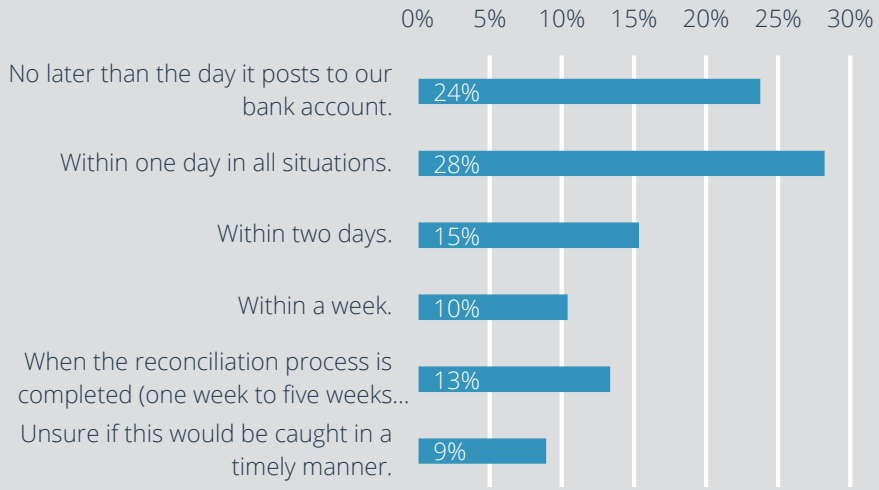
File Control
The reconciliation, or comparison, includes various processes that systematically confirms that there is file integrity. This can include various comparisons including:

1. total amounts match details;
2. nothing is missing within the file;
3. nothing is missing between the files;
4. the file is not altered.

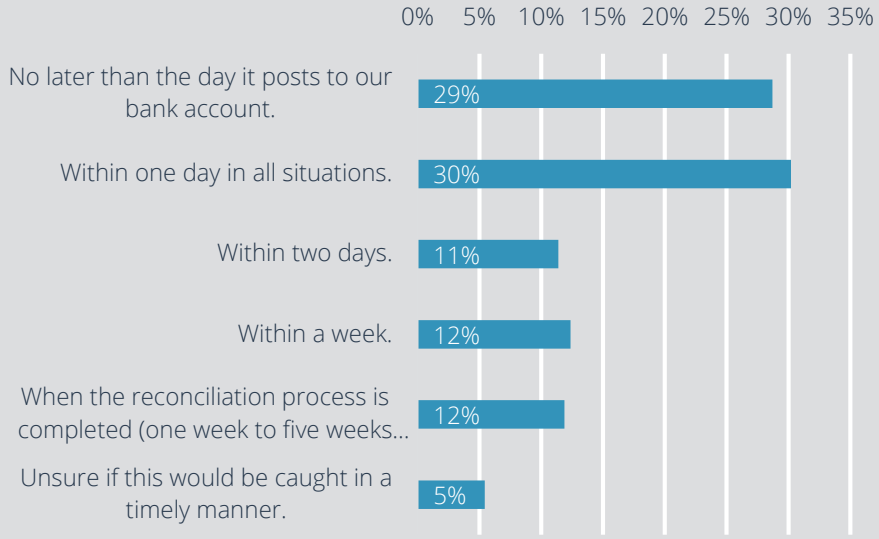
Reconciliation. Strategic Treasurer typically categorizes reconciliation activities into four groups or categories [see chart for an explanation]. We asked if the organization performs the following activities:

- Bank Reconciliation. 90% perform bank reconciliation. Our expectation was that 95-98% of firms complete bank reconciliation despite the near universal agreement that matching the bank records to the cashbook records is a requirement.
- GL Reconciliation. Nearly 3/4ths (72%) of firms perform the matching of sub-ledger records to the control accounts on the general ledger.
- Treasury Proof. Just over half (56%) of organizations are performing a validation of significant differences in the cash position.
- File Control. File control includes various systematic processes that ensure a file maintains base integrity (the totals match the details, nothing has been lost) and that no one has altered the file.

How quickly will you detect and/or prevent a small value amount of ACH and Check Conversion Fraud (i.e. under $1K)?



How quickly will you detect and/or prevent a moderate value amount of ACH and Check Conversion Fraud (i.e. between $1K-$5K)?



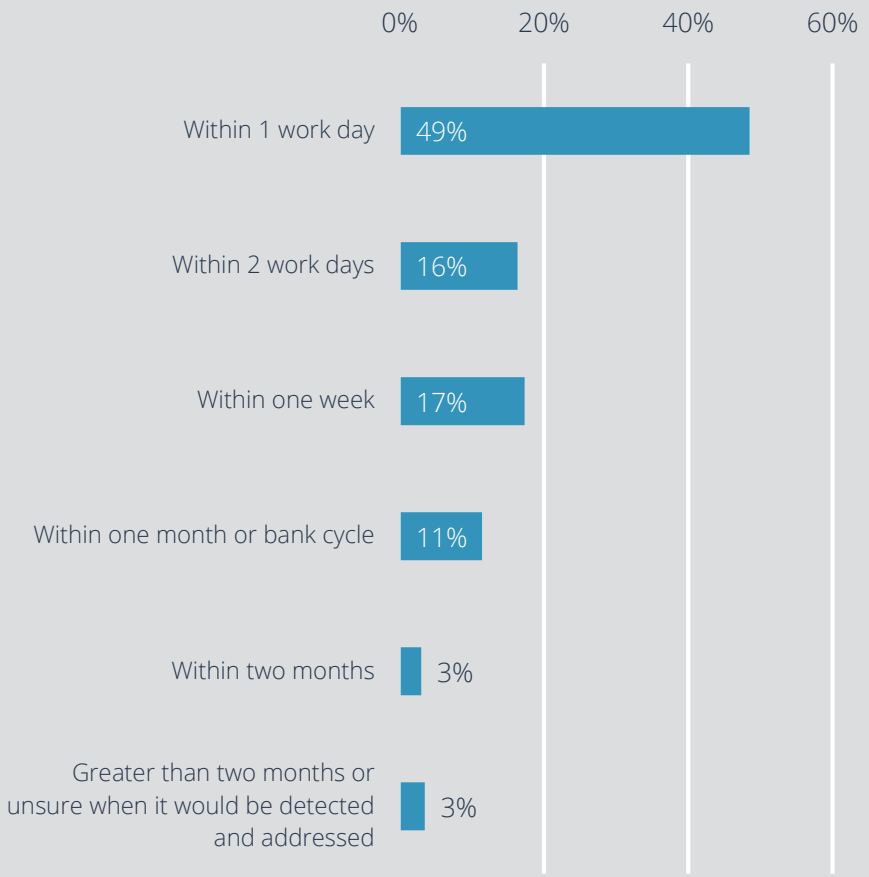
Speed of Fraud Detection (ACH/Check | Small Value). We asked a series of questions to determine the speed of detection or prevention for various fraud types and amounts. In this case, we asked about ACH and Check Conversion Fraud for smaller amounts (under $1,000 USD or equivalent).

a. Immediate. No later than the day it posts to our bank account is 24%, which is a very strong showing for a small dollar amount. This demonstrates that daily-automated reconciliations help detect fraud quickly and allows organizations to have the greatest opportunity to return those items.
b. Rapid. Within one day in all situations is 28%. Between Rapid and Immediate, over half (52%) of firms have very good fraud detection for these types of transactions.
c. When the Reconciliation Process is completed is 13%. Since this can be one to five weeks from the actual event, this indicates strong exposure to the slower control processes for a significant portion of organizations.
d. 9% are Unsure. This represents significant exposure to check fraud due to the level of controls they have. Combining this with 'when the reconciliation process is completed' we reach 22% (more than 1/4th of firms) for slow identification of fraudulent items.

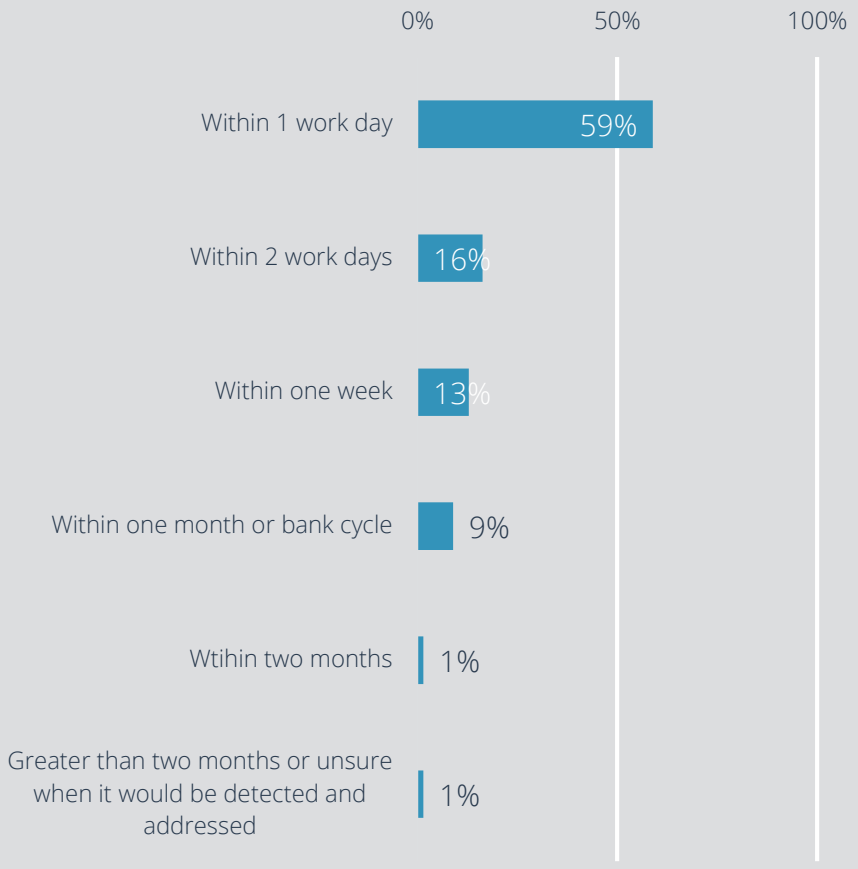
Speed of Fraud Detection (ACH/Check | Moderate Value). In this case we asked about ACH and Check Conversion Fraud for moderate amounts (between $1,000 and $5,000 USD or equivalent).

a. Immediate. 29% report that it is no later than the day it posts to their bank account. This yielded an additional 5% over the small value items (vs. 24%). We surmise that the increase in detection speed is due to the increased dollar value and a review process that would include automated prioritization or identification that has a heightened priority.
b. Rapid. Within one day in all situations is 30%. Slight increase over the small fraud amounts. For moderate amounts for both the Rapid and Immediate periods, respondents now total 59%.
c. When the Reconciliation Process is completed is 12%. Since this can be one to five weeks from the actual event, this indicates strong exposure to the slower control processes for a significant portion of organizations.
d. 5% are Unsure. While this represents a significant exposure to check fraud due to the level of controls they have, the number of organizations that were unsure dropped from 9% to 5% for small to moderate amounts. Combining this with 'when the reconciliation process is completed' we total 17% (about 1/6th of firms) for slow identification of fraudulent items.

How quickly would you detect and address an ACH, wire or check fraud <$1,000?



How quickly would you detect and address an ACH, wire or check fraud between $10K and $100K?

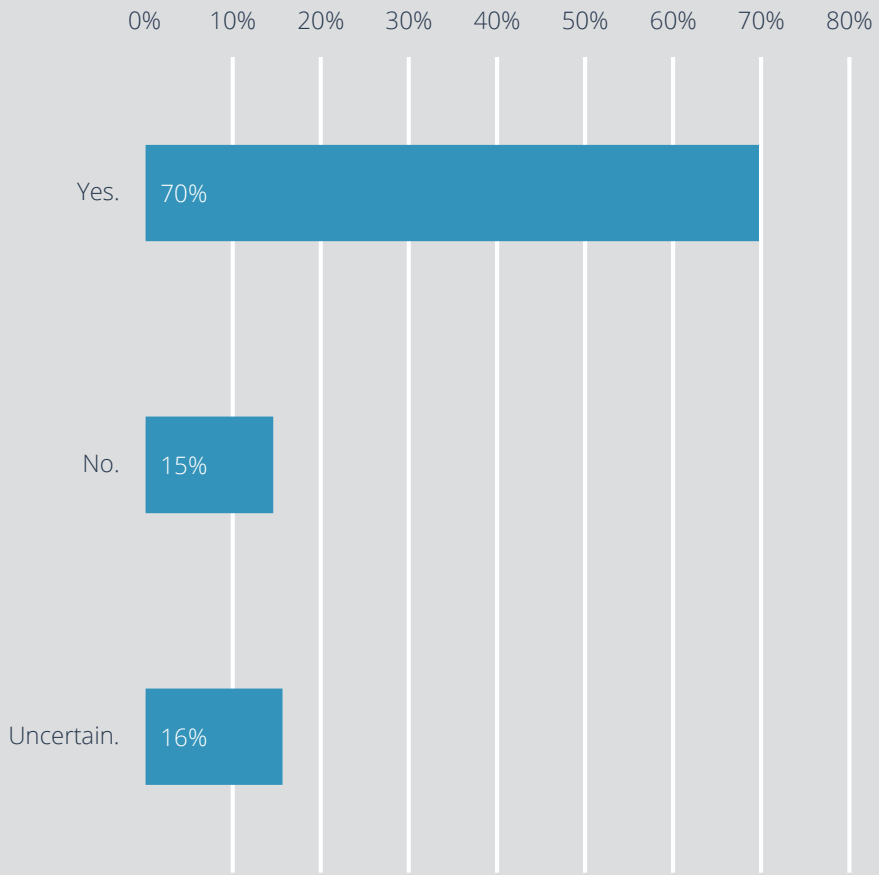


Speed of Fraud Detection: ACH, Wire, Check Fraud (Small <$1,000). This question grouped three common payment types to determine how quickly fraud would be detected. This is the first part (small payment amount) of three related questions.

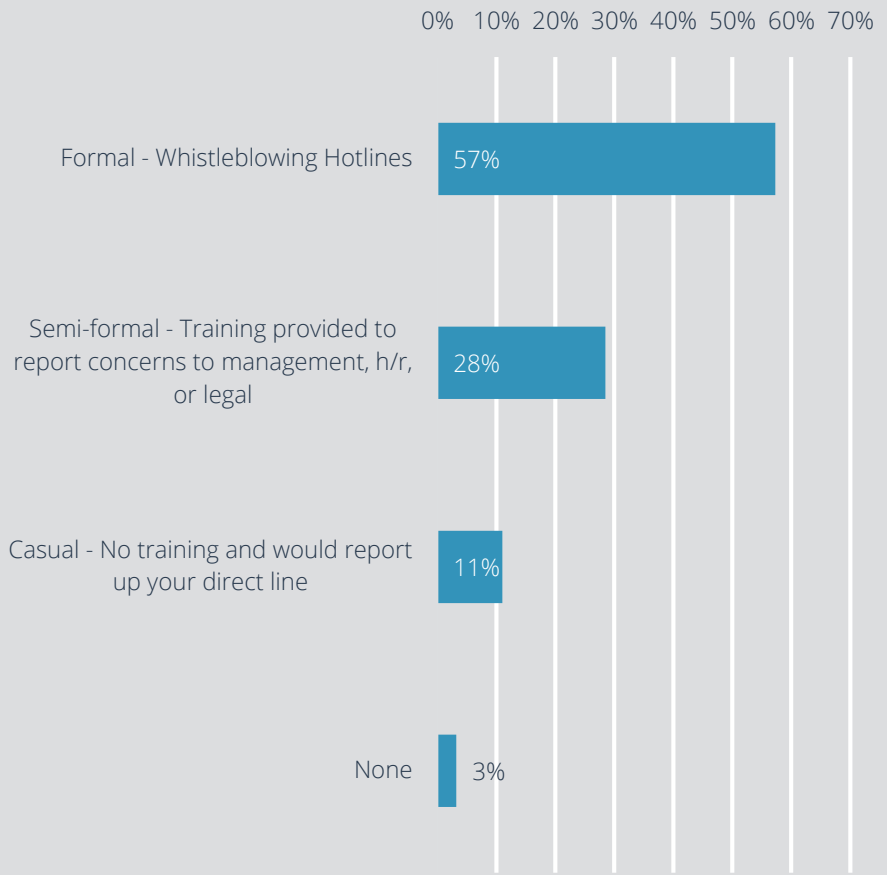
Speed of Fraud Detection: ACH, Wire, Check Fraud (Large $10,000 to $100,000). This is the 3rd question of three that makes a distinction based upon size of the payment. This is the larger sized payment option. We did not ask for extremely large payments as we expect that nearly all firms would catch those items very quickly since they would impact cash positioning.

- Within one work day is 59%. For the same items under $1,000 it was 49%. More than one tenth of firms would detect this larger amount at this size versus under $1,000. There is a 7% spread between this amount and medium sized amounts (52% of firms would detect the medium sized items within one day).

Does your organization have a policy for Anti-bribery/Anti-corruption (ABAC)?

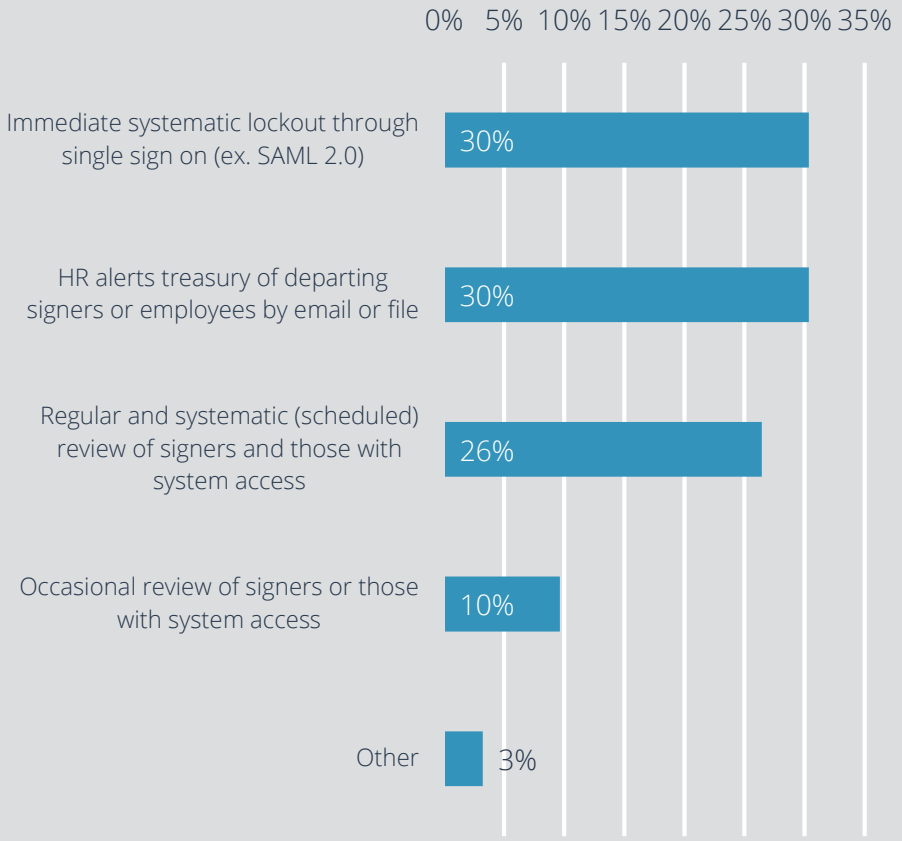


Which best describes your organization's process for reporting fraud, bribery or compliance?



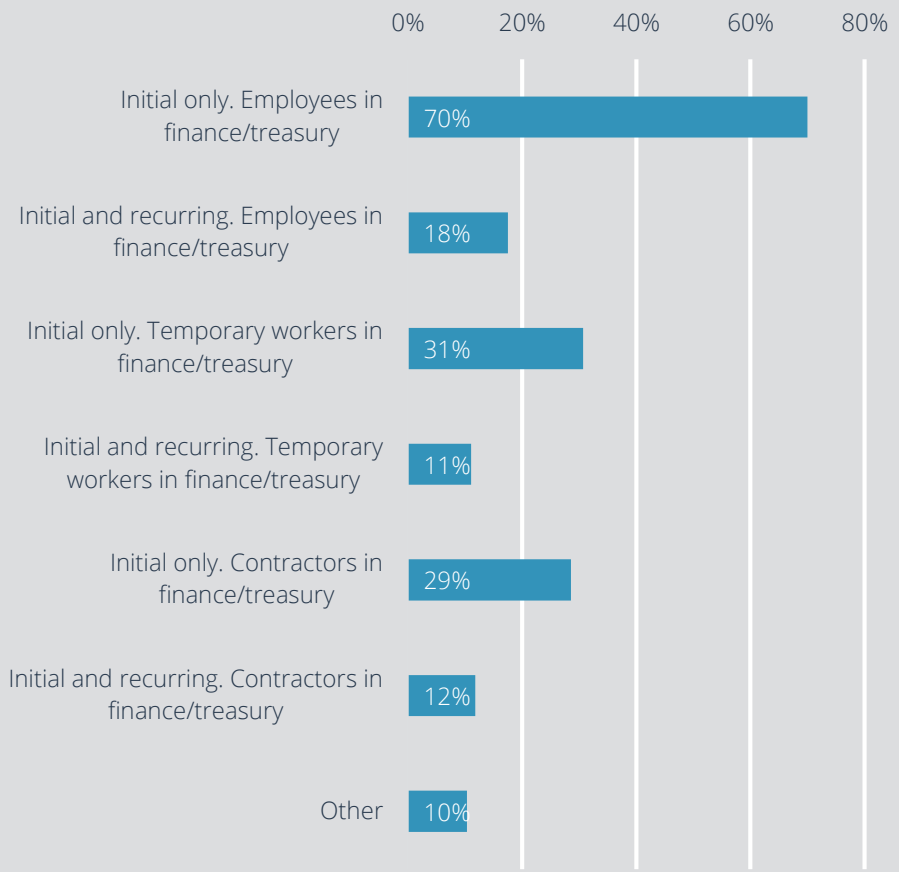
Fraud Reporting Process. 85% of firms have a formal (whistle-blowing hotline) or semi-formal (general training) process for reporting fraud.

Access Control. If someone leaves the organization then system access is removed from treasury/banking systems by:



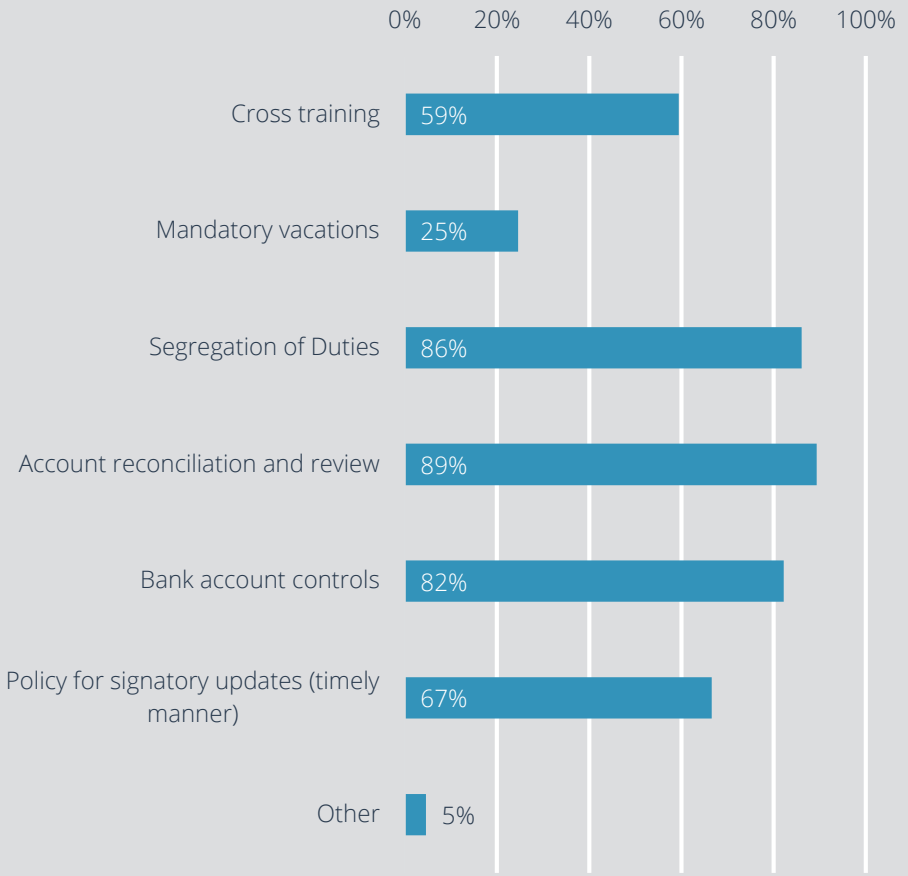
Access Control. An organization must remove the system access of employees who leave their organization quickly and completely. This is clearly not the case for the vast majority of companies currently.

Staff / Personnel. We perform background checks (Initial & Recurring) on: (Check all that apply)

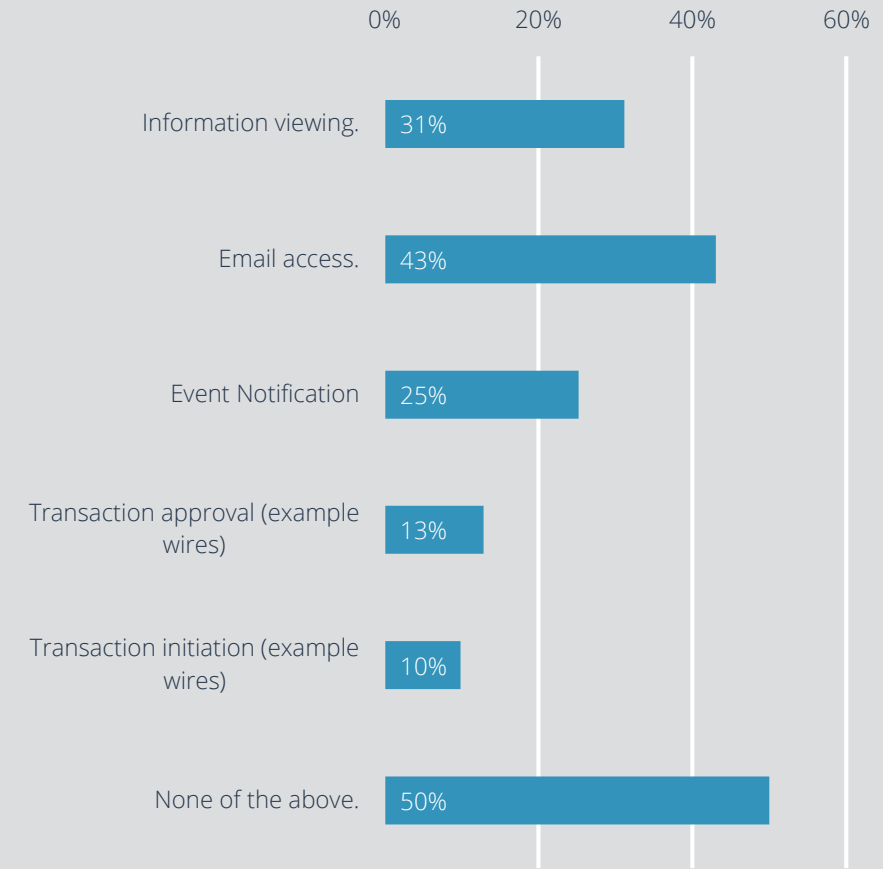


Staff & Personnel. What may cause you to scratch your head is the surprising common practice that organizations are far more likely to perform background checks on full-time employees than temporary employees in finance (70% versus 31%).

What controls do you have in place to prevent employee fraud? (Check all that apply)



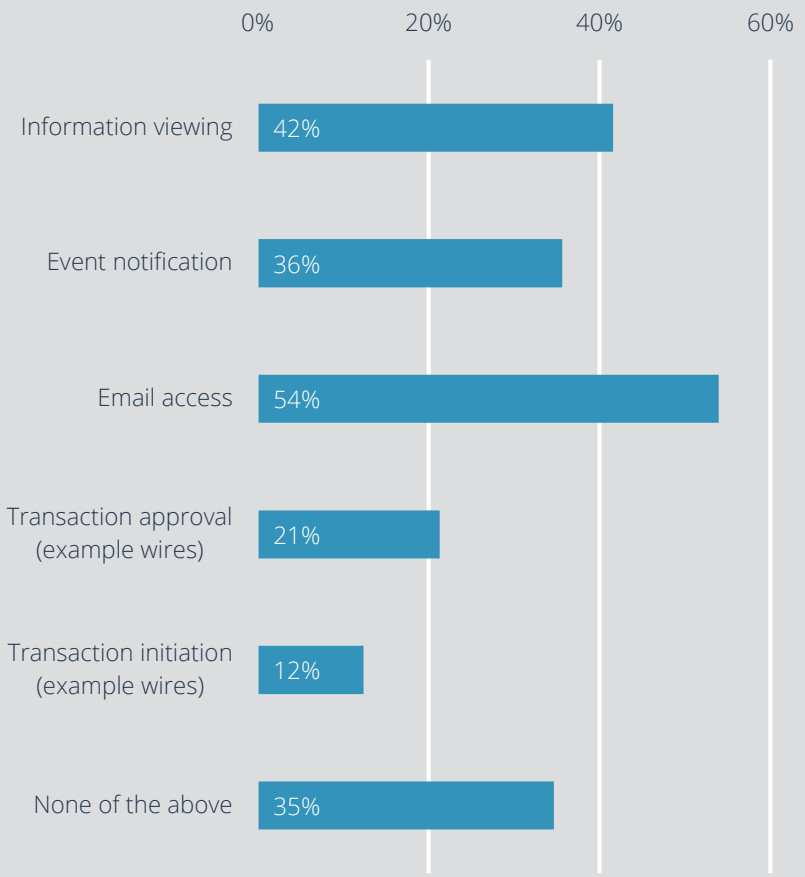
Bring Your Own Device. Our company allows treasury to do this for (Check all that apply):



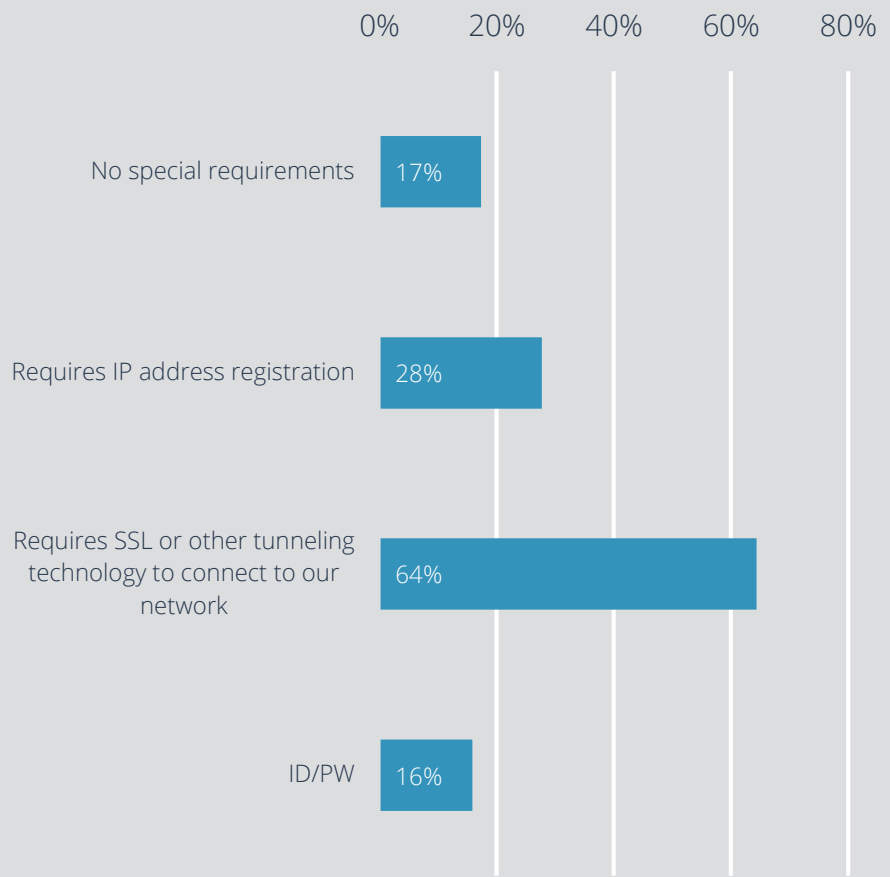
Employee Fraud – Prevention Steps. The top three prevention steps to combat employee fraud are: Account Reconciliation and Review 89%; Segregation of duties 86%; Bank Account Controls 82%. At the bottom was mandatory vacations required by 1/4th of the survey respondents.

Bring Your Own Device (BYOD). The increasing corporate acceptance of personal devices raises questions of security and acceptance. Our concern focuses primarily on Treasury use. A related question has to do with mobile device use and acceptance. Approving an already entered transaction is accepted by 13%. Only 10% firms allow transactions to be initiated on devices that were not corporate owned. Given differing levels of antivirus protection and firewalls, it is not surprising that the vast majority of firms do not allow this type of connection.

Mobile. Our company allows treasury to do this for (Check all that apply):



Remote access by computer (besides email) for treasury (Check all that apply):

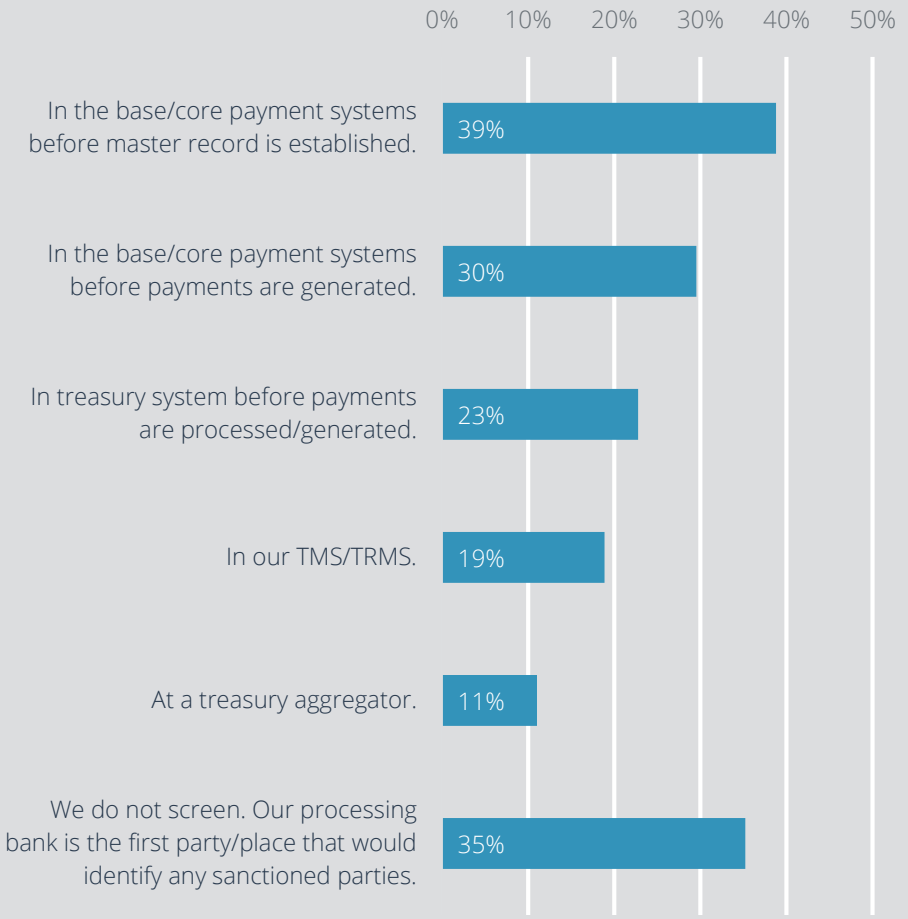


Mobile. This is a "check all that apply" question.

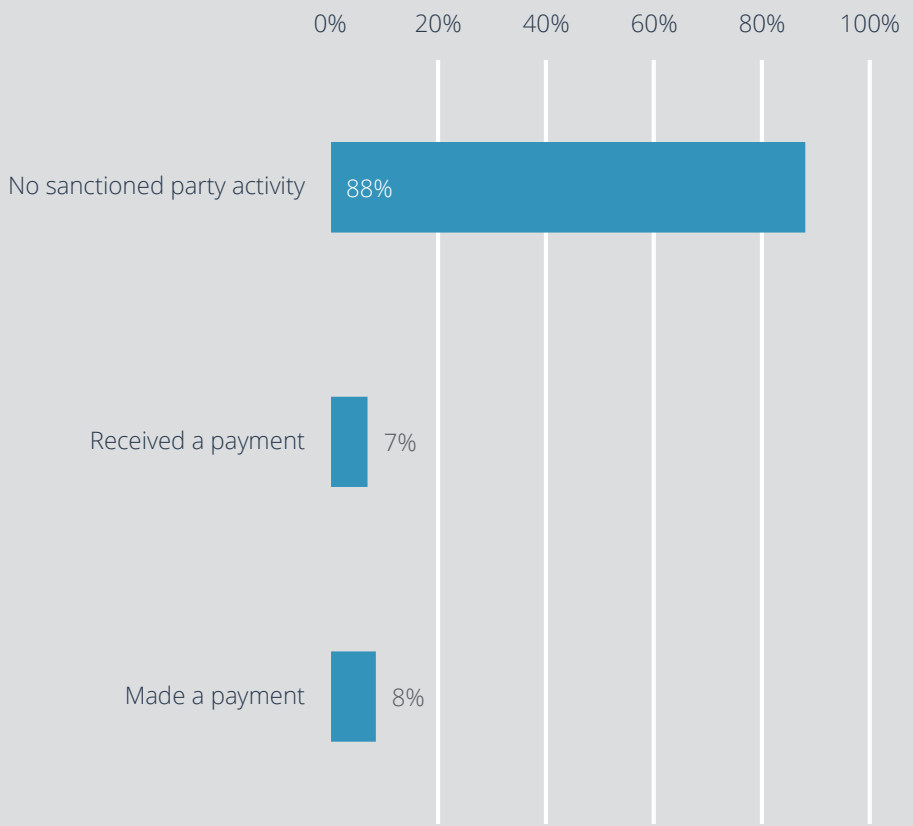
- Transaction Approval is 21%, which is an 8% increase over the BYOD response (13%) for approving transactions that are already entered.
- Transaction Initiation is 12%, which is only a 2% increase over BYOD (10%). This demonstrates strong reluctance to allow mobile for transaction initiation. Increasing corporate acceptance of personal devices raises crucial questions of security.

Remote Access by Computer (besides email) for Treasury. Simply put, we wanted to understand what the market was doing to control, or not control, access to corporate data.

We screen for sanctioned parties (Check all that apply):



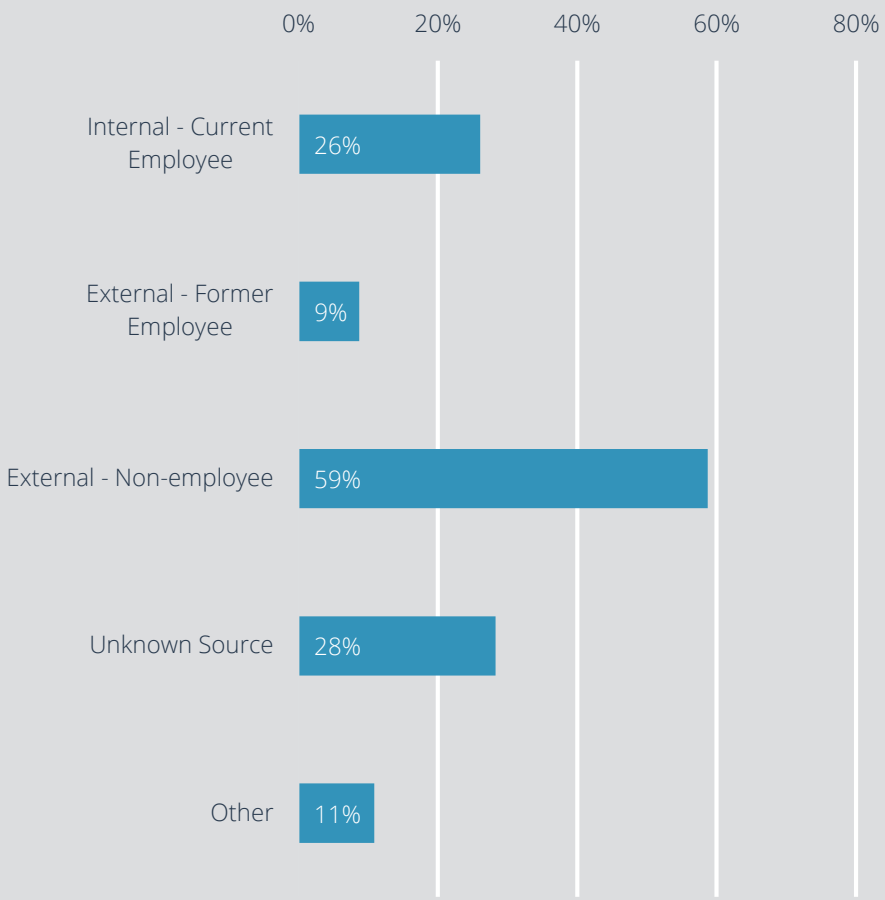
Have you inadvertently made a payment to or received a payment from a sanctioned party in the past 12 months? (Check all that apply)



Sanctioned Party Screening. 35% of respondents do not screen for sanctioned parties at any time. This lack of screening is surprising given the penalties and requirements. This is a significant company risk and area of exposure. Only 30% screen before payments are made. This leaves a gap in coverage as a counterparty can become sanctioned after they are established on the organization's system. Given the requirements that organizations may not rely solely on their bank for sanction screening, we expect significant compliance work and action over the next few years.

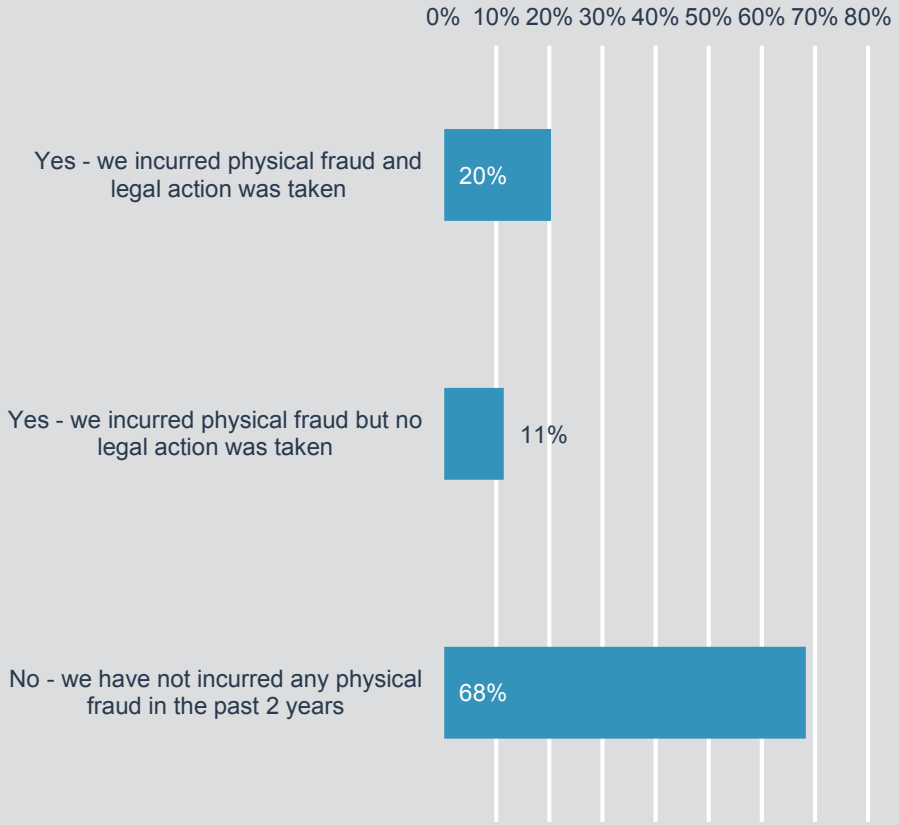
Sanctioned Parties – Past year. The issue of managing the payment and collection process so that your organization does not deal with various sanctioned parties (criminal enterprises, terrorist sponsoring organizations, etc.) continues to grow in importance and expectations. Regulations are pushing more organizations to have controls in place and they may no longer rely on the bank's screening process. Once a sanctioned payment has hit the banking system, it becomes a reportable event. We asked about receipts and disbursements. This question was a select all that apply so we could capture those organizations that had experienced both types of activity.

From which party did you experience fraud? (Check all that apply)



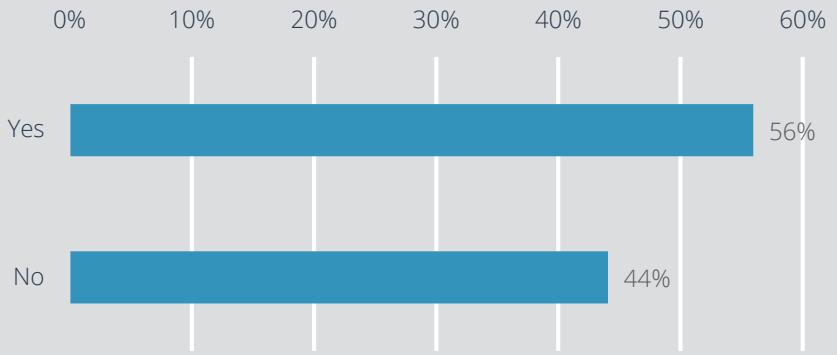
Fraud Source. Of the 40% of firms that experienced fraud we wanted to find the amount of fraud that originated internally and externally, if known. Multiple answers are permitted since an organization could have experienced more than one fraud attempt or loss in a year. And, the fraud cases may have originated from different sources. The order of frequency of parties that caused the fraud went from a high of 59% for an external non-employee, down to 9% for an external former employee. In just over 1/4th of the organizations, there was an experience with fraud where the source was unable to be determined.

Has your organization experienced any type of physical fraud in the past two years and was legal prosecution initiated?

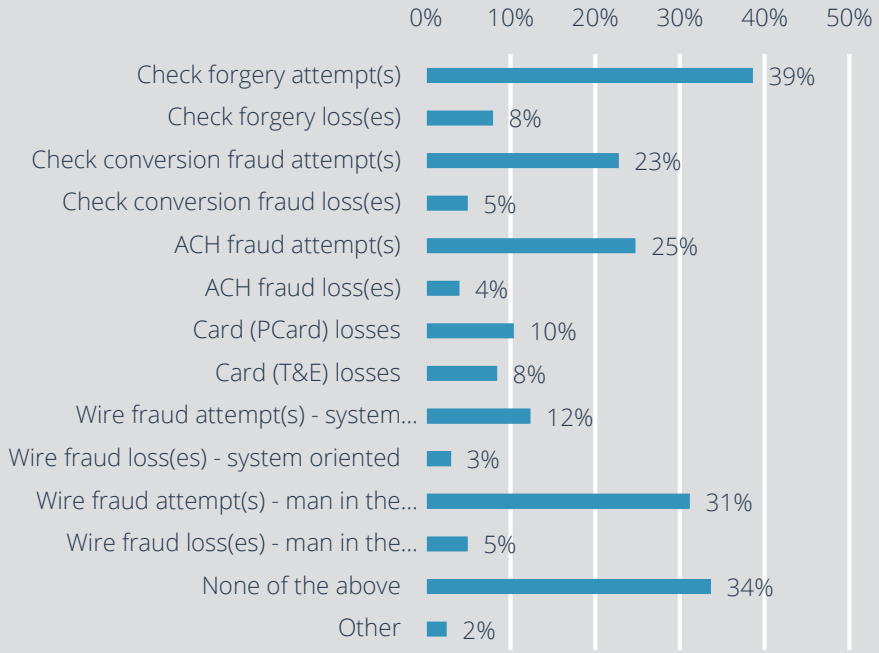


Physical Fraud. We wanted to see the frequency of physical fraud and determine how aggressive organizations were in going after the criminals.

Has your company experienced any payment fraud attempts in the last 12 months?



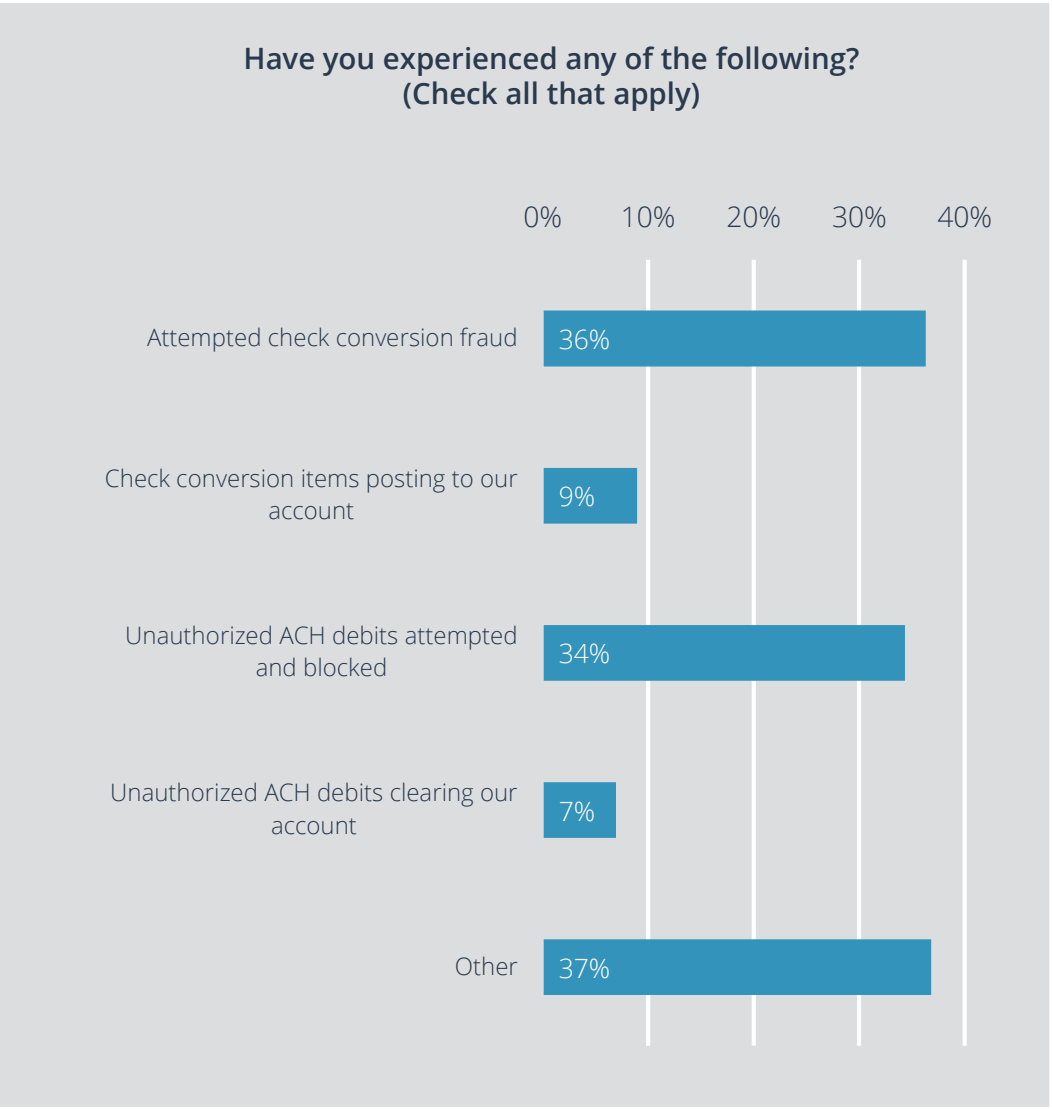
Have you experienced any of the following in the past 2 years? (Check all that apply)



Fraud Experience in the Past Two Years.

1. **Most Frequent Attempts:**
   - Check Forgery was 39%. The susceptibility of paper, due to the low entry point for fraud, maintains the top attempted fraud.
   - Wire Fraud – Man in the Middle was 31% and Wire Fraud – System oriented was 12%. These two responses capture the social engineering and technology/hack approaches to committing crimes that result in financial losses via wire transfer.
   - ACH Fraud reported was 25%. Despite the traditional safety of the low value payment networks due to the controlled access put in place by banks and the networks, criminals are still working to get these payments through.
   - Check Conversion Fraud was 23%. Converting checks to electronic items seems to provide the ideal blend of the openness of the paper/check world with the speed of the digital realm.

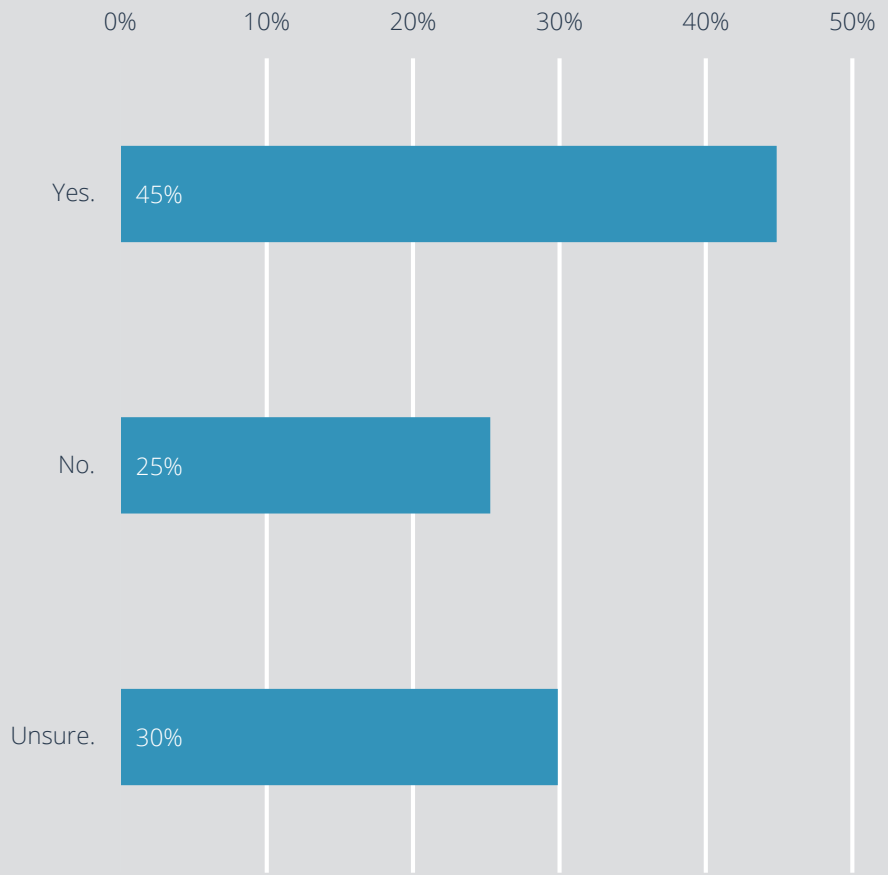
2. **Highest Percentage of Losses vs. Attempts:** We thought those curious about fraud frequency would also like to know the actual loss to attempt ratio. This is a fraud efficiency calculation.
   - Wire Fraud – System Oriented (24%). Almost 1 out of 4 attempts at wire fraud from a system attack/attempt were successful. While only 12% of firms had wire fraud-system attacks, almost one quarter were successful.
   - Check Conversion (22%). More than 1/5th of these attempts were successful. What is most surprising about this is that there are services offered by banks to stop this type of attack from being successful.
   - Check Forger (21%). This old school fraud approach does not show signs of stopping anytime soon, especially with this success rate.



ACH Fraud - Have you experienced any of the following (no time limit specified). We wanted to dive more deeply into the area of ACH and Check Conversion and asked this question that had five different response options (all that apply).

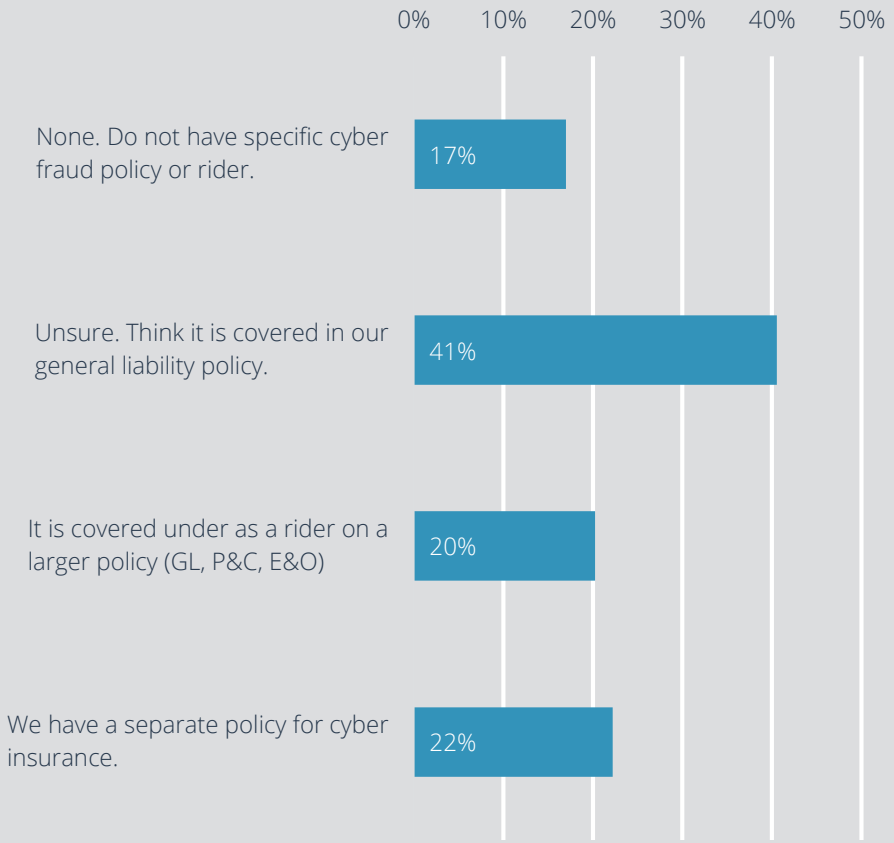
- Attempted Check Conversion Fraud affected over 1/3rd (36%) of the respondents! 9% reported checks clearing which represents an almost 25% fraud success rate.
- Unauthorized ACH Debits attempted was reported by over 1/3rd (34%) of the audience. 7% cleared representing over a 20% fraud success rate.

Insurance on cyber fraud. We protect our losses against cyber fraud with cyber fraud insurance.



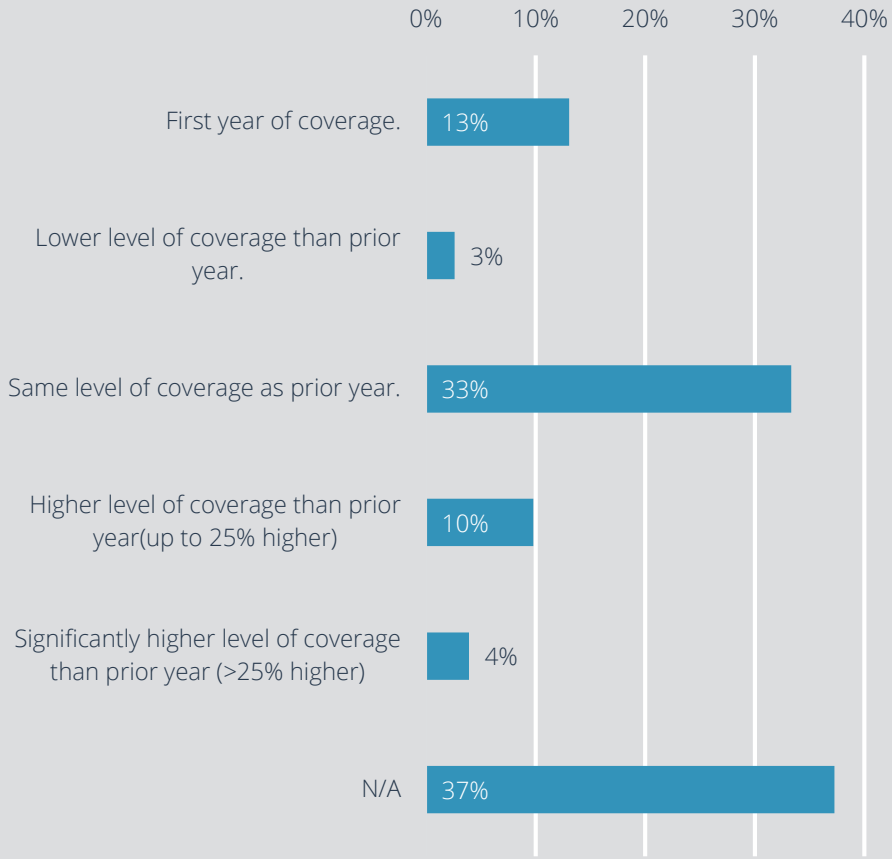
Insurance on Cyber Fraud. 30% were unsure if their organization carried cyber fraud insurance. Of those that knew the status, the covered outnumbered the uncovered by a 9 to 5 ratio.

What type of cyber fraud insurance policy do you carry?



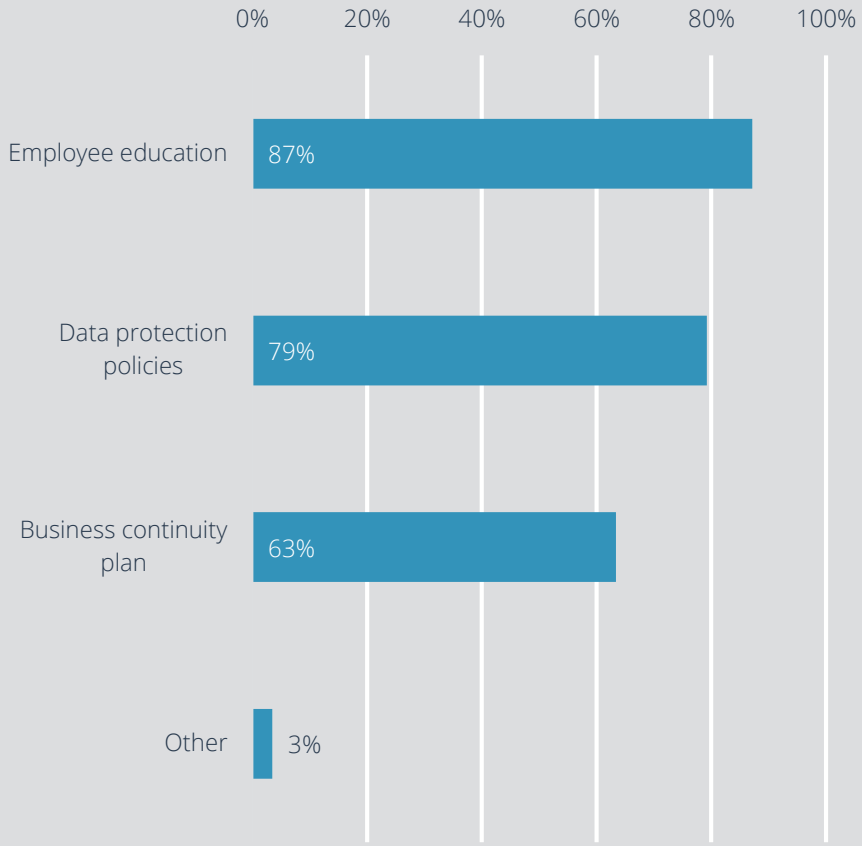
Type of Cyber Fraud. More than four out of 10 (41%) of respondents were unsure of the type of cyber fraud insurance they were carrying. Others indicated that they were covered under a policy rider (20%) or a specific cyber fraud policy (22%).

If you have cyber fraud insurance, how long and what level of coverage do you have?



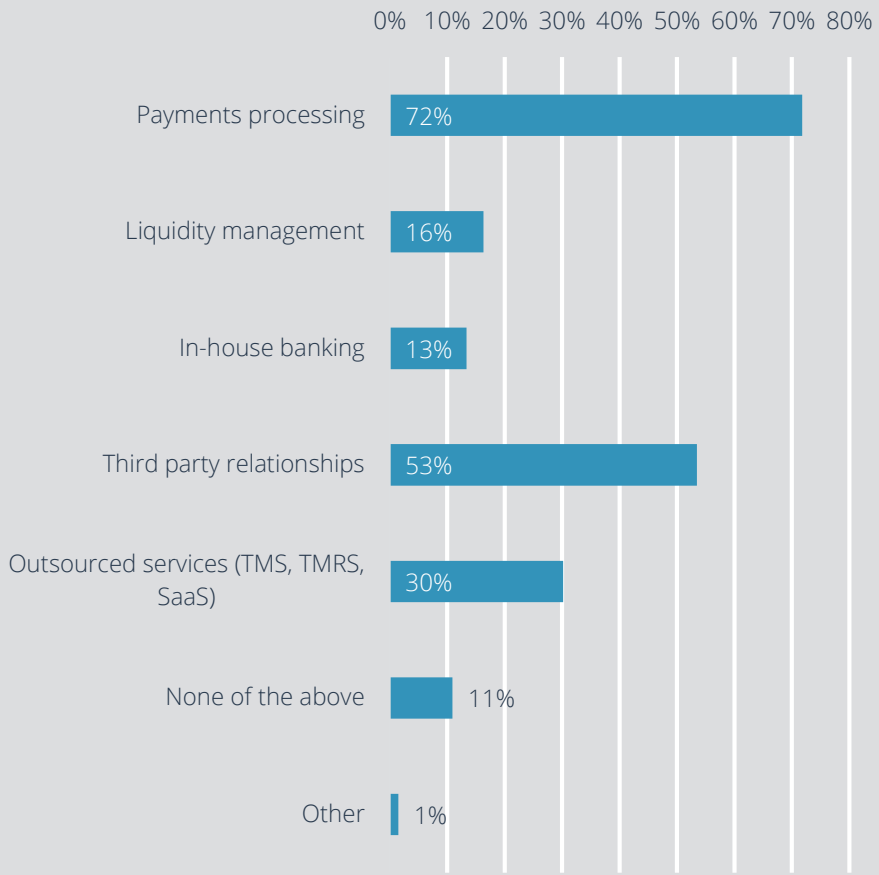
Level of Cyber fraud Insurance Coverage. We wanted to gauge if the level of cyber fraud insurance coverage was increasing, staying the same, or pulling back. 33% of firms had the same level of coverage as the prior year. When we look at decreased coverage, we only see 3%. To determine an increase of coverage we added up a number of items which showed over a quarter (27%) of firms increasing their coverage over the prior year (first year 13%, higher coverage 10%, significantly higher coverage 4%). Thus, the trend to add and increase coverage continues in full force.

What controls do you have in place to prevent cyber fraud? (Check all that apply)



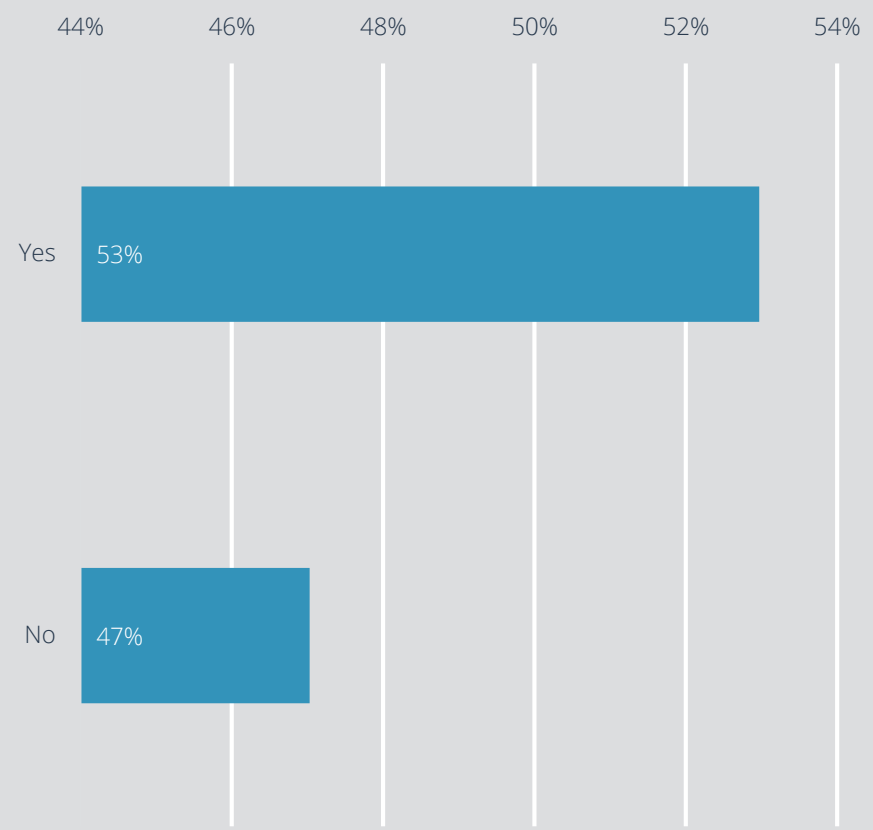
Cyber Fraud Controls. Employee education topped the list followed closely by data protection policies. Since many successful cyber fraud attacks come by way of social engineering, employee education flows logically.

Which of the following pose cyber threat risks to your organization? (Check all that apply)



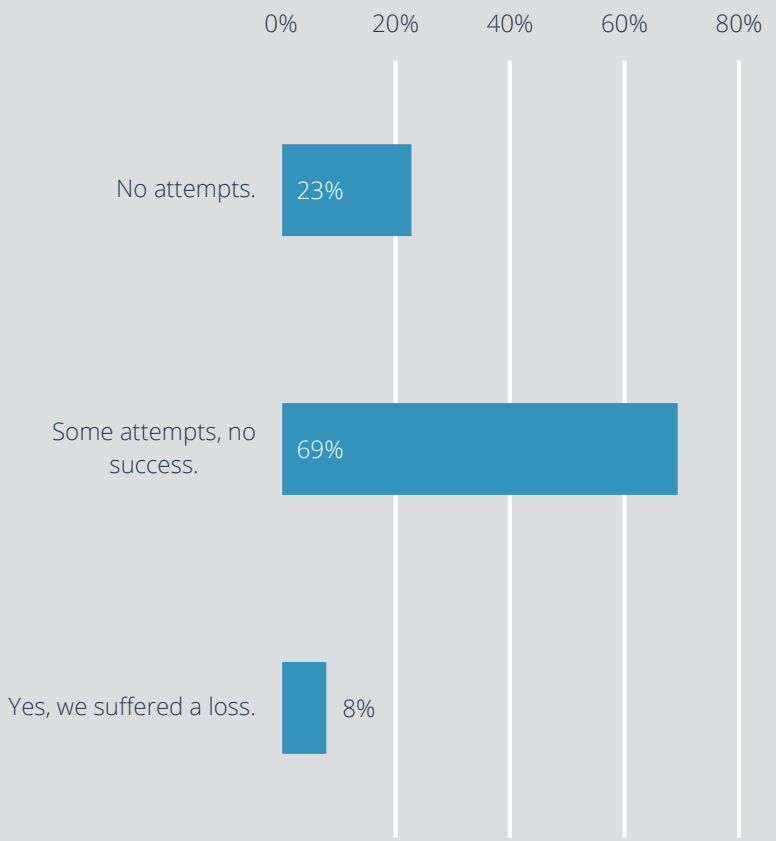
Cyber Risks. Which of the following pose cyber risks to your organization? Respondents can select any and all answers that apply to their situation. Accessing funds (72% - payment processing) was the breakaway leader. Third-party relationships (53%) came in second and we suspect it was due to the general awareness of a major cyber attack that happened when a 3rd party entity was given access to an HVAC system and through that channel attacked more valuable cyber assets.

Has your company experienced any cyber fraud attempts in the last 12 months?



Cyber Fraud Attempts. More than half of the survey respondents were exposed to attempted cyber fraud.

Has your organization experienced any type of impostor fraud/man in the email attempts or otherwise in the past two years?



Man-in-the-Email Fraud Attempts – 2 years. Imposter fraud is not always classified as cyber fraud, thought it often seems to include email account monitoring or access. We have included this question within the cyber fraud section for that reason. There are several types of names that are used for this type of fraud such as Imposter Fraud or Man-in-the-Email.

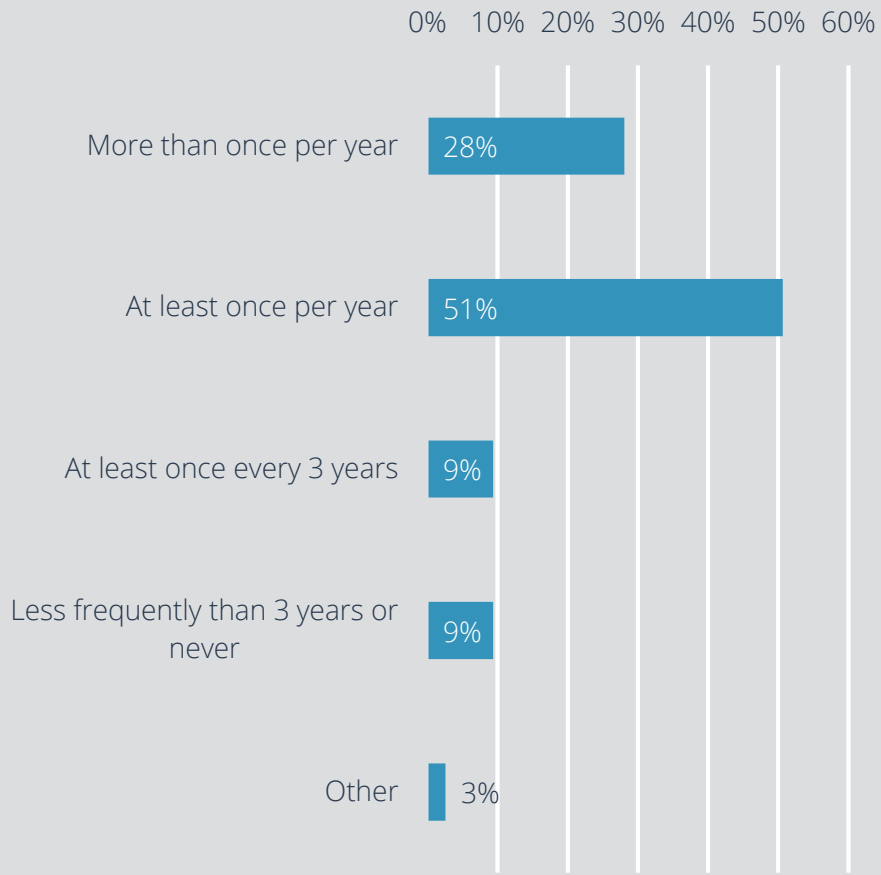
1. The method of fraud is perpetrated by the criminals in this general pattern: Secure access to email traffic of a senior executive, or a lower level manager who receives emails from top executives.
2. Understand their communication style and who makes things happen.
3. Secure a domain name that is extremely similar to the target.
4. Send an urgent and super-confidential email to the person who can wire funds and explain the secretive nature of the transaction and why no one else should be involved.
5. Do this when the executive is out of the office (determined by email traffic).
6. Push hard for the release of funds indicating that time is of the essence.

The sheer number of attempts of this sort is a bit astounding. The extent of these attempts helps us understand better why Wells Fargo, PNC and others have been making numerous presentations warning treasury professionals of these types of fraud.

The results were as follows:

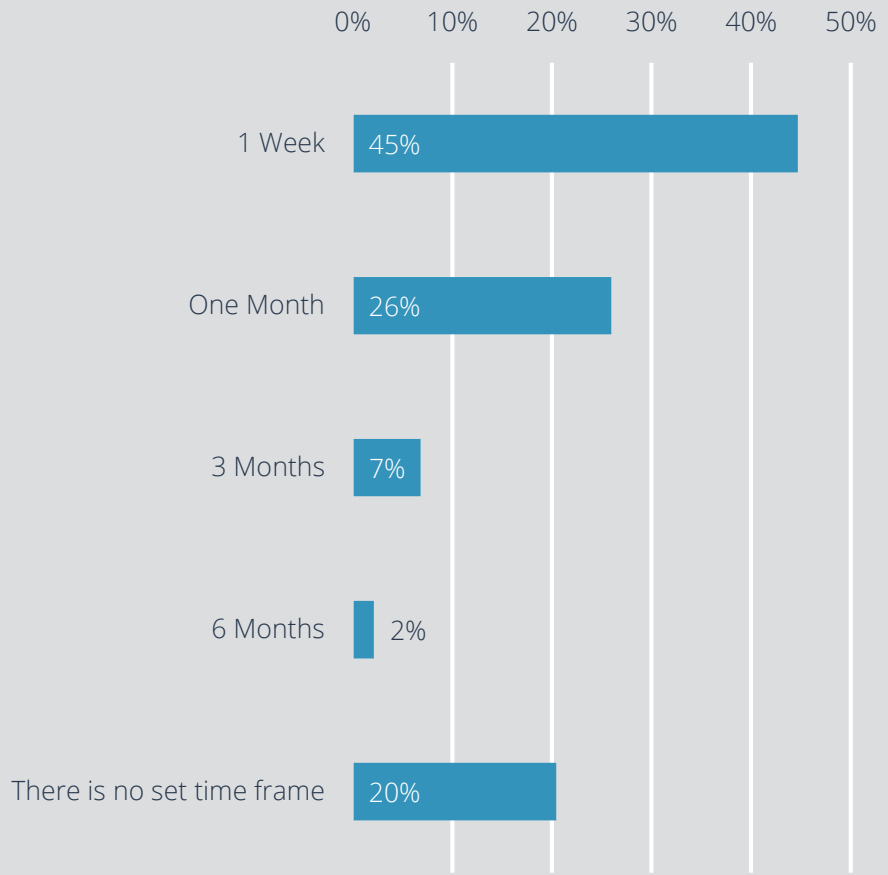
- Some Attempts, No Success (69%). This could be under reported if the attempt has occurred and this person is not informed of the situation.
- Attempts, Suffered a Loss (8%). The payoff for the criminals was real for an amazing number of companies. In most circumstances, the 'social engineering' caused people to violate their organizational control requirements.

How frequently do you audit your bank's authorized signer records for your accounts?



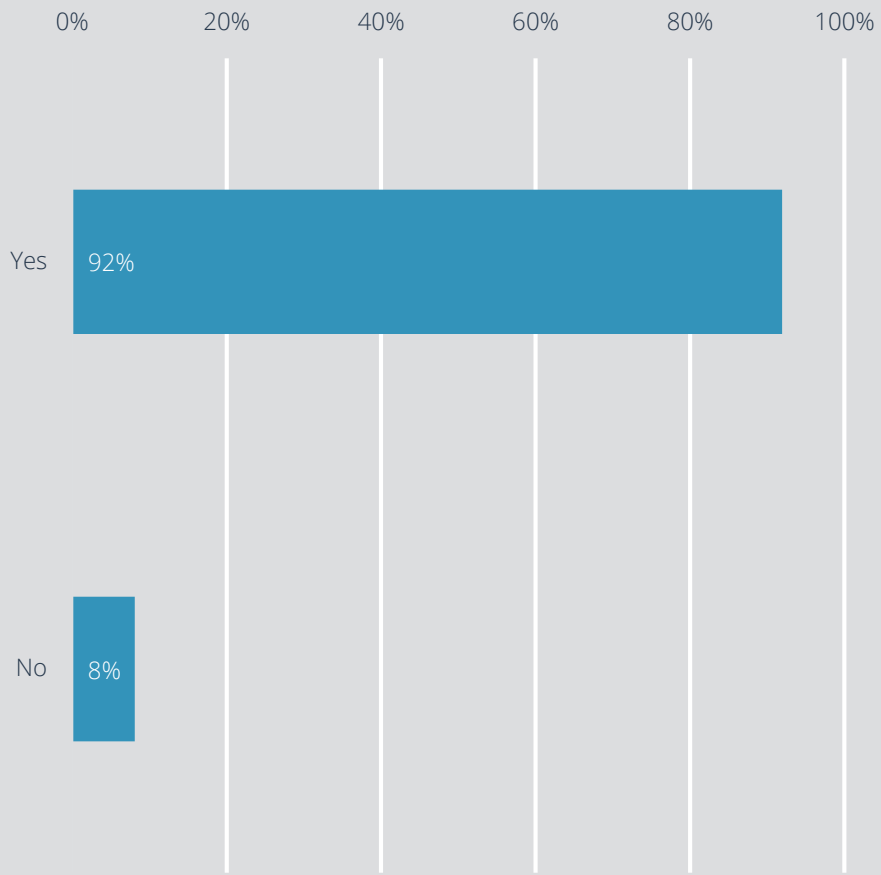
Audit of Authorized Signer. We asked how frequently the respondent audited their bank's authorized signer records for their accounts. We were both delighted and surprised to find out that nearly 4 out of 5 organizations did this at least once per year.

What is the normal time frame for updating signers on bank accounts when an employee leaves the company?



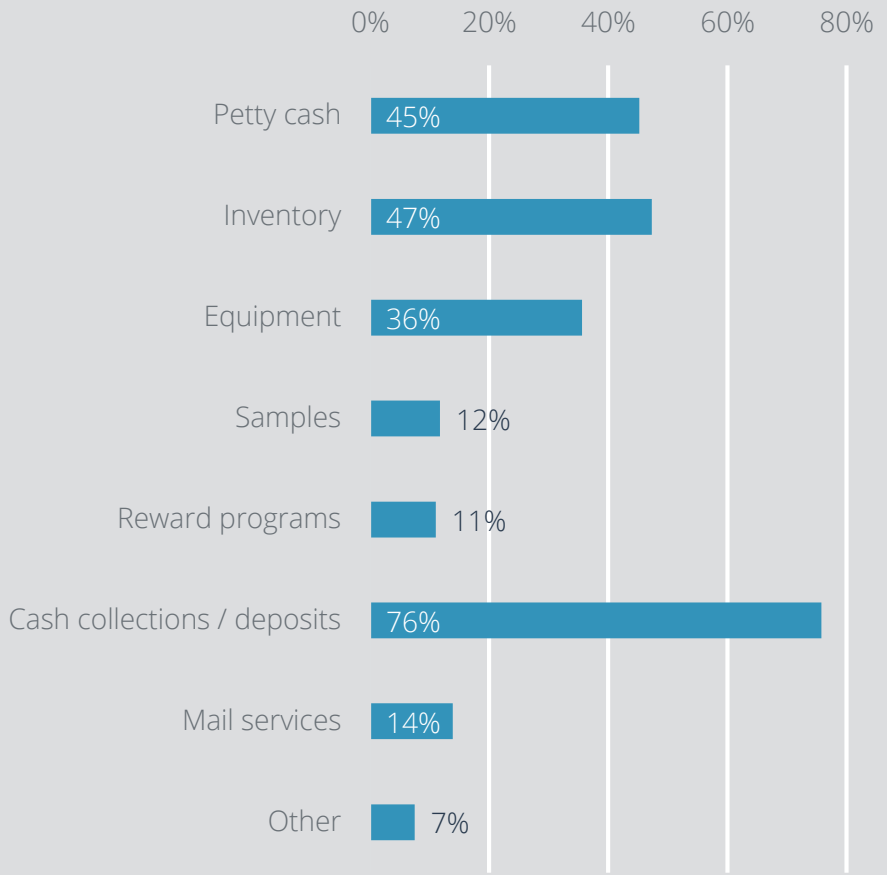
Timeframe for Updating Signers when the Leave the Company. When a signer leaves a company, there can be a time gap between that event and having their signing authority actually removed. Since this is a significant exposure, the impetus would be on the organization to remove the signer with great speed. However, this is not the case for the majority of firms as a standard practice. And, for over half of the firms it takes one month or longer. Fully 1/5th of organizations have no set timeframe to remove active signers when they leave the organization.

Does your organization ensure that both primary and back-up originators and approvers have appropriate segregation of duties?



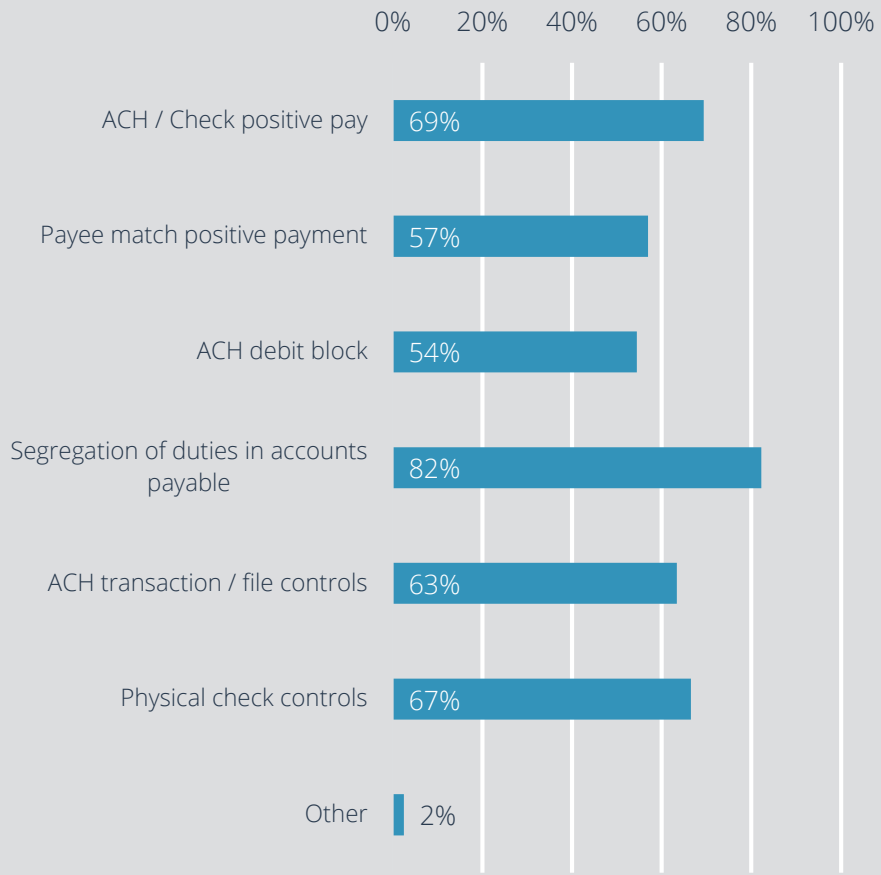
Approvals Backup and Primary. Yes, at 92%, is clearly the runaway favorite.

Which areas of the organization do you routinely audit for physical fraud? (Check all that apply)



Audit for Physical Fraud. Part of the intent of this question was to gauge which areas were most susceptible to fraud and used the actual emphasis on this area as evidenced by an audit. It's interesting to note that Travel & Entertainment (T&E) and Card activity were referenced multiple times for those who entered miscellaneous comments.

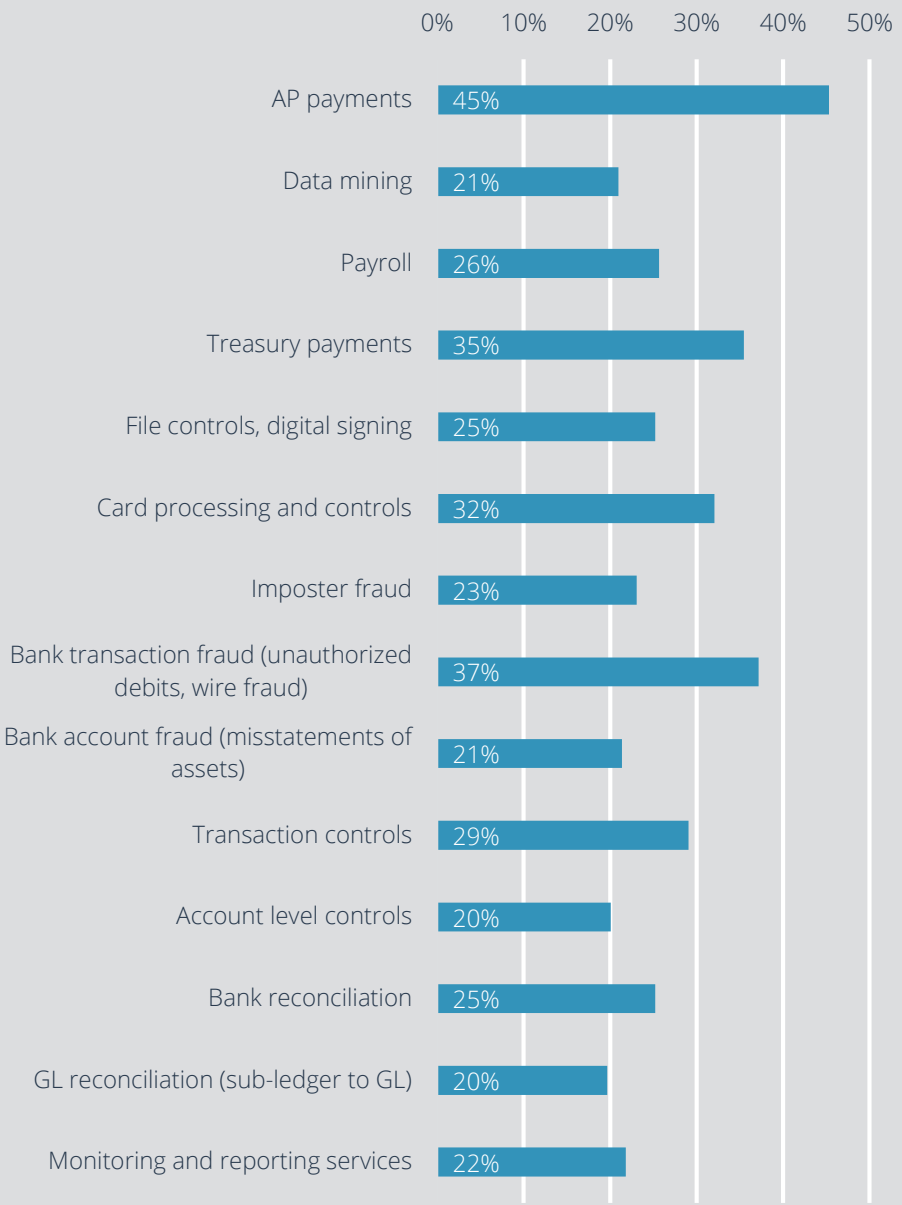
What controls does your organization have to prevent payment fraud? (Check all that apply)



Controls to Prevent Payment Fraud. 57% Payee Match Positive Payment represents a long push by banks for a superior positive payment. Over 50% of the respondents have standing ACH Debit Blocks. This has moved from a leading practice to a standard.

Spending Plans on Treasury Fraud Prevention, Detection and Controls. We wanted to see how plans to spend in this area were changing.

Which areas do you intend to spend more or significantly more on fraud prevention, detection or controls? (Check all that apply)



Significant Spend Areas. In order to probe in depth where organizations plan to spend significantly more, we polled the audience over 14 topics and offered a free-form additional field. Payments (AP 45%, Treasury 35%) held the 1st and 3rd position. Bank transaction fraud (37%) and card processing (32%) took the 2nd and 4th positions respectively.

STRATEGIC TREASURER | Market Intelligence

Awareness

Current & Precise

Assessment

Experienced & Intelligent

Application

Qualified & Actionable

FOR ADDITIONAL INSIGHT AND EXPERTISE ON HOW TO ENHANCE YOUR TREASURY SECURITY FRAMEWORK, OR FOR A COMPLETE ASSESSMENT OF YOUR EXISTING SECURITY FRAMEWORK, CONTACT STRATEGIC TREASURER & BOTTOMLINE TECHNOLOGIES

STRATEGIC TREASURER
Consultants in Treasury

525 Westpark Drive, Suite 130
Peachtree City, GA 30269

info@strategictreasurer.com

+1 678.466-2220

http://strategictreasurer.com

Bottomline Technologies®

325 Corporate Drive
Portsmouth, NH 03801

info@bottomline.com

+1 800.243-2528

http://bottomline.com