Special Report

2018 TREASURY FRAUD & CONTROLS SURVEY REPORT

Fraud Experience • *Bank Account Management* • *Control Framework* • *Technology Use*

Sponsored by

Bottomline Technologies®

Written & Produced by

Strategic Treasurer
Consultants in Treasury

Contents

Survey Contacts

CRAIG JEFFERY, CCM, FLMI
Founder & Managing Partner
craig@strategictreasurer.com

BRIAN COCHRUM
Director of Marketing
brian@strategictreasurer.com

ISAAC ZAUBI, CTP
Publications Manager
isaac.zaubi@strategictreasurer.com

Executive Summary

Not that long ago, the primary method for criminals to steal funds from a bank or organization was to physically rob it. Then, along came a few savvy fraudsters who introduced more elaborate and inconspicuous methods of extraction, such as check fraud. Fast forward to today and the fraud landscape has become incredibly sophisticated and advanced. When looking at the criminal's playbook in 2018, fraudulent techniques such as Business Email Compromise (BEC) and Ransomware have become the norm. Given that these methods are more difficult to prevent and result in much larger losses for organizations, it is not an overstatement to say that criminals have drastically increased the size of their payouts and their ratio of successful attempts. These successes have been driven largely by greater levels of automation and technological advancement, as well as clever subterfuge and patience. They have continually improved their tactics over time, which has only further increased their yield, and they aren't done yet.

In an effort to stem the flow of losses, treasurers have invested heavily in their security infrastructure. But despite their best efforts, practitioners have proven themselves largely unprepared for a more organized, strategic, and persistent type of criminal.

As criminals continue to target the treasury environment, Strategic Treasurer and Bottomline Technologies have partnered for the third consecutive year to examine the trends found among practitioners and their organizations and determine actual experiences in fraud, best practices for controls, and plans for response. This year-over-year data provides a basis for understanding the direction of change in the dynamic environment of today's digitized marketplace. Our hope is that practitioners can benefit from this unfiltered view of the landscape to better educate themselves on the complex and constantly evolving state of treasury fraud.

Despite increased awareness and spend, corporations have proven themselves largely unprepared for a more organized, strategic, and persistent threat.

Craig Jeffery, FLMI, CCM

Strategic Treasurer,
Founder & Managing Partner

Craig Jeffery formed Strategic Treasurer LLC in 2004 to provide corporate, educational, and government entities direct access to comprehensive and current assistance with their treasury and financial process needs. His 20+ years of financial and treasury experience as a practitioner and as a consultant have uniquely qualified him to help organizations craft realistic goals and achieve significant benefits quickly.

About the Survey

The 2018 Treasury Fraud & Controls Survey, conducted by Strategic Treasurer and underwritten by Bottomline Technologies, is now in its third year and continues to capture key insights from both corporate and bank practitioners regarding treasury fraud experiences and security practices. The results have been categorized into five general sections - demographics, fraud experience, bank account mgmt, control framework, and technology use. The data will be presented at numerous junctures throughout the year via industry whitepapers, webinars, and presentations, and will serve as an educational tool for the financial environment in developing a response to the pandemic of fraud. This survey has become a pivotal component of our market research, and we look forward to furthering our analysis and understanding of the fraud and security landscape in the years to come.

Key Survey Statistics

2017			2018			
OCTOBER	NOVEMBER	DECEMBER	JANUARY	FEBRUARY	MARCH	APRIL
Planning		Survey Run Time			Analysis	

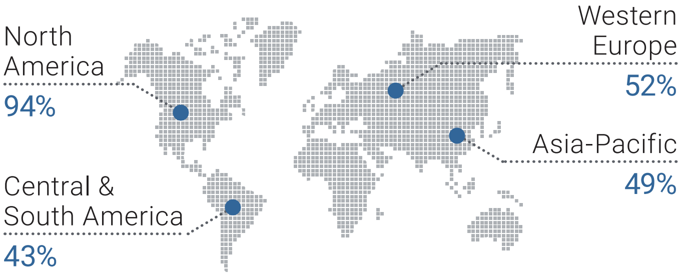
200+ breakouts

300+ respondents

3rd year of analysis

15+ industries represented

RESPONDENT REGIONS OF OPERATIONS



TOP CORPORATE RESPONDENT ROLES

26%	Treasury/Cash Manager
17%	Treasurer
15%	Assistant Treasurer
15%	Treasury Analyst
4%	CFO

Top Ten Statistics

This survey produced a high volume of data. Among the key findings:

6x

more corporates plan to spend more on fraud / security tools this year over prior years compared to those planning to spend less

41%

of corporates plan to invest in security controls for their AP payment operations over the next year; more than any other area of security

31%

of corporates have a standalone policy for cyber fraud insurance

90%

of corporates have implemented dual controls for all transactions

29%

of firms that experienced a system-level wire fraud attack suffered a loss

18%

of companies that experienced check forgery actually suffered a loss

3x

more corporates experienced a ransomware attack in the 2017-2018 timeframe compared to 2016-2017

33%

of firms that were hit with fraud had at least one attempt that originated from a completely unknown source

61%

of corporates see themselves as being in a better or significantly better position to fight fraud this year as compared to last year

84%

of corporates have indicated that the threat of cyber and payments fraud has increased over the past year

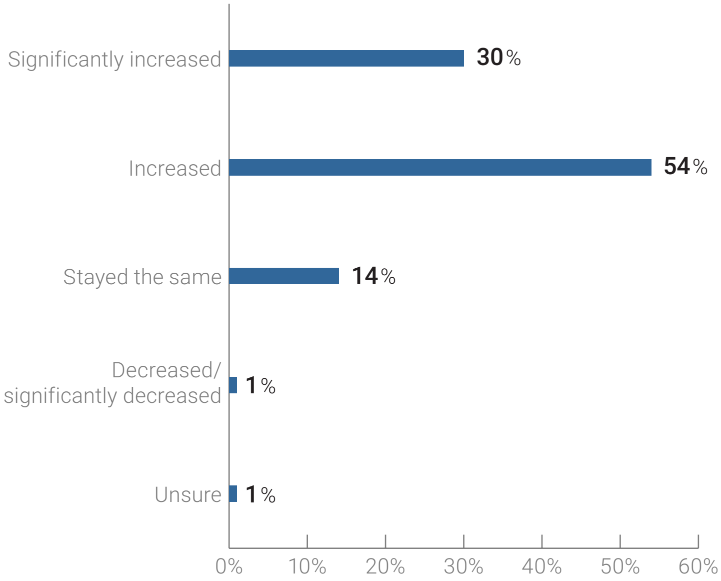
Key Findings

1| FRAUD REMAINS A TOP CORPORATE FOCUS

▸ *Heightened Threat Perception.*

One of the first questions asked to respondents of this year's treasury fraud survey was about the perceived threat of fraud and how the outlook has changed over the past year. Given that fraud has been on most practitioners' minds for several years now, and that many firms have had ample time to invest in enhanced security controls and tools, do treasurers still view fraud as a significant threat? The answer to this question is an overwhelming "yes". In fact, 84% of corporates believe the threat of cyber fraud has increased over the past year. Clearly, the threat that fraud poses has not dissipated in the eyes of treasurers; fraud continues to be at the forefront of practitioners' minds and security remains a top priority for treasury in 2018.

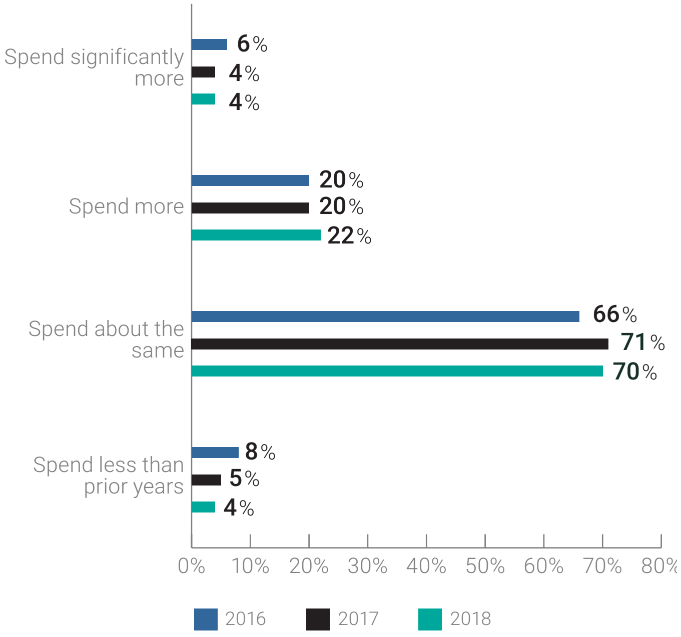
Corporates: In the past year, I think that the threat-level of cyber fraud and payment fraud has:



▸ *Continued Security Investments.*

As the threat of fraud persists, organizations continue to pour money into their security controls. Since 2016, approximately one quarter of corporates have consistently spent more on security and controls than in prior years, which has amounted to 3-5x more firms increasing their security spend versus those reducing their investment. This elevated spend has targeted a broad array of areas, ranging from AP and treasury payment controls to reconciliation features, account level controls, and fraud monitoring / reporting services. It is also worth noting that cyber fraud insurance has been an area of increased focus for corporates as well, with 31% of firms indicating a higher level of coverage in 2018 as compared to prior years.

What are your spending plans for treasury fraud prevention, detection, and controls?

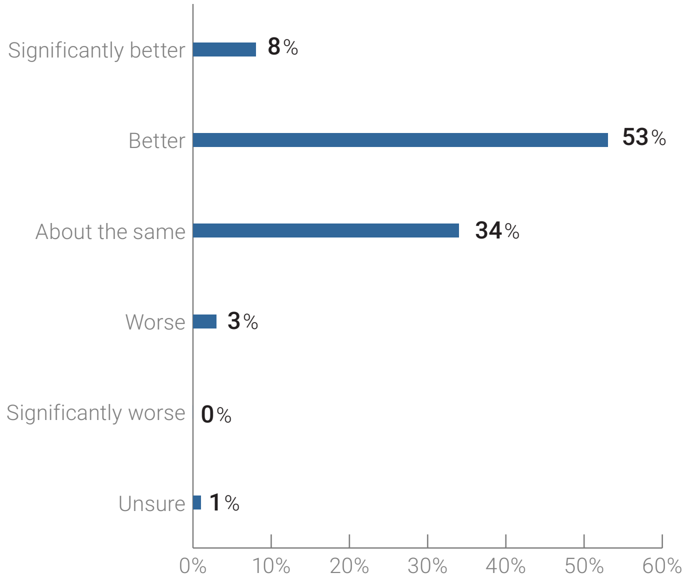


Data excludes "unsure" responses.

Increased Corporate Confidence.

Interestingly, despite viewing today's fraud landscape as more threatening than in past years, corporate practitioners are more confident in their company's ability to prevent losses. In fact, 20 times more corporates believe they are in a better position to deal with fraud this year as compared to last year. As part of a similar but separate question, two thirds of firms believe their ability to prevent, detect, and respond to fraud has improved in the past year. The reason for this increased confidence within the corporate ranks may be that practitioners feel as though the security investments they have made within the past few years have resulted in their ability to more effectively deal with any attempts that target their assets. But while some firms have done well with strategically developing a comprehensive control framework, as we will see, not all of these investments have resulted in a more secure environment.

Corporates: With regard to the threat level associated with cyber fraud and payment fraud and considering our current security posture, we are in a(n) __________ position as compared to last year.

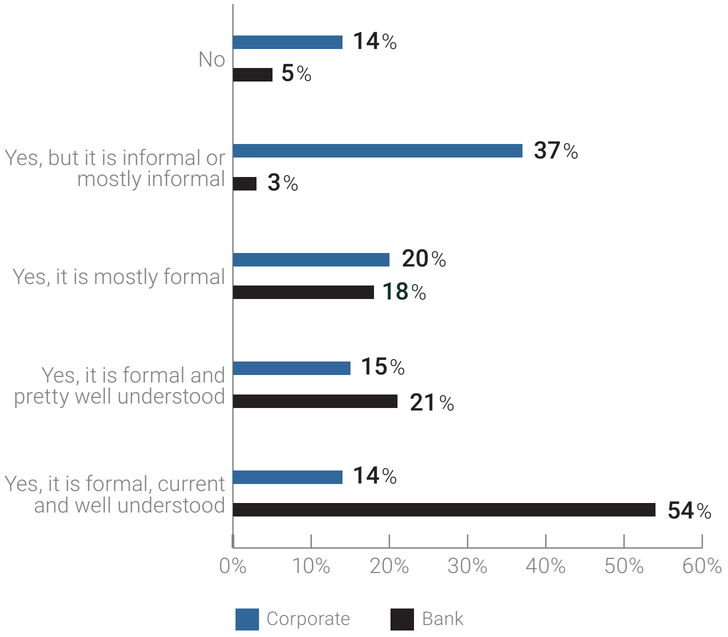


2 | SECURITY CONTROLS STILL INADEQUATE

Piecemeal Approach to Security.

As corporate security and fraud prevention practices are analyzed in aggregate, it seems as though investments in certain tools or technologies are not always part of a more holistic strategy. Instead, practitioners may identify one or two large areas of exposure that are subsequently addressed through the purchase of a new security solution, while other exposures or areas of weakness go unnoticed. This piecemeal approach to security is highlighted when looking at corporate control frameworks compared to banks. As it stands today, 75% of banks have developed a formal treasury fraud control framework, while only 29% of corporates have done the same. Without a definite and comprehensive strategy for fighting fraud, it is difficult to identify every gap that exists and nearly impossible to ensure that one's security infrastructure is all-encompassing. While investments in security are encouraged, they only work as part of a larger and more holistic security framework; purchasing new tools arbitrarily will plug some holes but leave other areas entirely exposed.

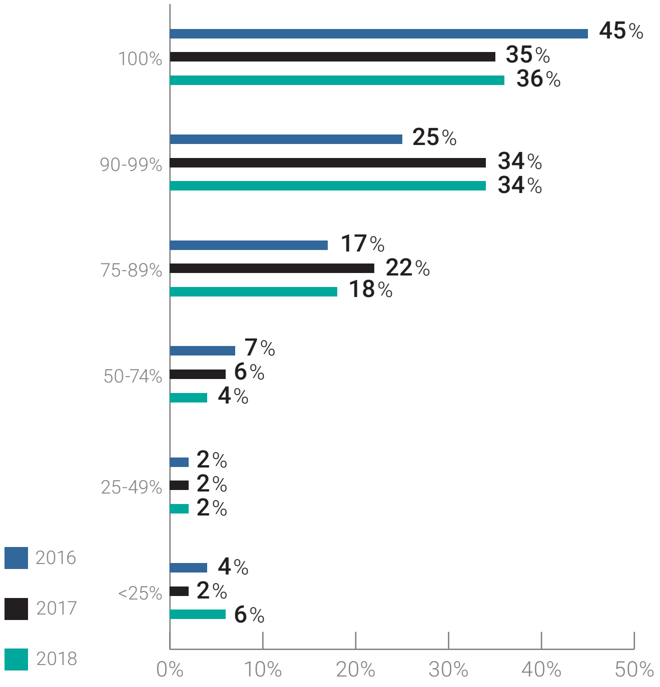
Do you have a treasury fraud and controls framework?



Static Improvements in Visibility.

The ability to view cash positions and receive transaction alerts / balances in real-time can assist treasury in the fight against fraud, as any anomalous transactions that hit an account can be quickly identified. Without daily or real-time visibility, a fraudulent transaction may go unnoticed for several days, at which point it is too late. Over the past decade, we have witnessed promising growth in corporate visibility, to the extent that nearly three of every four firms have daily visibility to more than 90% of their accounts. But progress along this front has dampened in the past two to three years. As it stands today, 70% of firms indicate that they maintain daily visibility to 90%+ of their accounts. This represents a three year stretch without growth in this area, as the levels of visibility in 2016 were the exact same (70%).

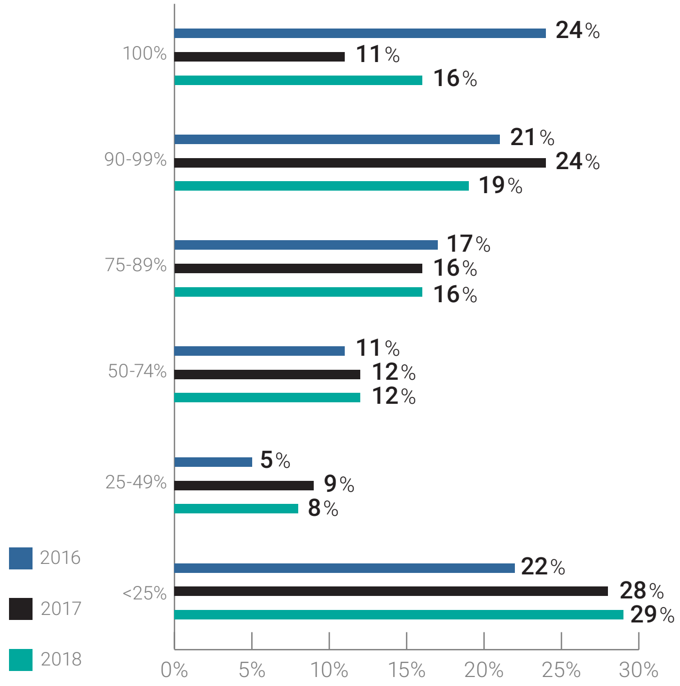
What percentage of your bank accounts do you have visibility to on a DAILY basis?



Reconciliation Capabilities Decline.

Similar to the stagnant growth in visibility, advancements in corporate reconciliation processes have been derailed in recent years. Since 2016, reconciliation has been a sizeable area of investment for treasury in specific and plays an important role in uncovering fraudulent activity. However, while the 2016 edition of the survey saw that 45% of corporates reconciled 90%+ of their accounts on a daily basis, in 2018, that number was only 35%. This represents a sizeable decrease in daily reconciliation practices in just a short time. Furthermore, only 31% of corporates indicated that their reconciliation process is primarily automated. Instead, 43% have a partially automated system and 22% are almost exclusively manual. Given the tools available to treasury today, visibility and reconciliation processes represent two areas where strategic investment by treasury can provide significant benefits quickly; as such, the fact that growth has stagnated is both puzzling and worrisome.

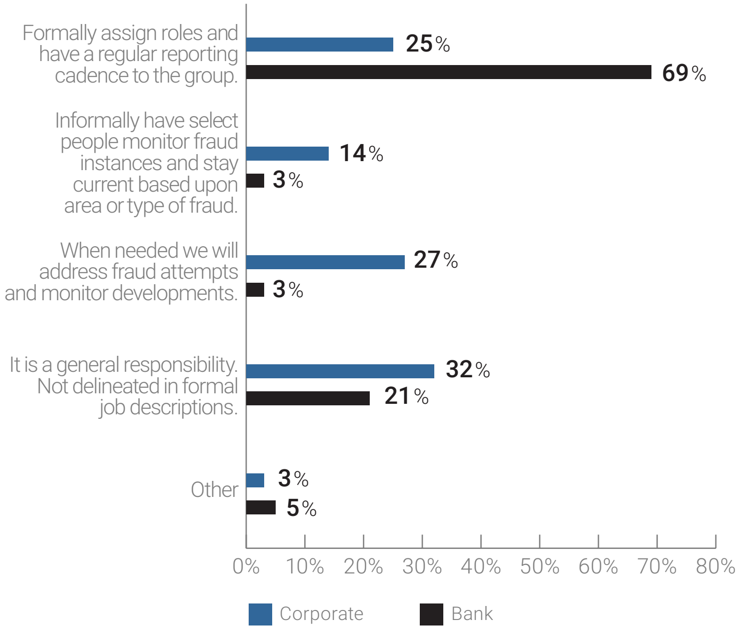
What percentage of your bank accounts are reconciled on a DAILY basis?



Fraud Management Responsibilities Unassigned.

While we cannot be sure of the cause for this, one likely reason is due to the absence of any fraud focus groups within the corporate environment. While fraud monitoring and security practices may be part of company policy, the actual development of a team to actively monitor fraud within the organization has yet to become a standard practice.

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

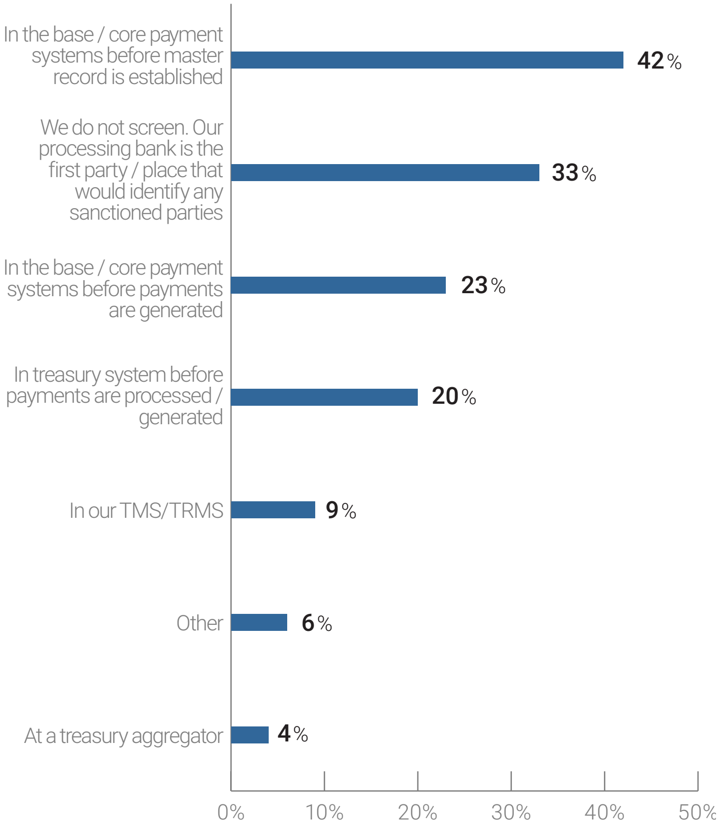


Sanctions Violations; An Ignored Threat.

Fraud briefly aside, there is an alternative area of treasury operations where losses can stem from fines and penalties, rather than criminal extractions. We are talking about sanctions violations, and although the impetus has been on banks to ensure their payment processes provide proper sanctions screening and compliance monitoring workflows, today's compliance environment places equal responsibility on corporates for managing their own compliance procedures. This may be news to some corporates, considering that a full one-third (33%) currently do not screen their payments for sanctioned parties at all. While some practitioners might believe that their bank would be the party fined if payments to a sanctioned party are executed, this is not necessarily the case. In the current environment, whichever party is found to be most negligible in a sanctions violation is the party that gets fined. In 2017 alone, OFAC* handed out $120 million in fines and penalties, and many of these were levied against corporates rather than banks. Given the shifting compliance landscape, this is an area of exposure, which corporates should be aware of and actively working to solve.

*OFAC statistics obtained from treasury.gov

Corporates: We screen for sanctioned parties: (Select all that apply)

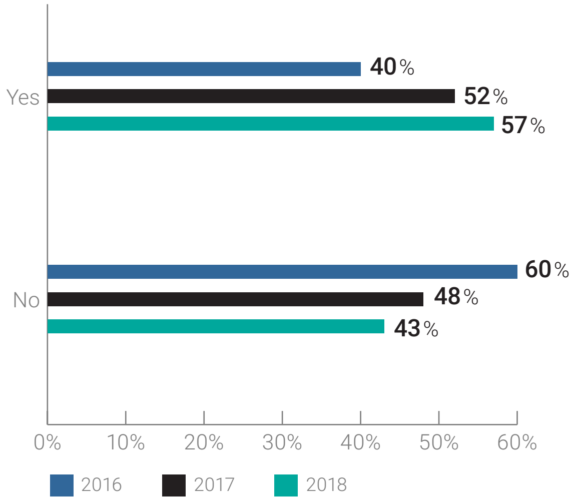


3 | LOSSES CONTINUE TO MOUNT

Fraud Experiences Rise.

Since the inaugural findings of the 2016 Treasury Fraud & Controls survey were obtained just over two years ago, we have witnessed a dramatic rise in the level of fraud activity perpetrated against the treasury environment. While 40% of firms indicated they had experienced fraud in 2016, that number has climbed to 57% in 2018. This represents a 40%+ year-over-year increase, and drives home just how prevalent fraud has become within the financial environment. In today's world, more organizations experience fraud than those that do not. Given this reality, there is really no excuse for firms not to have sophisticated control frameworks in place. If your company has not already been targeted for fraud, it will be, and given the current trend, the frequency of attacks will only escalate moving forward.

Have you experienced fraud in the last 12 months?

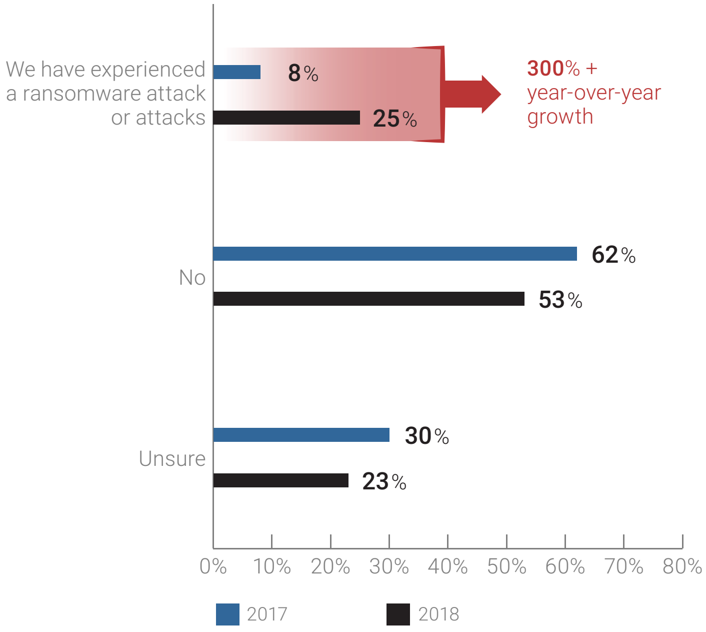


Data excludes "unsure" responses.

New Fraud Types Surface.

In 2017, respondents were polled over their experiences with ransomware just before the massive Wannacry outbreak occurred. At that time, only 8% or so of corporate practitioners had experienced a ransomware attempt. What a difference one year makes. Fast forward to today and nearly 1 in 4 firms have experienced a ransomware attack. This represents more than 300% growth in ransomware attacks in just one year's time, and pays testament to the fact that once criminals identify a new exposure, they act quickly to exploit the weakness and extract funds. Similar growth in BEC fraud was identified several years ago, and today, three in four firms have experienced a BEC attempt in the past two years. This data serves to further emphasize the fact that the criminal's playbook is constantly expanding and new fraud techniques are constantly being developed and improved upon.

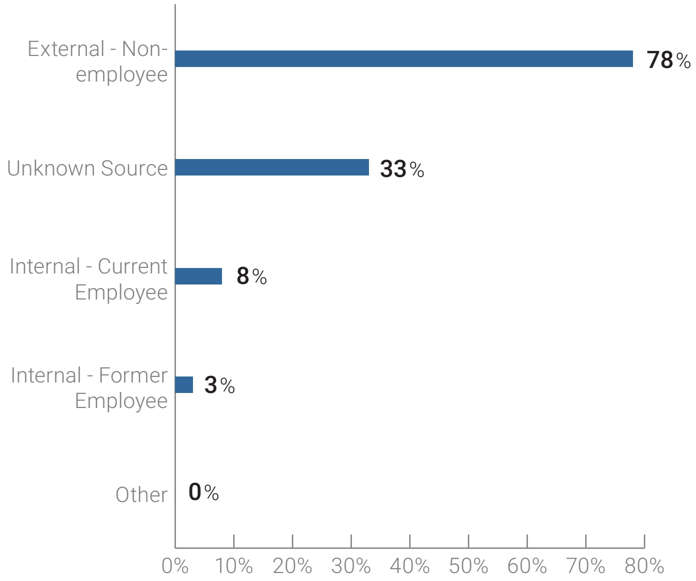
Corporates: Thinking of the last two years, please label your company's experience with the following (ransomware)



Where Did it Come From?

One of the more frightening statistics uncovered through this year's results is that 33% of firms that experienced fraud were not sure of the source. Did it originate internally or was it an external party? Was it an orchestrated group effort or a sole perpetrator? As cyber fraud activity becomes the norm, the terrifying truth is that criminals can now initiate attacks on corporations from entirely separate countries or different world regions, increasing the difficulty of identifying the source. An actor in Egypt can launch an attack on a U.S.-based company without ever leaving his or her home.

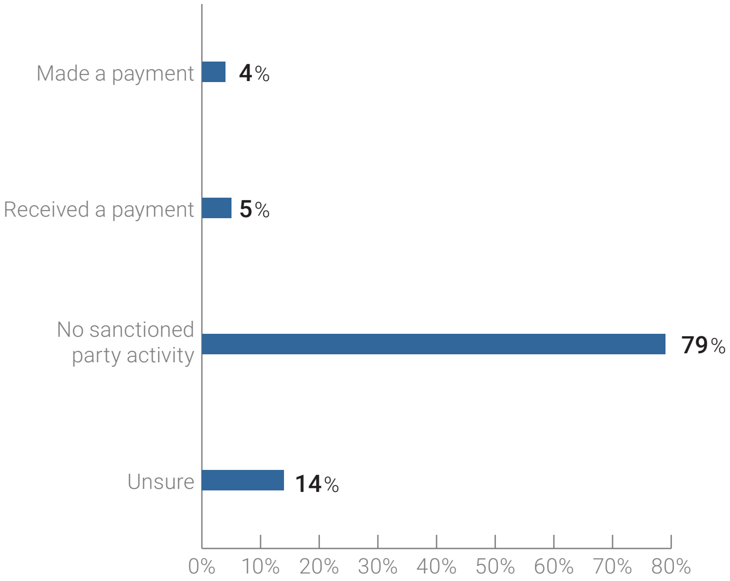
Corporates: From which party did you experience fraud? (Select all that apply)



Sanctioned Party Payments.

With regards to the aforementioned fact that one-third of organizations do not conduct internal sanctions screening on their payments, we have seen several firms inadvertently exchange funds with a sanctioned party over the past year. In total, nearly one in ten firms made this mistake. Today, the availability of enhanced compliance and sanctions screening software enables organizations to screen internally before disbursing payments. As such, a simple software installation should fix this issue, and many TMS or Treasury Aggregators have even implemented sanctions screening tools into their solution. While the threat of making a sanctioned payment is not yet as widespread as the threat of fraud, the consequences can be equally if not more severe in terms of dollar losses and reputational damage. As organizations develop their control framework, compliance tools and sanctions screening solutions are components that should be strongly considered.

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



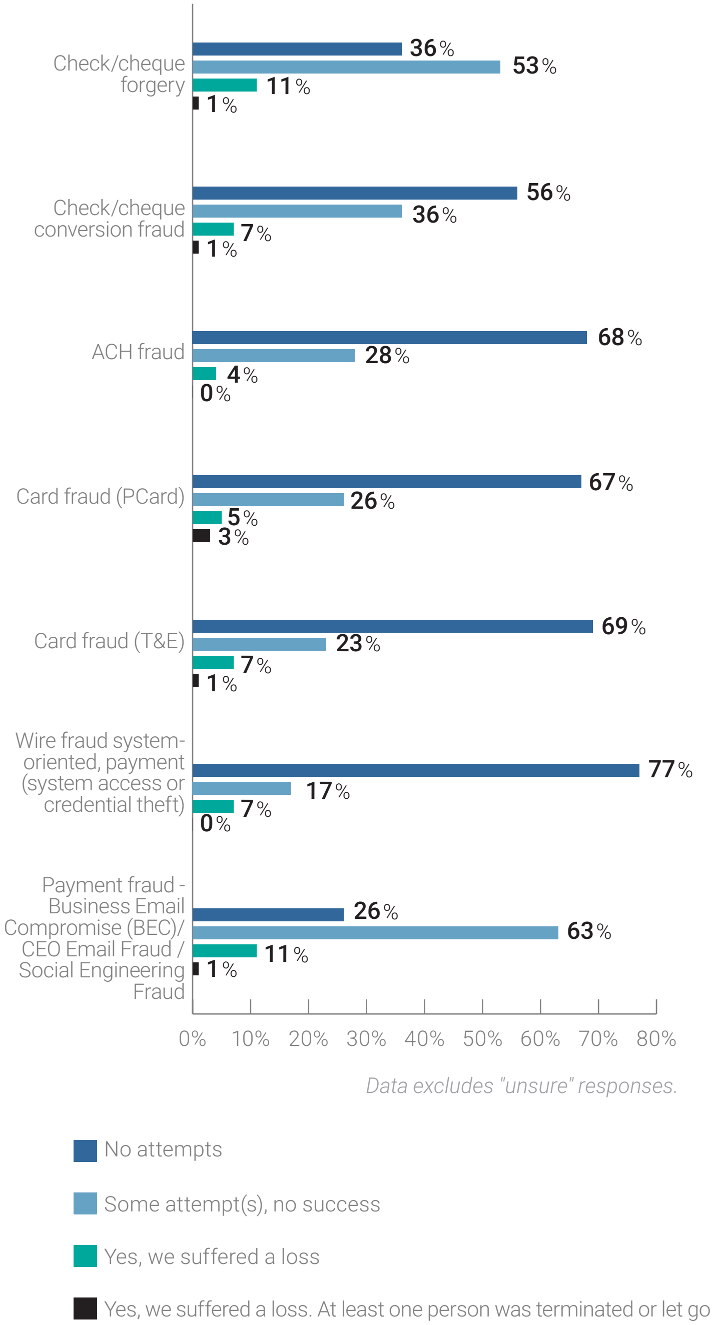
Corporate Losses Grow.

As the frequency of fraud attacks has grown, so too have the level of losses sustained by organizations. Depending on the type of fraud, criminal success rates range anywhere from 10-30%. Interestingly, there was no notable improvement in the ability of corporates to prevent more common attacks like check fraud versus sophisticated attempts like ransomware and wire fraud; in fact, criminals experienced greater levels of success with check fraud than ransomware or BEC. In total, 10% of ransomware attempts were successful, 16% of BEC attempts were successful, nearly 19% of check forgery attempts were successful, and 24% of PCard fraud attempts were successful. Across the board, we saw significant levels of loss for corporate treasury. Despite the rise in security investments and the spike in corporate confidence, it would appear as though criminals are still being rewarded handsomely for their efforts.

CRIMINAL SUCCESS RATIOS BY FRAUD TYPE	
ACH Fraud	12.5%
BEC/Imposter Fraud	16%
Check Conversion	18.2%
Check Forgery	18.5%
PCard Fraud	23.5%
T&E Card Fraud	26.7%
Wire Fraud *(System-Oriented)*	29.2%

The above chart shows the percentage of fraudulent attempts that were successfully carried out by criminals for each type of fraud. Percentages were calculated using the graph on the right.

Have you experienced any of the following in the past TWO YEARS? (Select all that apply)



Data excludes "unsure" responses.

Key Takeaways

In analyzing results from this year's survey, the image that comes to mind is of a recent Olympic track race where the frontrunner celebrated too early, thinking he had won, only to be passed and ultimately lose in the final meters of the race. Since many companies are investing more in security tools, they feel better prepared to take on the criminal activity that threatens their funds and data. This has generated some positive feelings, but it does not make their systems and processes impenetrable and it does not mean they can now just sit back and relax.

Although many organizations have invested heavily in security technology and fraud prevention tools, a significant portion still have gaps in their security that continue to be exploited by criminals. In analyzing the full scope of corporate fraud experience and preventative tactics, this seems to be due to the fact that while corporates have been plugging holes as best they can, the lack of any comprehensive treasury fraud and controls framework results in some exposures never being identified or addressed. Subsequently, any persistent and probing criminal is still able to find weaknesses and gaps to penetrate. This scenario has played out all too frequently over the past year, and until corporates are able to develop a more robust and holistic approach to security, their losses will continue to grow.

If your organization is among those that has recently upgraded their defenses, that is excellent. But don't celebrate too soon. Your adversaries are also enhancing their capabilities; vigilance has no end date! Stay cautious, continually monitor your security layers, and do not hesitate to improve upon any area of weakness. Be thorough in developing your control framework and strategic with your security spend. It is the only way to protect against the modern criminal.

Since many companies are investing more in security tools, they feel better prepared to take on the criminal activity that threatens their funds and data. This has generated some positive feelings, but it does not make their systems and processes impenetrable and it does not mean they can now just sit back and relax.

Action Items for Treasury Practitioners

- *Understand that fraud prevention is not a "One and Done" project; it is an ongoing responsibility*
- *Recognize that criminals are constantly evolving to become more sophisticated and calculated.*
- *Consider both the technology and human components of your security infrastructure and don't hesitate to update your controls whenever an exposure is identified.*

Appendix

This next section of the report contains a subset of questions from each of the major categories contained within the survey; demographics, fraud experience, bank account management, control framework, and technology use. Although each section of the survey was comprised of over 30 questions, we have only provided a limited selection from each section. Other questions we have chosen to house internally and not share publicly at this time.

However, for those individuals that completed the survey, we have provided additional data points and areas of analysis. This special report contains over 50 questions from the survey, as compared to the general report, which contains over 25 questions. Survey respondents are also provided with early access to results documents and early sign-up for results webinars and presentations. This special report, along with the actions taken to offer additional commentary for survey respondents, are part of our efforts to give back to those who complete our surveys. As a token of gratitude for the time spent giving us their feedback and helping us prepare these research reports, we will continue to provide extended analysis and commentary, as well as other benefits, to our survey takers.

Total Survey Size *(Full Data Library):*

Over 150 questions cut by industry and company size

SPECIAL REPORT ***(For Survey Respondents Only):***
Over 50 uncut questions with commentary

GENERAL REPORT ***(For Broader Public Audience):***
Over 25 uncut questions with commentary

Although Strategic Treasurer and Bottomline Technologies maintain cuts of data according to company size and industry, we do not generally make these detailed findings available to the public at large. Subsequently, all the responses provided in this survey index are not split by respondent role, industry, or size. Any reader wishing for further analysis or feedback on any point of interest is encouraged to contact Strategic Treasurer or Bottomline.

Note: These two icons indicate whether the question shown was asked of corporates, banks, or both within the survey's branching logic.

Appendix Sections

DEMOGRAPHICS

FRAUD EXPERIENCE

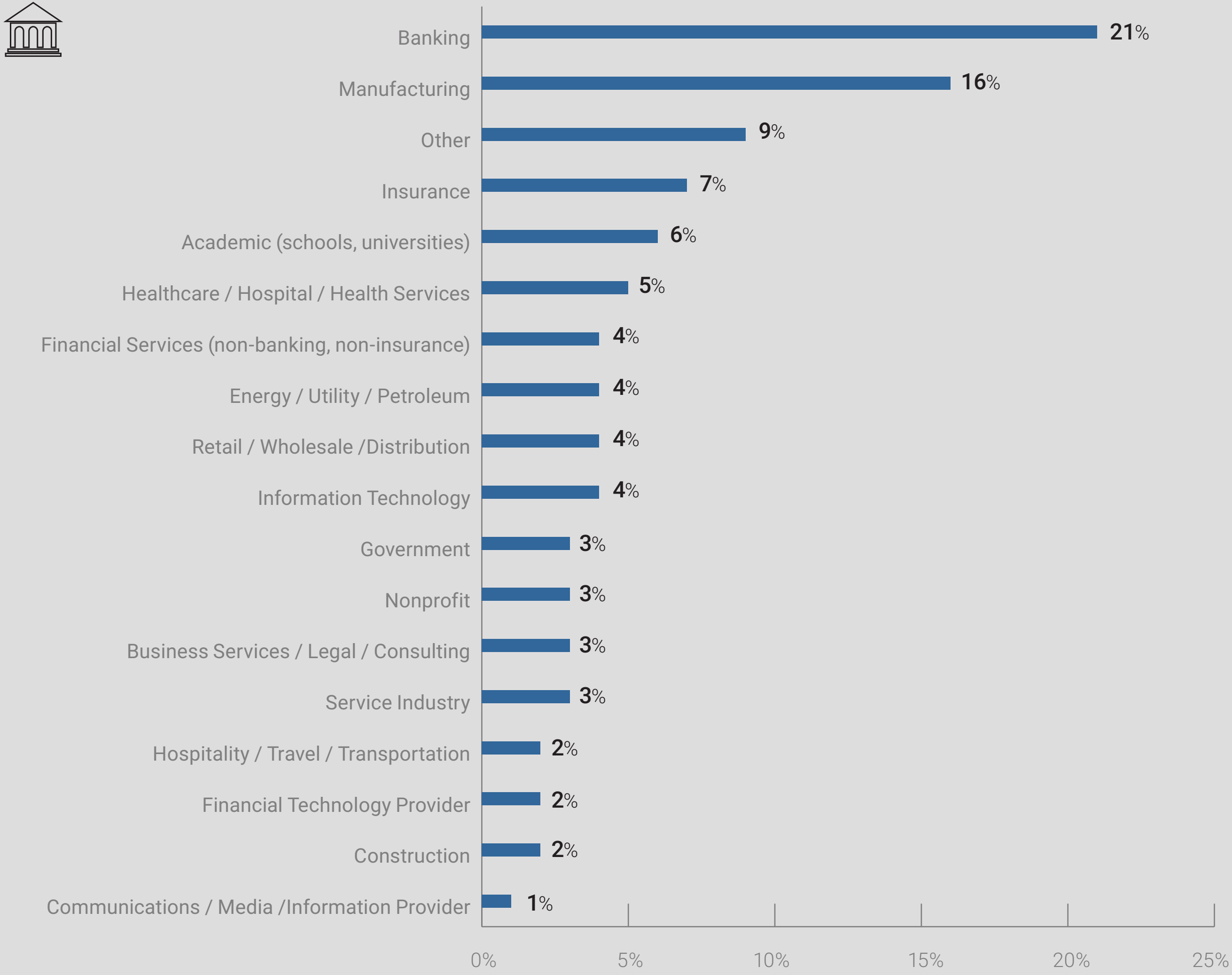
BANK ACCOUNT MGMT

CONTROL FRAMEWORK

TECHNOLOGY USE

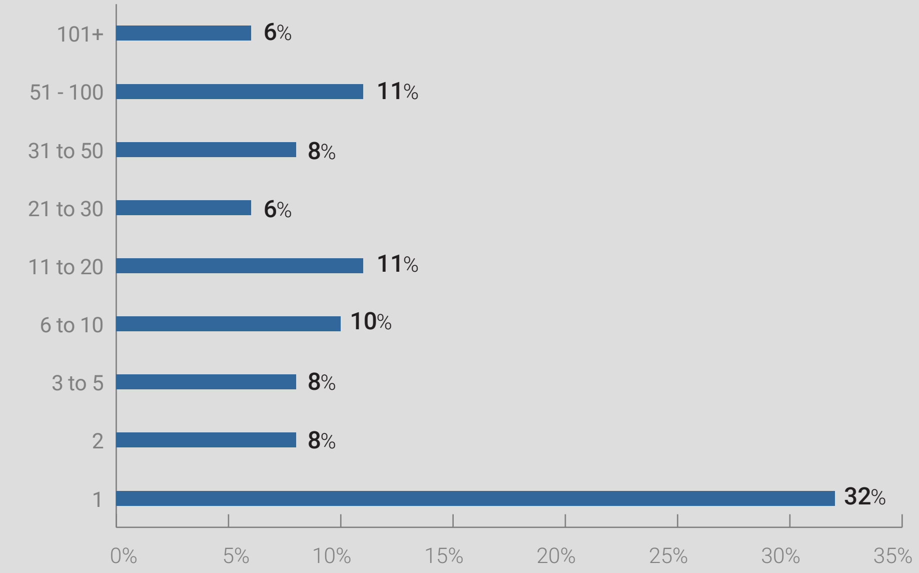
Demographics

What is your organization's industry?



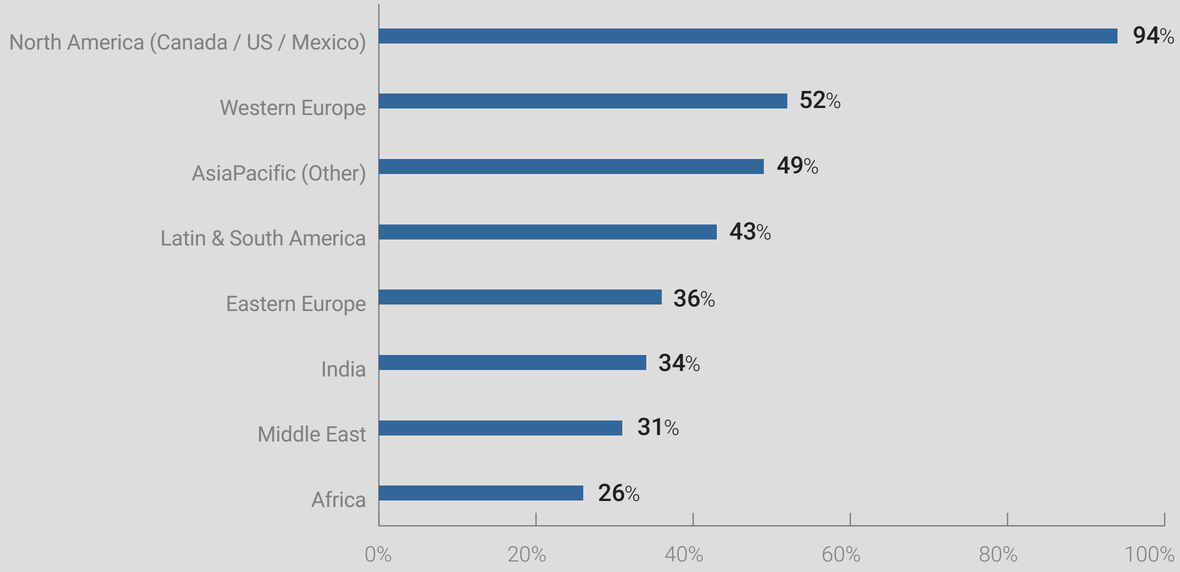
The banking industry accounted for one-fifth of the total survey population. Manufacturing was the next highest industry at 16% and also served as the highest corporate industry represented.

Our business operates in this many countries: *(Enter a number)*



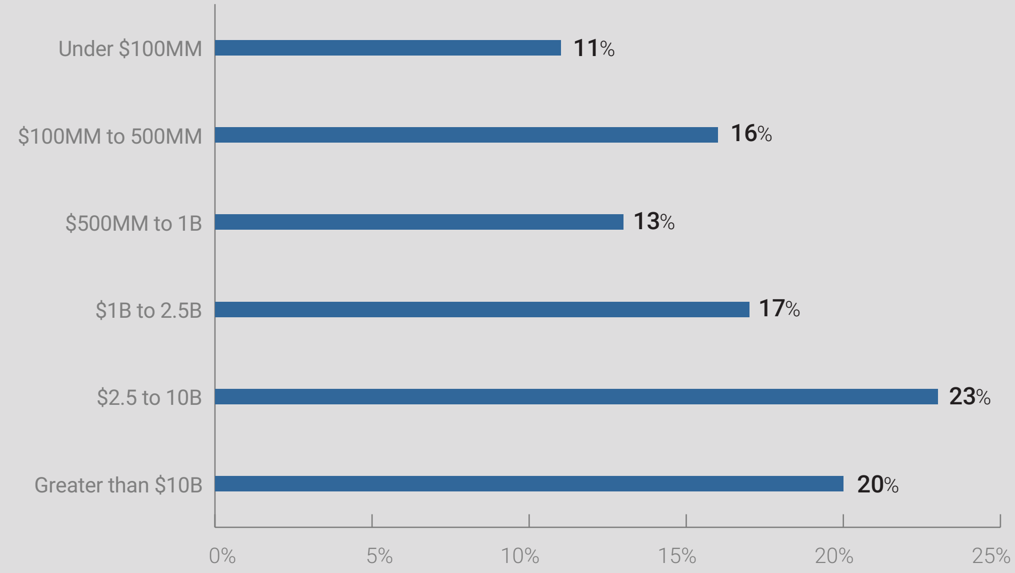
Just under a third of the survey population only operated in one country. Over half operated in 6 or more countries and 17% operated in more than 50.

Which regions does your company operate in? *(Select all that apply)*



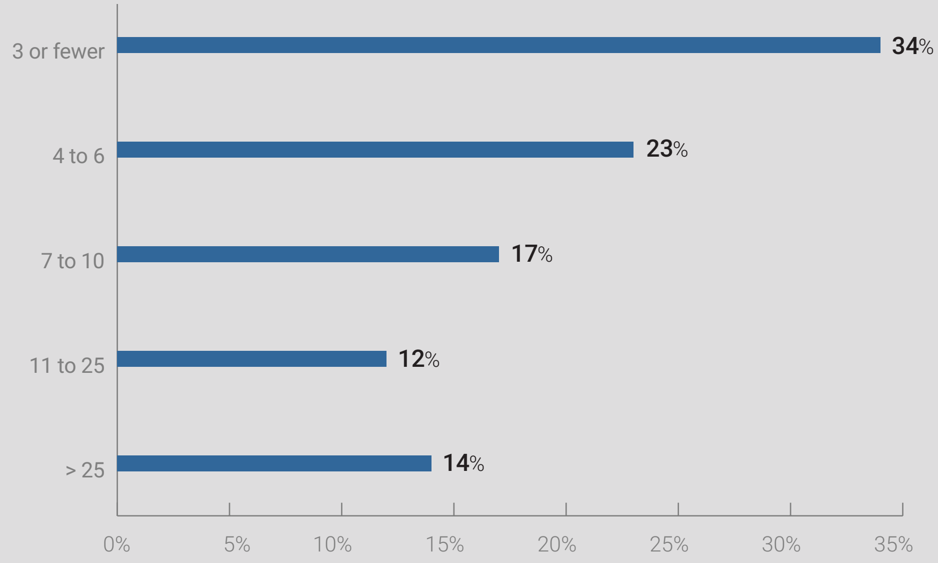
In total, at least one-fourth of respondents were conducting business operations in each of the major world regions.

What is your company's annual revenue?



At 60% of the total population, large corporates (Revenues $1Billion+) constituted a slightly larger portion of the respondent pool compared to small corporates (Revenues <$1Billion).

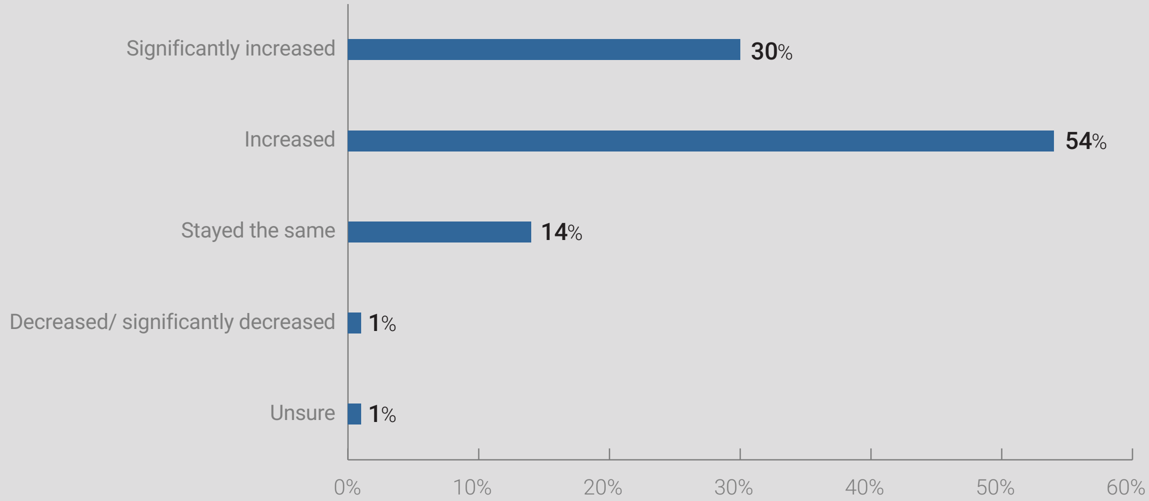
How large is your global treasury organization, including analysts?



Approximately one-third of corporate respondents were operating with three or less staff members in their treasury department. On the opposite end, 26% are operating with more than 10 in treasury.

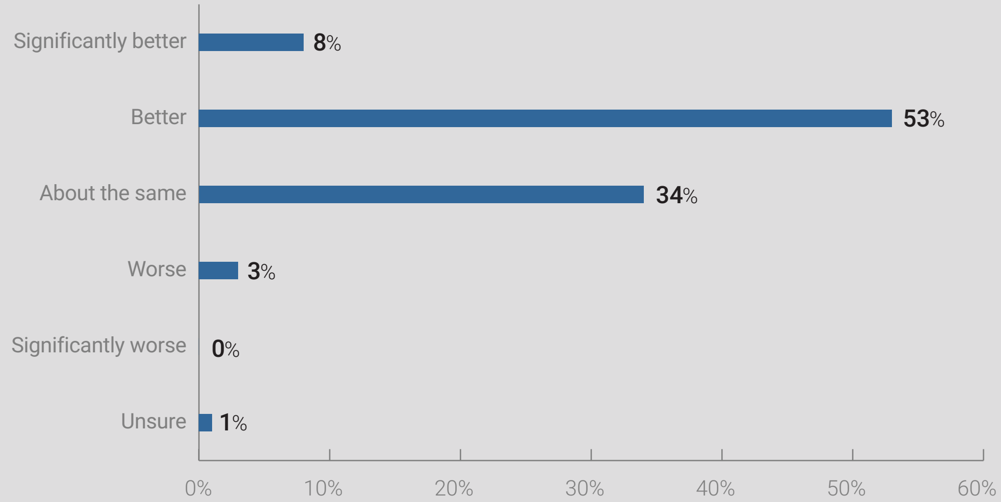
Fraud Experience

In the past year, I think that the threat-level of cyber fraud and payment fraud has:



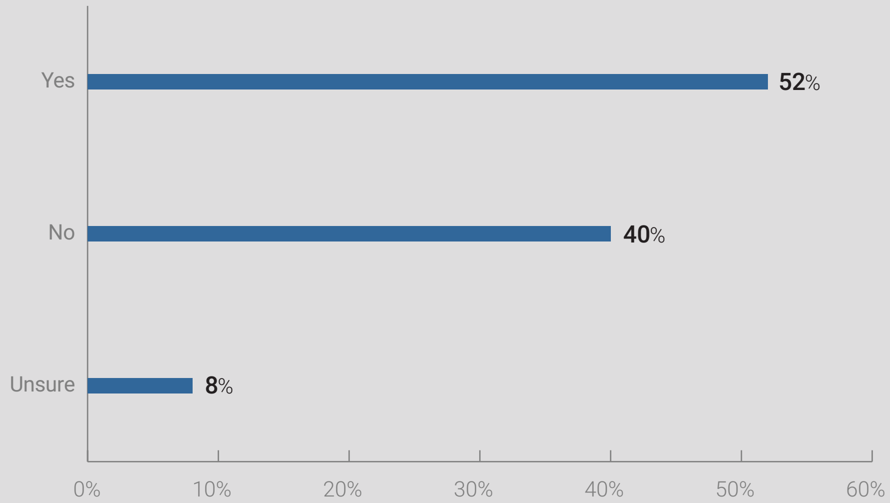
Only 1% of corporate respondents thought that the threat of cyber and payment fraud has decreased in the past year. Alternatively, 84% thought that threat of fraud had increased or significantly increased.

With regard to the threat level associated with cyber fraud and payment fraud and considering our current security posture, we are in a(n)__________ position as compared to last year.



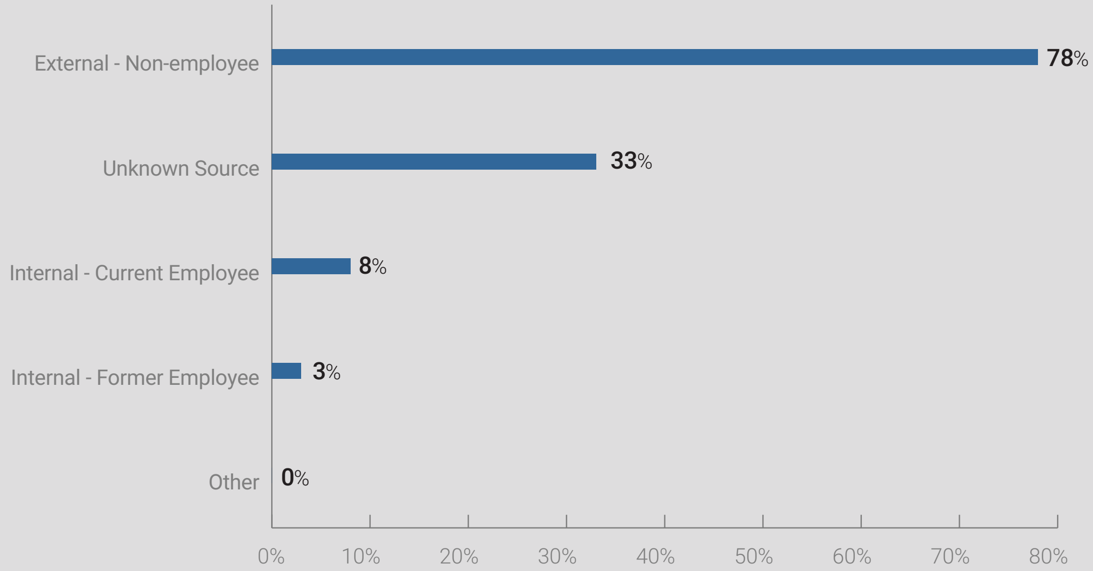
Only 3% of corporates viewed their security posture as worse than it was in the last year. On the other hand, 61% believed their posture had improved or significantly improved.

Have you experienced fraud in the last 12 months?



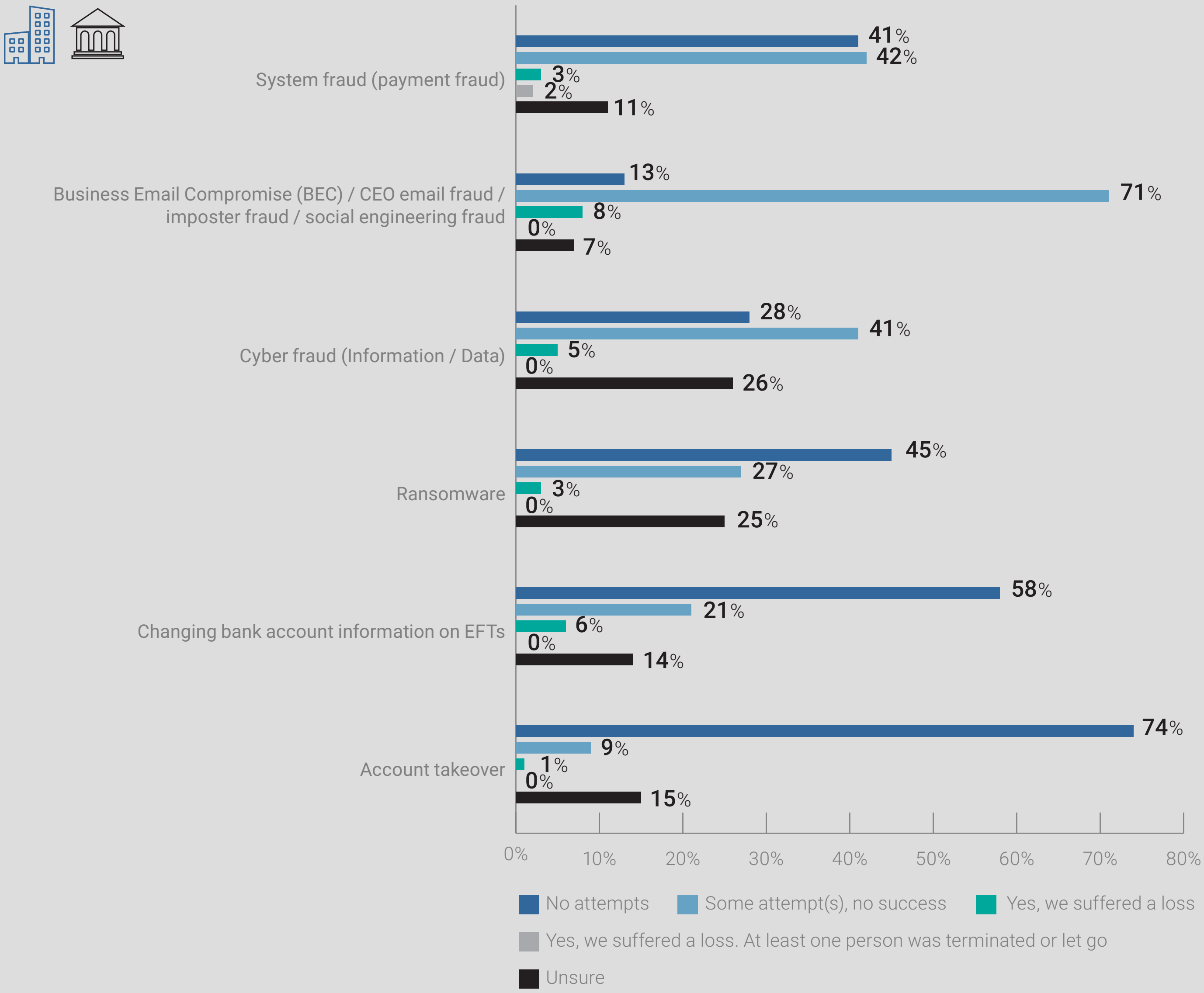
Interestingly, 8% of corporate respondents were unsure that if they had experienced fraud. 52% had experienced some sort of fraud in the last 12 months.

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



More than three-quarters of corporations experienced fraud from an external, non-employee source, while a full one-third were unsure of where their fraud had originated from. Attempts by current or former employees had been experienced by over one in ten companies.

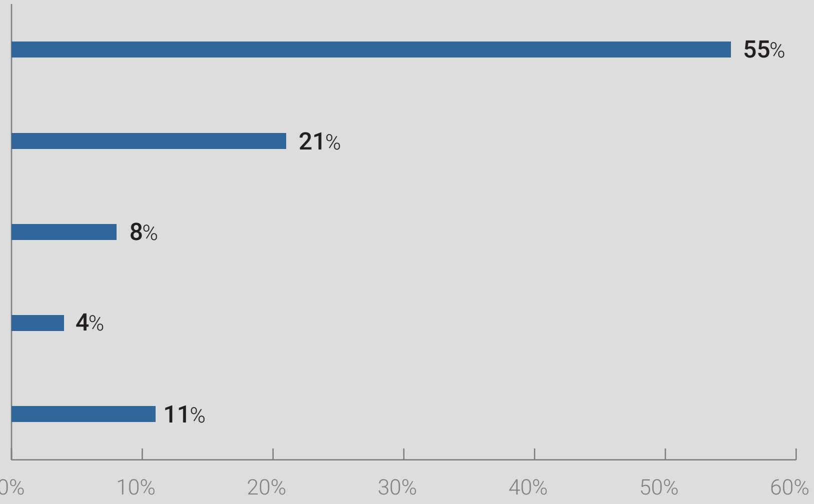
Thinking of the last 12 months, please label your company's experience with each of the following:



When looking at the frequency of attacks by fraud type, it appears that business email compromise (BEC Fraud) is the most common tactic employed by criminals against treasury.

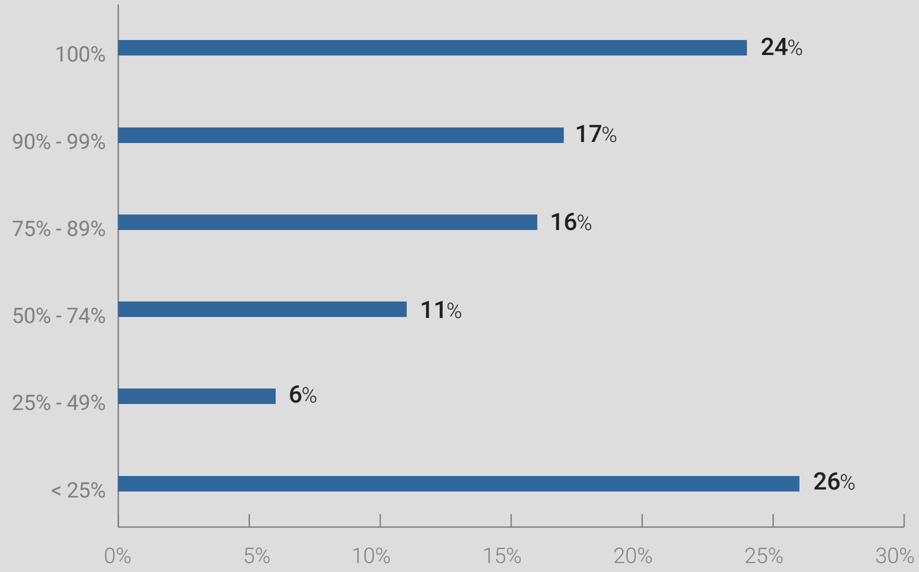
Bank Account Management

Our Bank Account Management process and records:



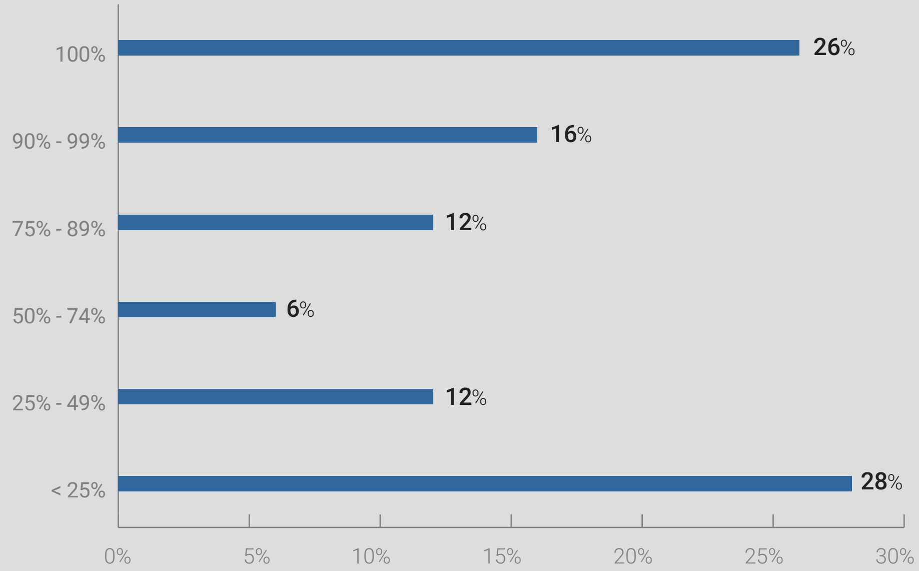
Over half of respondents said that both their bank account management process and records were current. Only 4% viewed both as out of date.

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



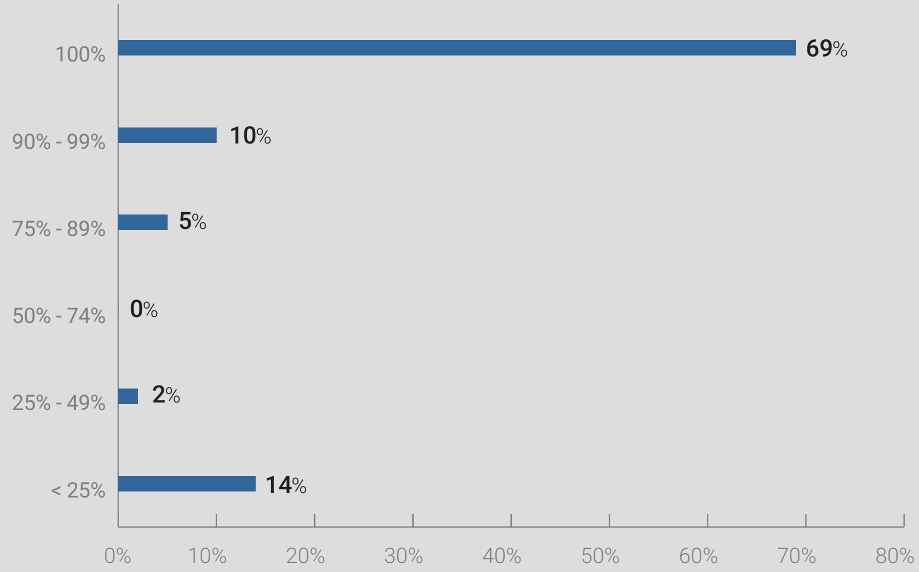
Overall, respondents' daily reconciliation capabilities were all over the map. In fact, almost equal portions were reconciling all their accounts daily vs. those reconciling less than a quarter of their accounts daily.

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



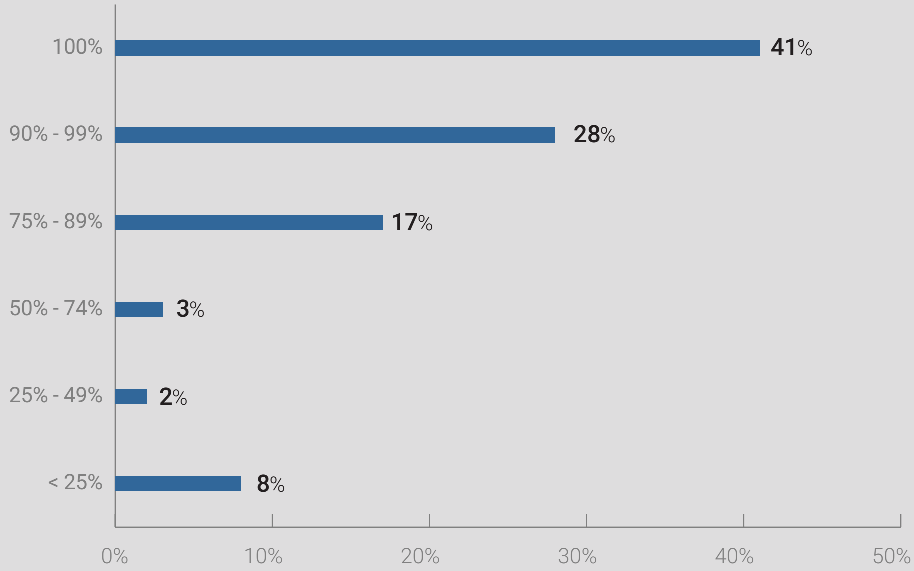
Weekly reconciliation follows a similar pattern to daily reconciliation. Across the board, reconciliation capabilities appear to be a mixed bag.

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



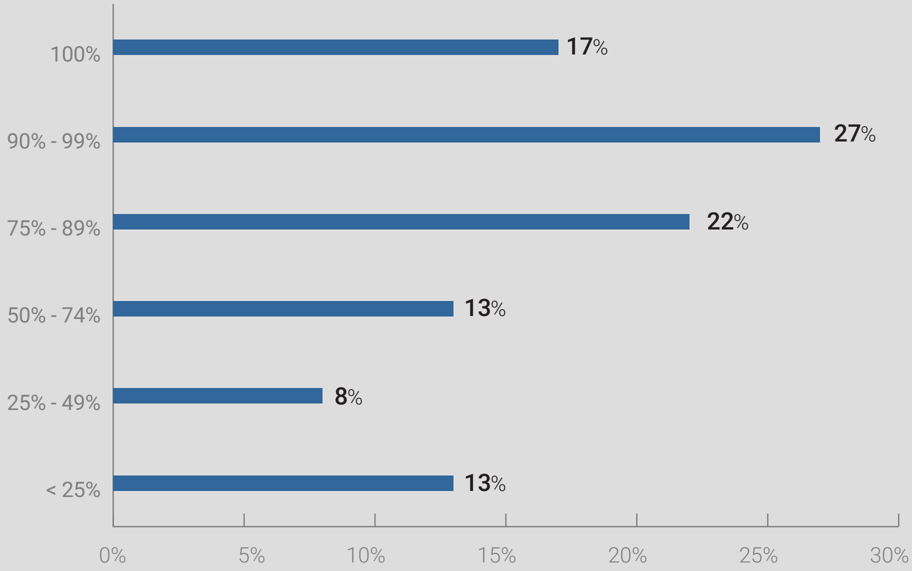
After one month, over two-thirds of respondents will have reconciled all of their accounts. However, this still leaves nearly one-third of the survey population without monthly reconciliation capabilities, which is concerning.

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



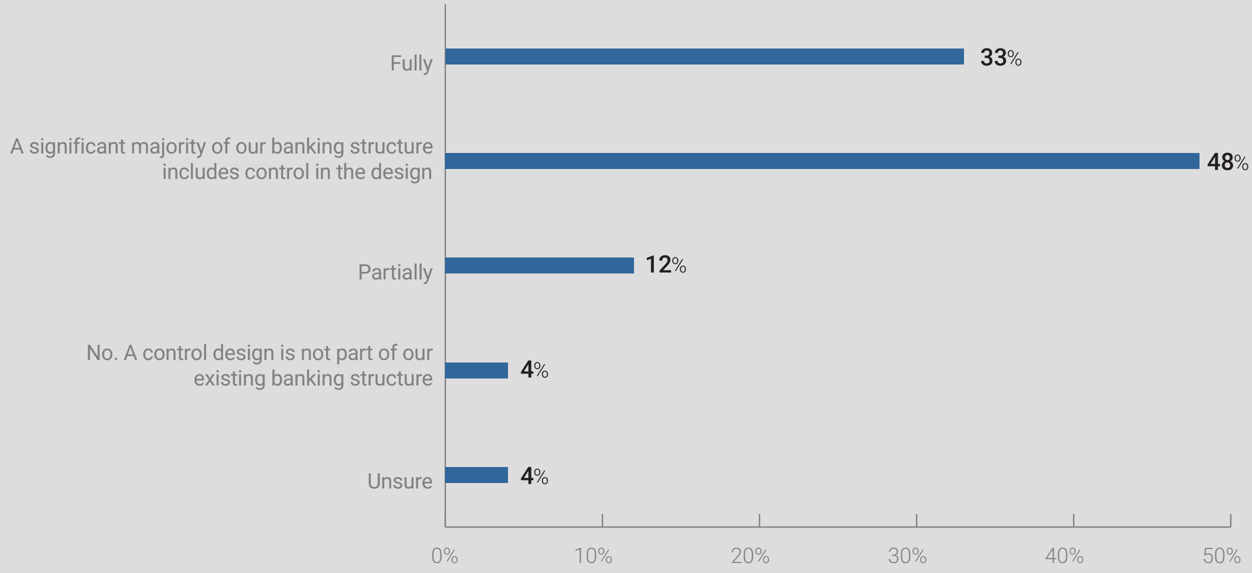
While over two-thirds of respondents maintained daily visibility to 90%+ of their accounts, 1 in 10 firms only had daily visibility to 50% or less of their accounts.

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



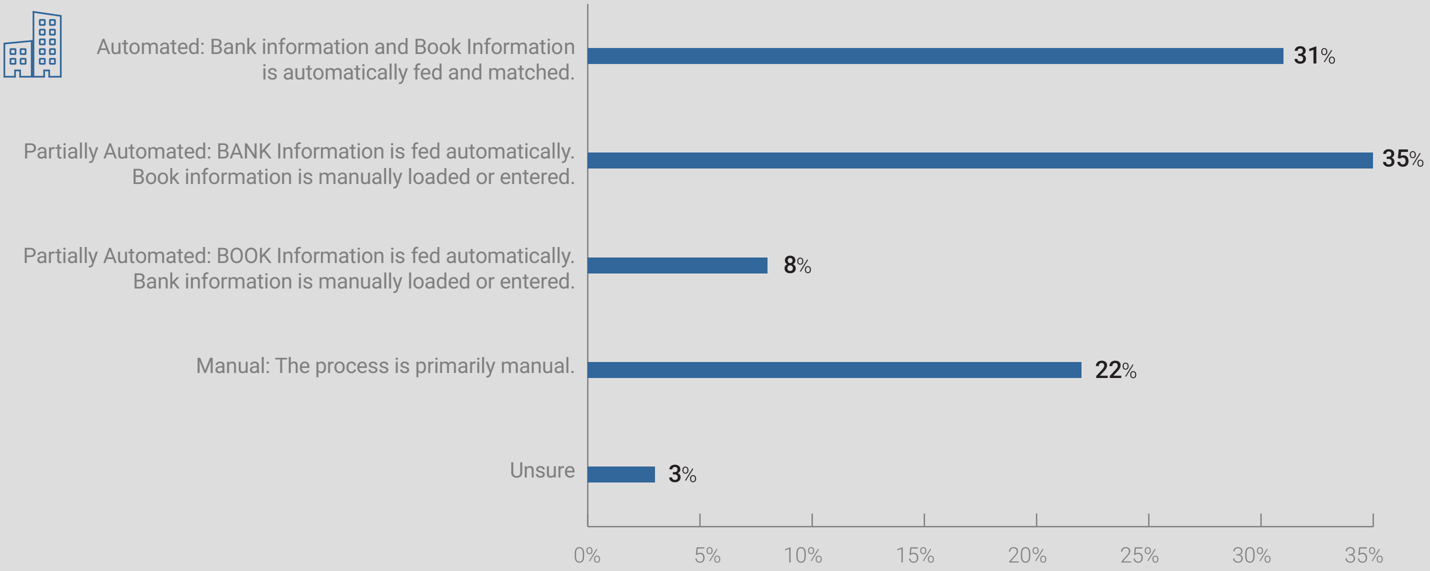
A significant majority (79%) of corporate respondents have more than 50% of their bank accounts connected to their core concentration bank account structure.

Does your banking structure intentionally reflect a control design?



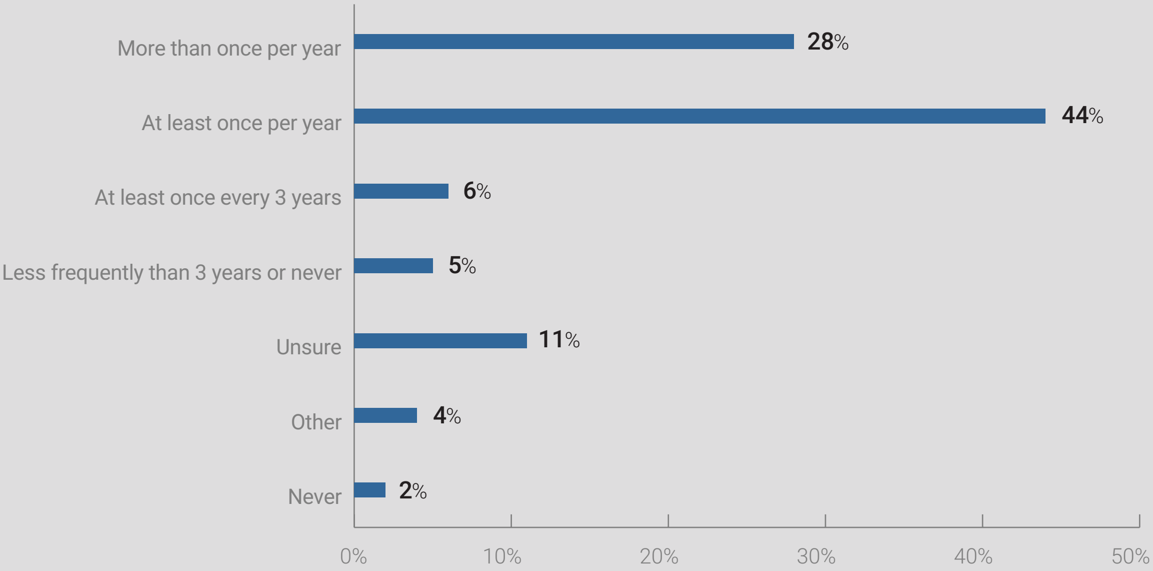
One-third of corporate respondents said that their banking structure fully and intentionally reflected a control design. Nearly half said that a significant majority of their banking structure reflected a control design.

For bank reconciliation, the following would most accurately describe our process:



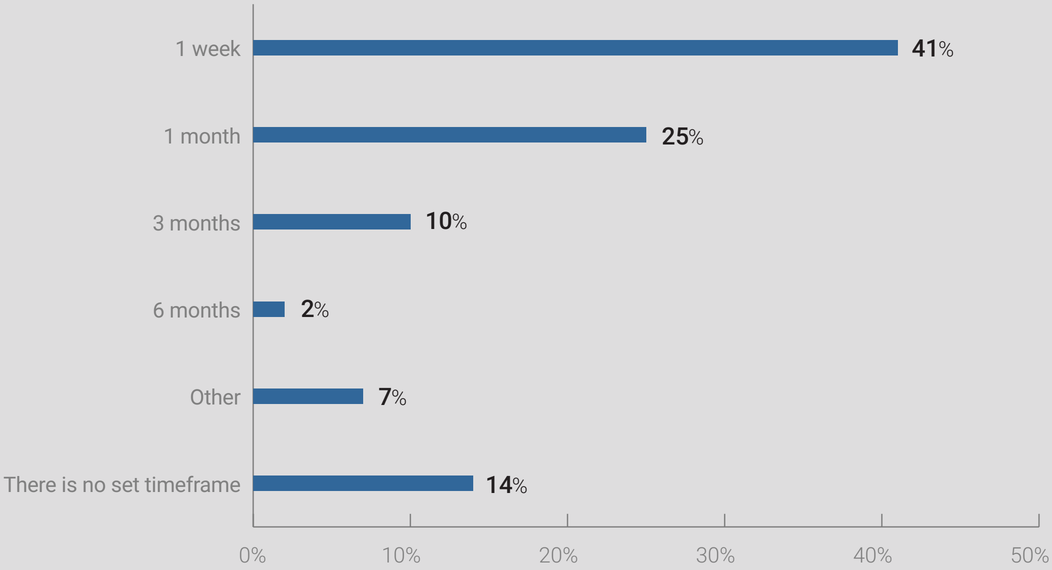
Nearly one-third of respondents had a fully automated reconciliation process, while a slightly larger portion (44%) only had partial automation. Just over one-fifth of respondents had manual reconciliation processes in place.

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



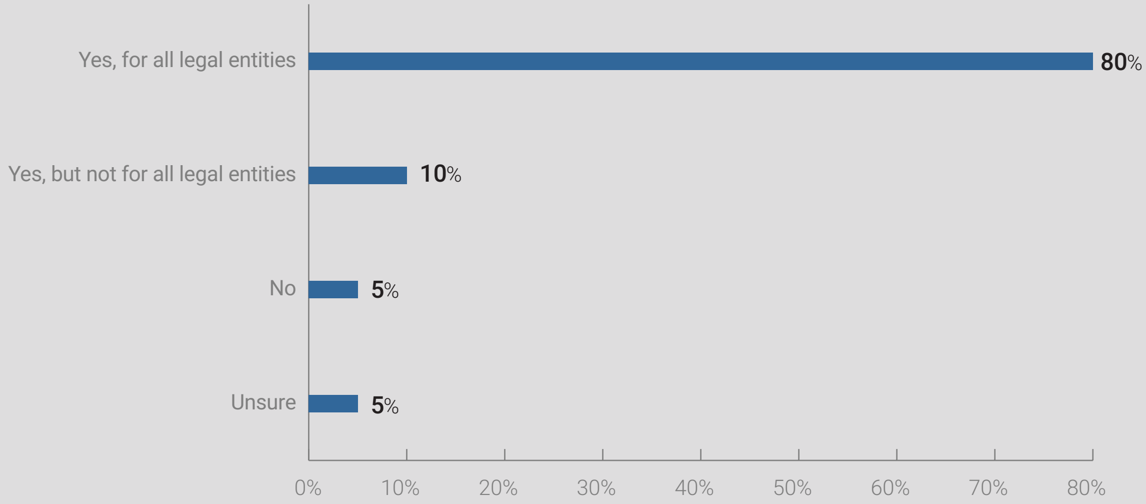
2% of organizations do not audit their bank's authorized signer records, and 11% were unsure of the auditing frequency. On the opposite end, 72% audited their signer records at least once every year.

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



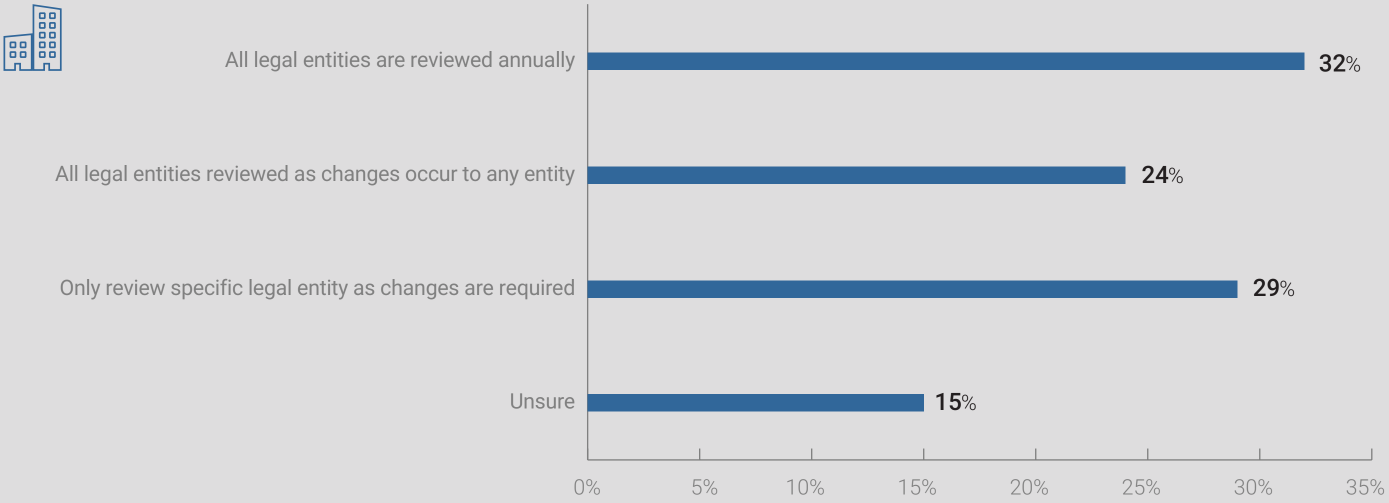
The majority of respondents updated their signer records within one month of an employee with signature authority leaving the company. However, 14% of firms had no set time frame for accomplishing this.

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?



A significant majority (90%) of the survey population have formalized banking resolutions defining who has signatory authority and how many of these signatories must be present.

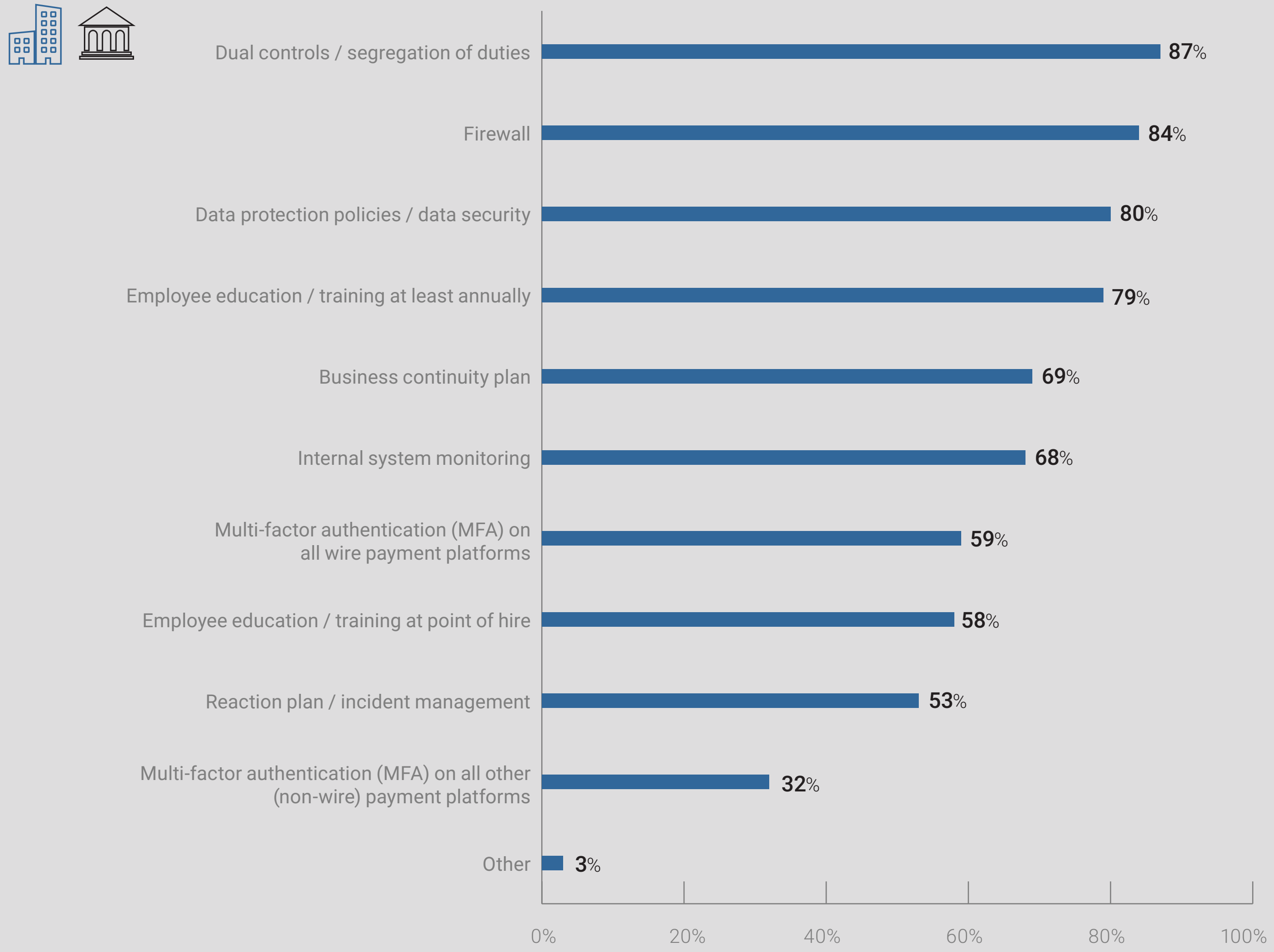
How often are your banking resolutions reviewed / updated?



Only 32% of corporate respondents reported that their banking resolutions are reviewed or updated annually for all legal entities.

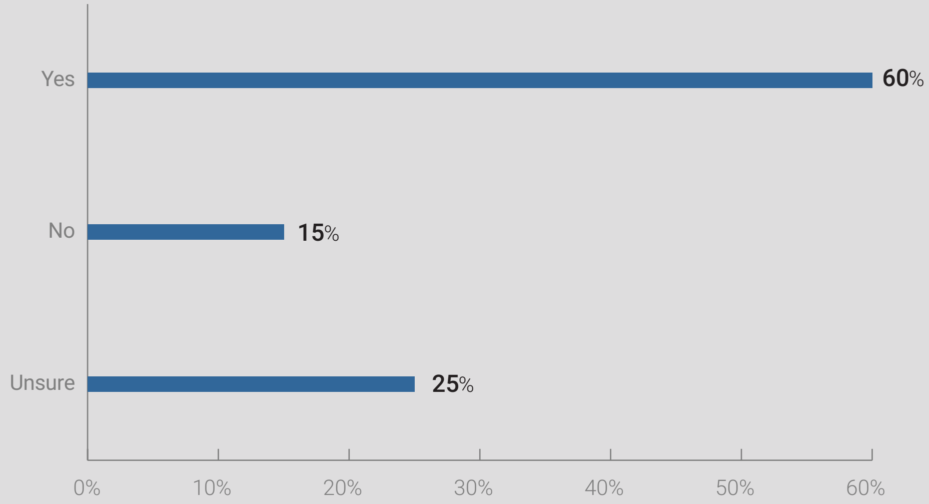
Control Framework

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



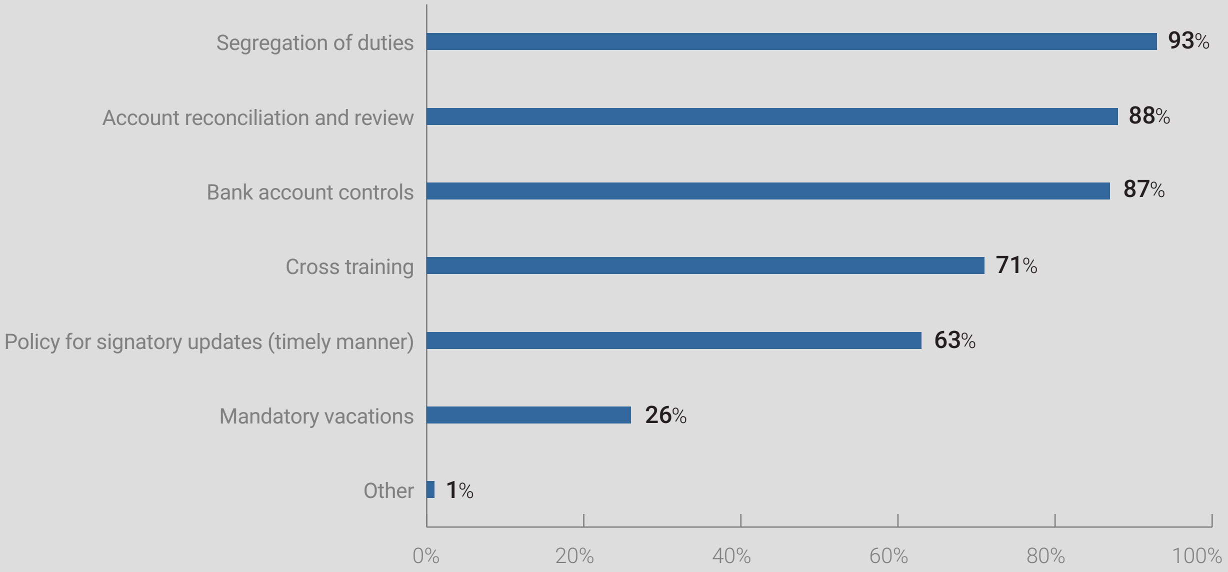
The majority of respondents were instituting more than one component of security as part of their control framework. However, only a few organizations were using every type.

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



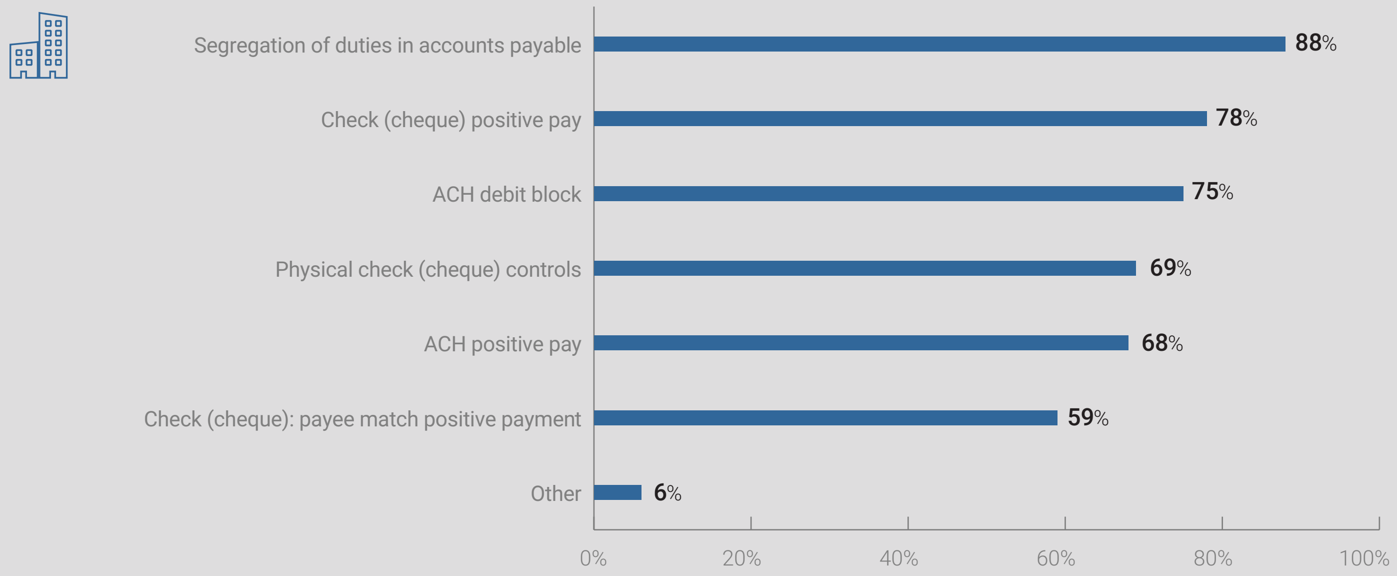
Nearly two-thirds of corporate respondents protect their losses against cyber fraud with insurance. 25% were unsure about their cyber fraud insurance status.

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



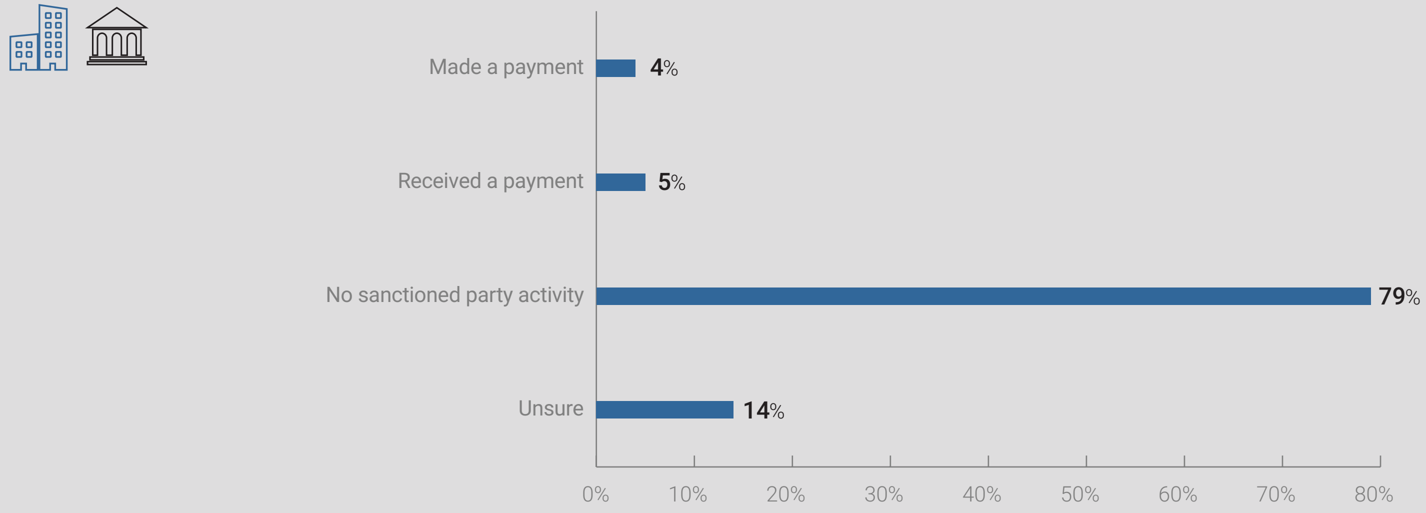
Approximately one-quarter of respondents utilize mandatory vacations to prevent employee fraud. Almost everyone used segregation of duties, account reconciliation and review, and bank account controls (93%, 88%, and 87% respectively).

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



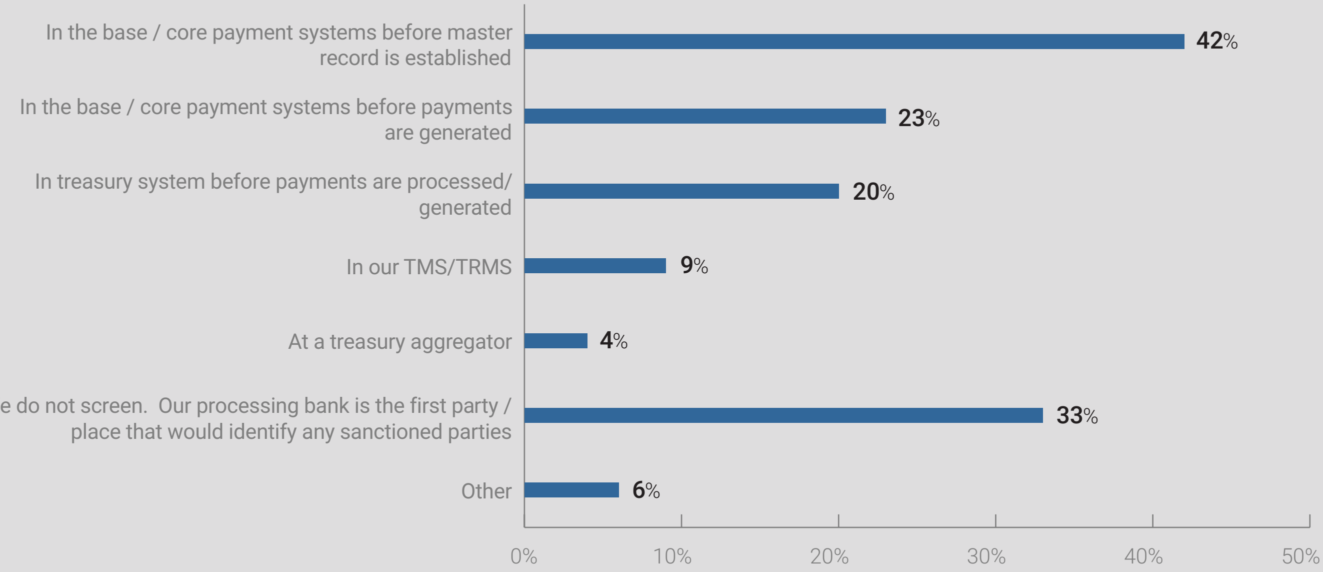
88% of corporates use segregation of duties in AP to help prevent payment fraud. Other top controls taken advantage of were check positive pay and ACH debit block.

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



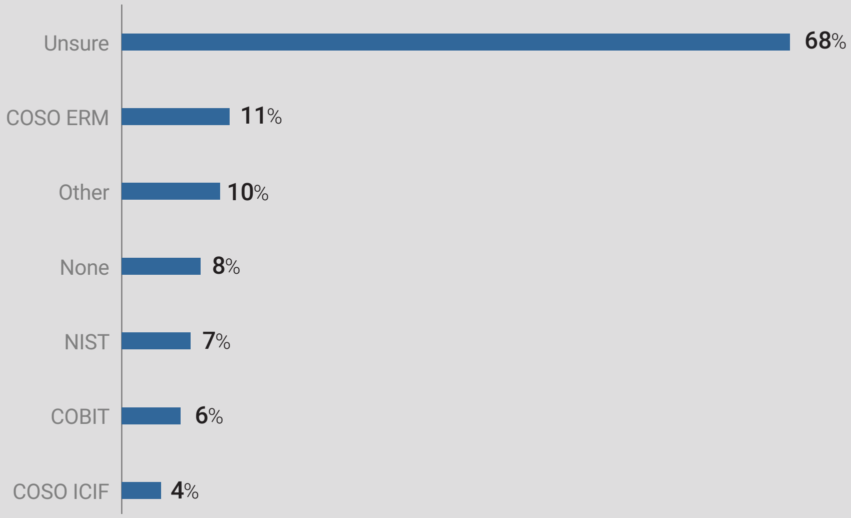
Less than 10% of organizations have made or received a payment from sanctioned parties in the last 12 months. 18% were unsure whether they had or not.

We screen for sanctioned parties: *(Select all that apply)*



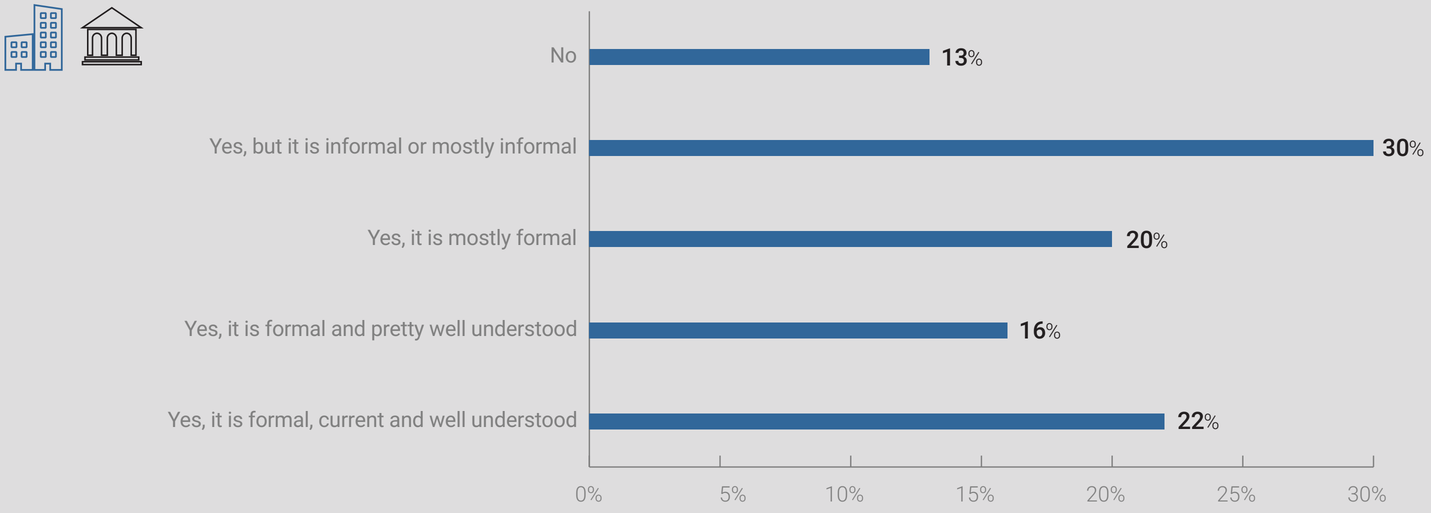
As it stands currently, approximately two-thirds of corporates have some form of sanctions screening process, while one-third do not screen for sanctioned parties at all.

We use the following control of IT control framework(s) *(Select all that apply)*



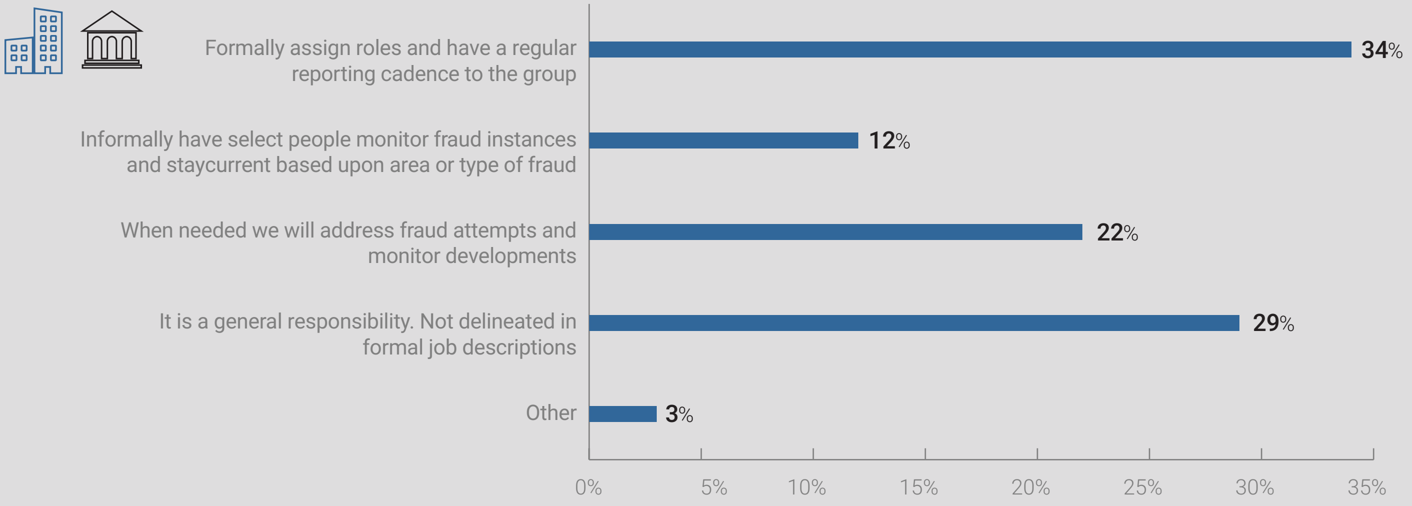
A majority of respondents (68%) were unsure which IT control framework they use. This large level of unsure responses could be due to this type of question being less treasury-based and more IT-based.

Do you have a treasury fraud and controls framework?



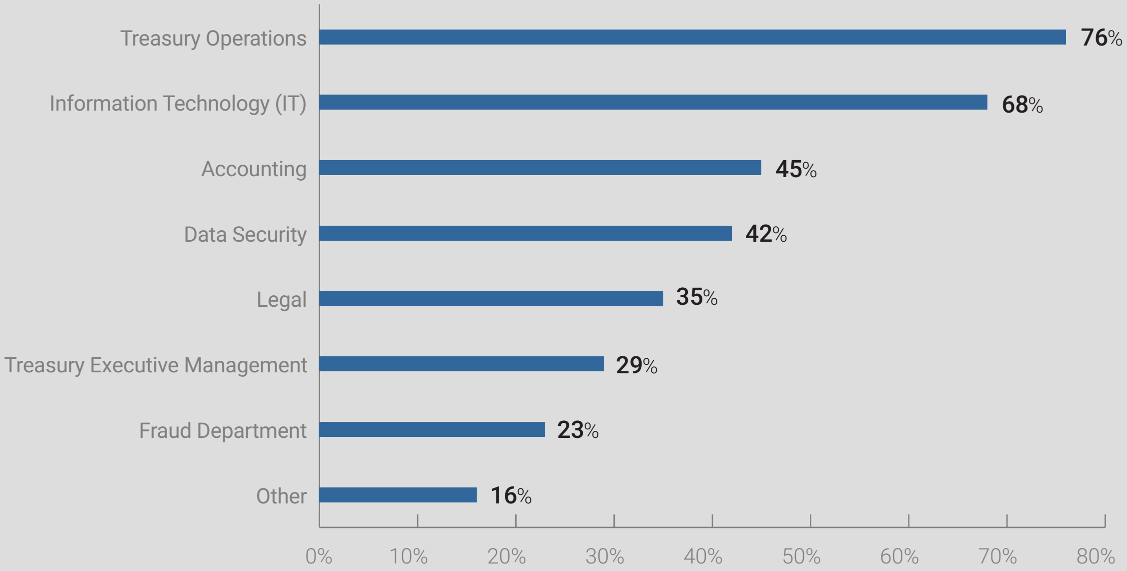
58% of respondents had a mostly formal or completely formal treasury fraud and controls framework. 43% only had an informal framework or did not have a framework at all.

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



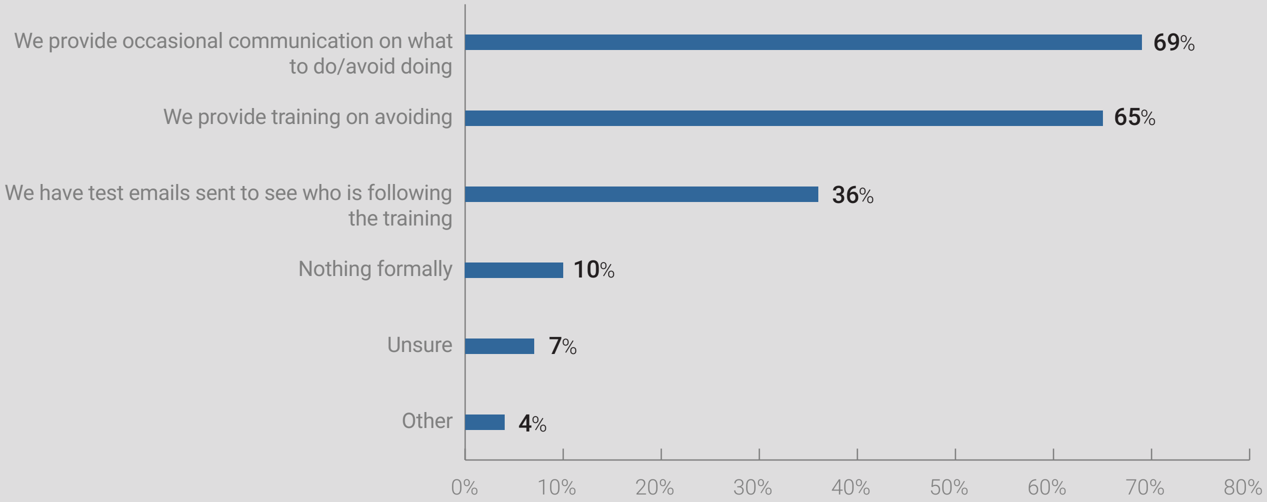
Only one-third of organizations had formally assigned fraud monitoring roles.

What areas have responsibility for tracking fraud and staying current on development? (Select all that apply)



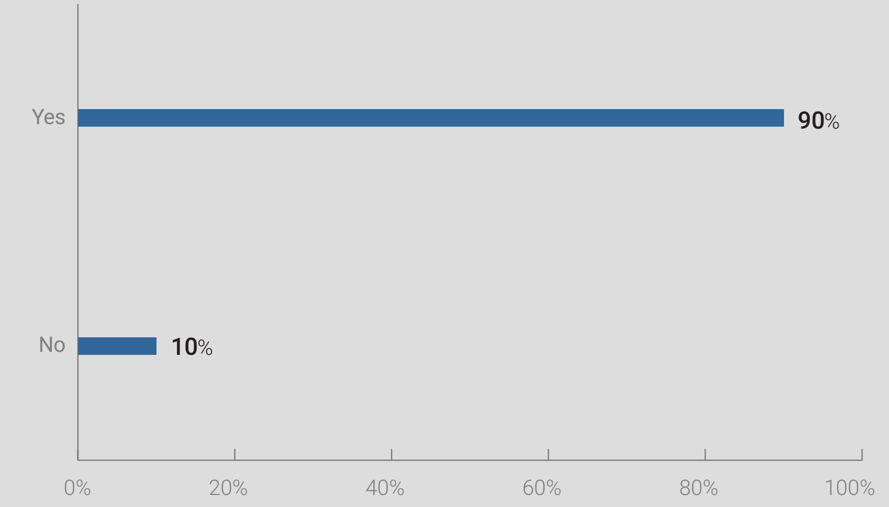
Treasury Operations and IT are overwhelmingly responsible for tracking fraud and staying current on development.

For managing spear phishing/clickbait attacks, we do the following (Select all that apply)



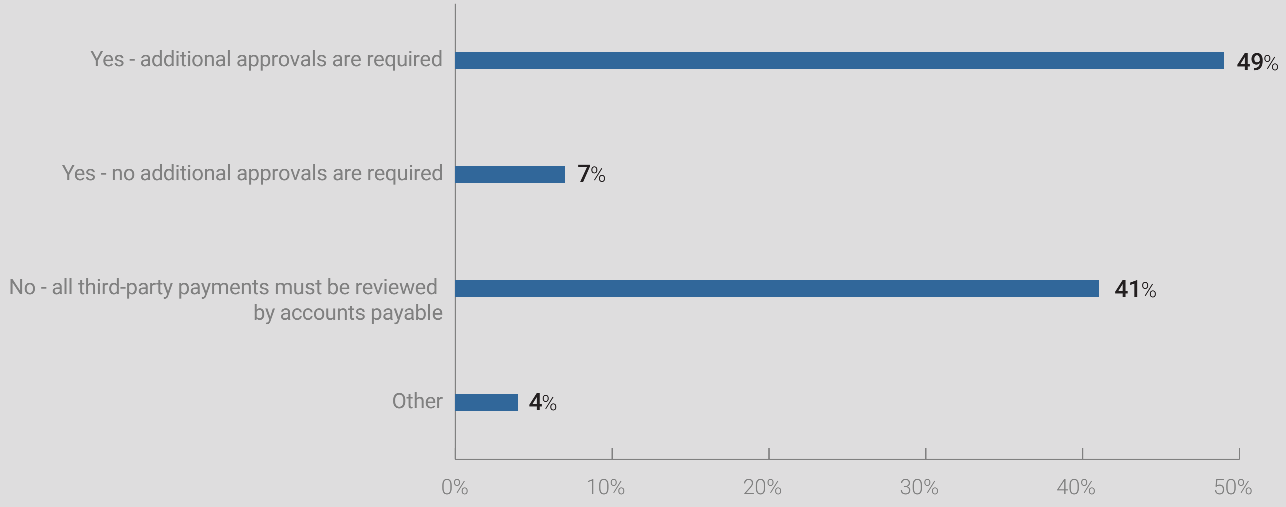
Almost two-thirds of corporates provide training on how to avoid phishing/clickbait attacks, and over one-third use testing emails to monitor employee susceptibility.

Does your organization require dual control for all transactions?



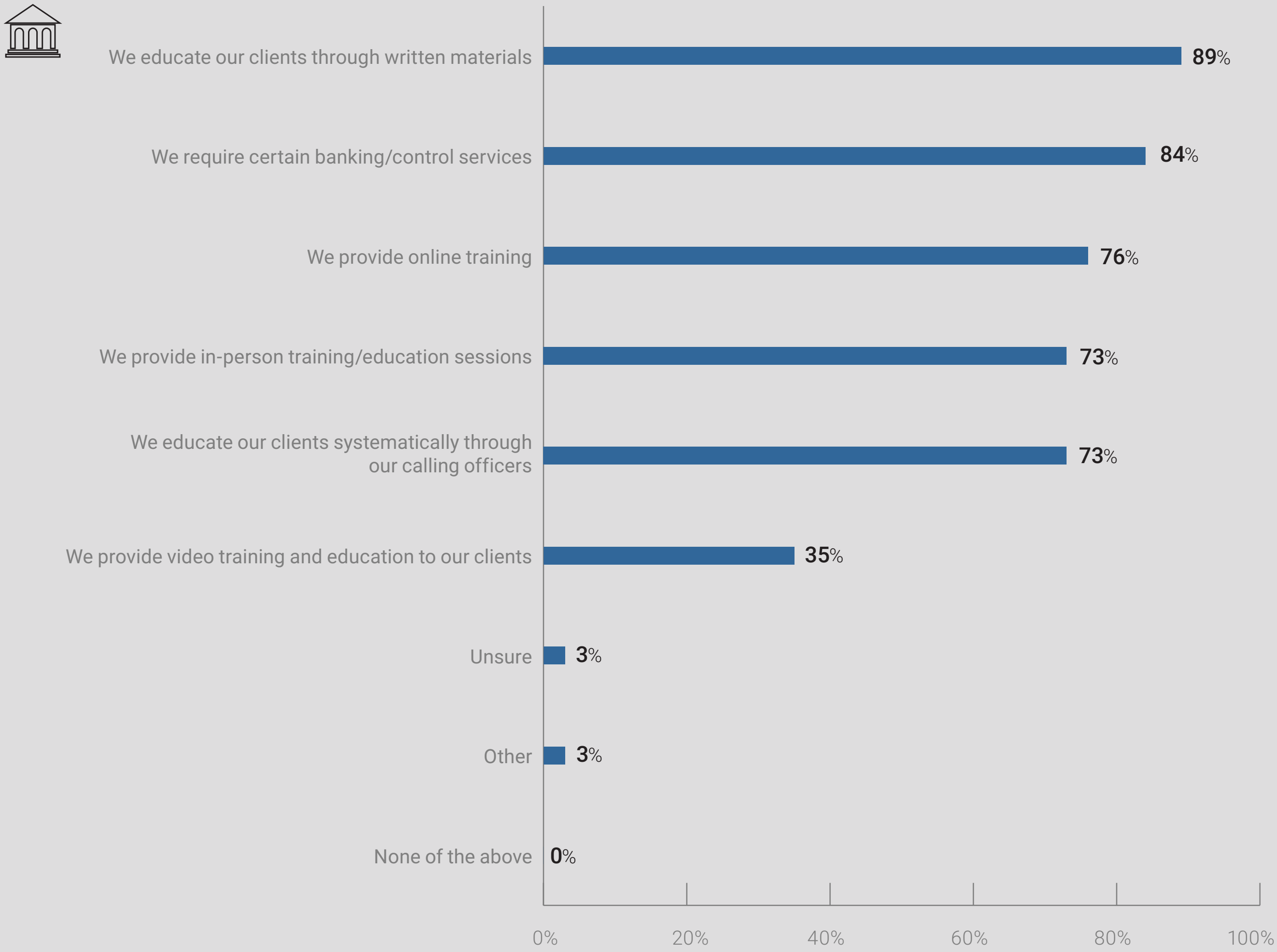
Almost all corporate respondents, 90%, require dual controls for all transactions.

Does your organization allow wires to be processed to third party accounts which have not been processed by the accounts payable process?



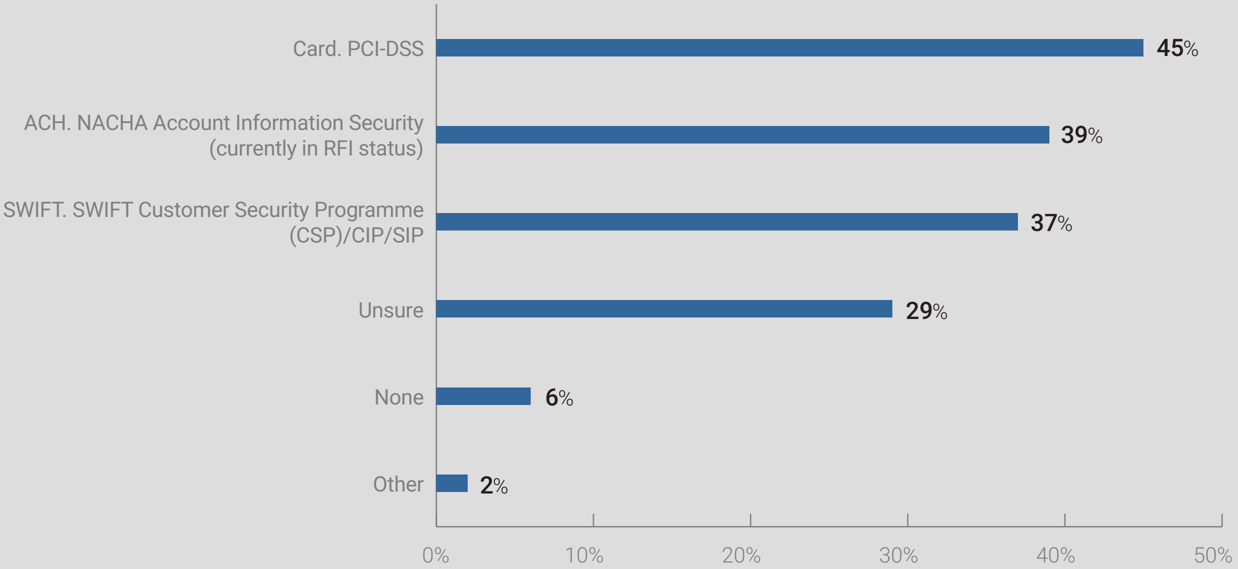
While a large portion of corporates are able to generate payments to third-party accounts without first going through AP, this process almost always involves additional approvals

How do you help your corporate clients detect and prevent fraud?
(Select all that apply)



Banks are stepping up their game to provide security and control for their clients. The two most popular components involve educating their clients through written materials and requiring certain types of controls and services to be purchased or used.

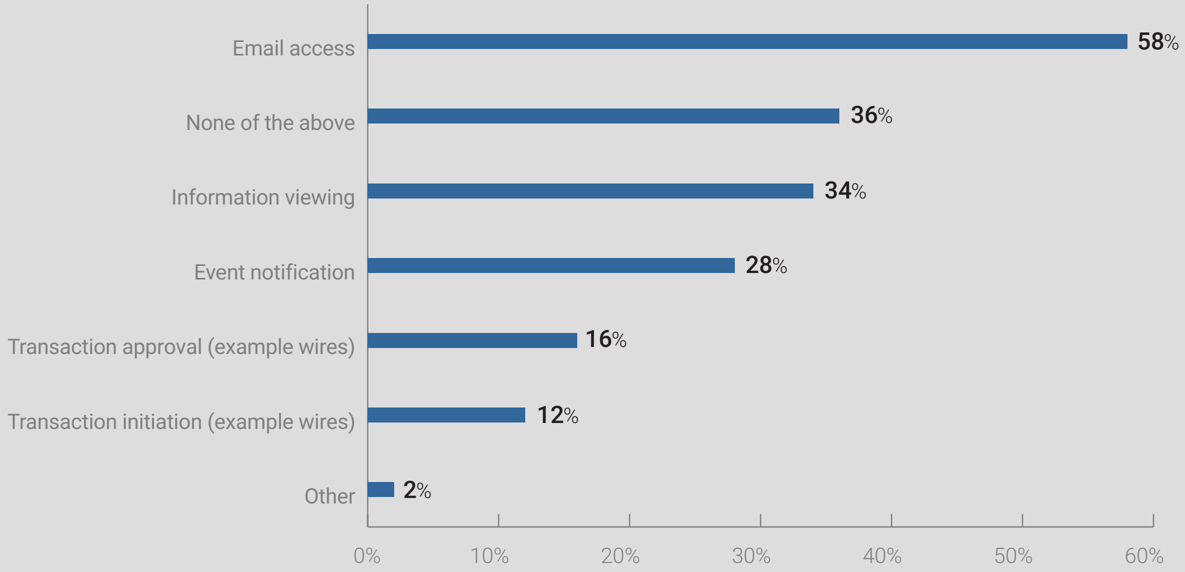
We are subject to the following compliance regulations or self-attestation or external testing review: *(Select all that apply)*



The survey population did not overwhelmingly have a specific compliance regulation that applied to them. In fact, 29% of respondents were unsure if any of these regulations applied to them, and 6% indicated that none of them did.

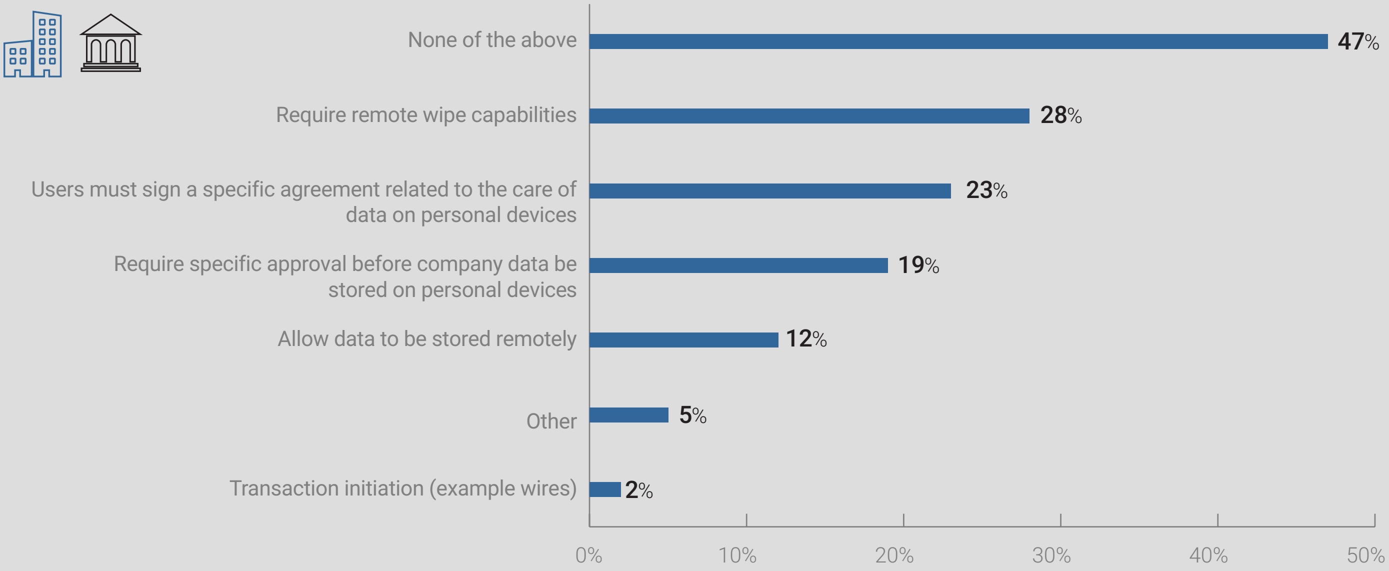
Technology Use

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



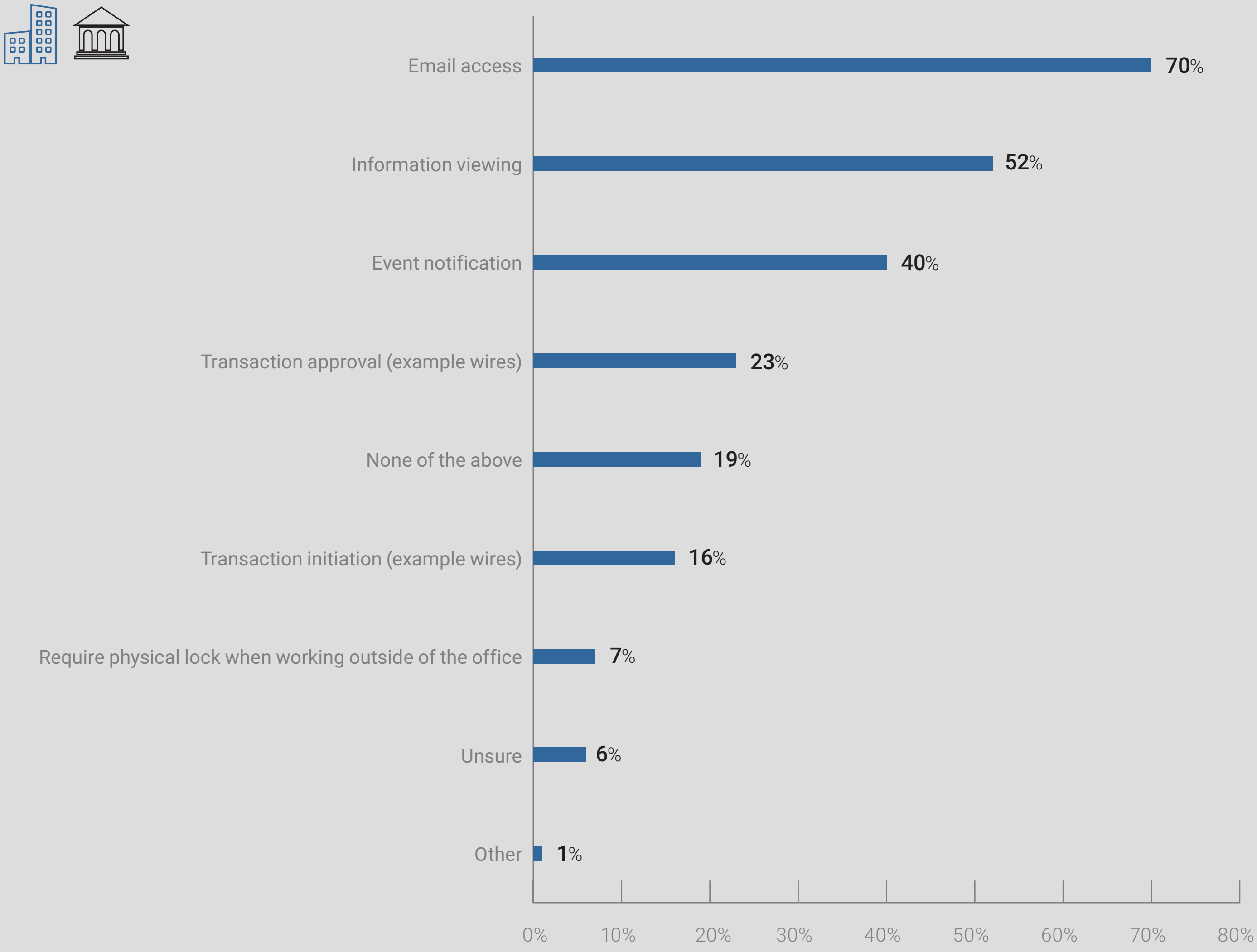
36% of the survey population doesn't allow treasury employees to use their own device for anything. Alternatively, 16% can use their own device for transaction approval and 12% can initiate transactions.

Bring Your Own Device. For company data that is stored on personal devices (i.e. smartphones) we: (Select all that apply)



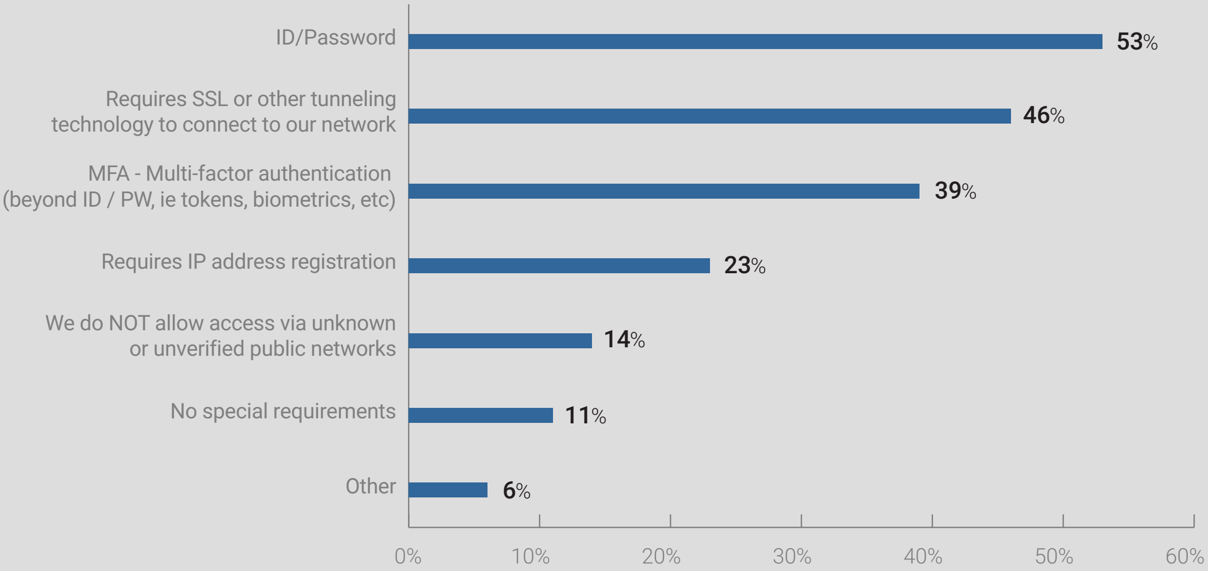
Even though there has been an uptick in BYOD, company security policies regarding these devices do not seem to have kept pace. In fact, nearly half of organizations do not require any additional controls in place to protect company data on personal devices.

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



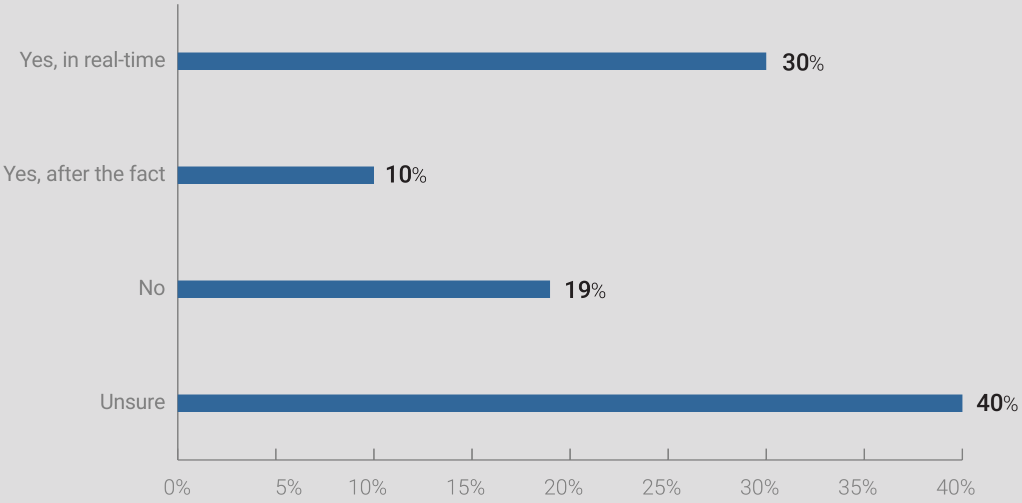
70% of organizations allow treasury to use their mobile device to check email. Other popular options for mobile use are information reporting and event notifications (52% and 40% respectively).

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



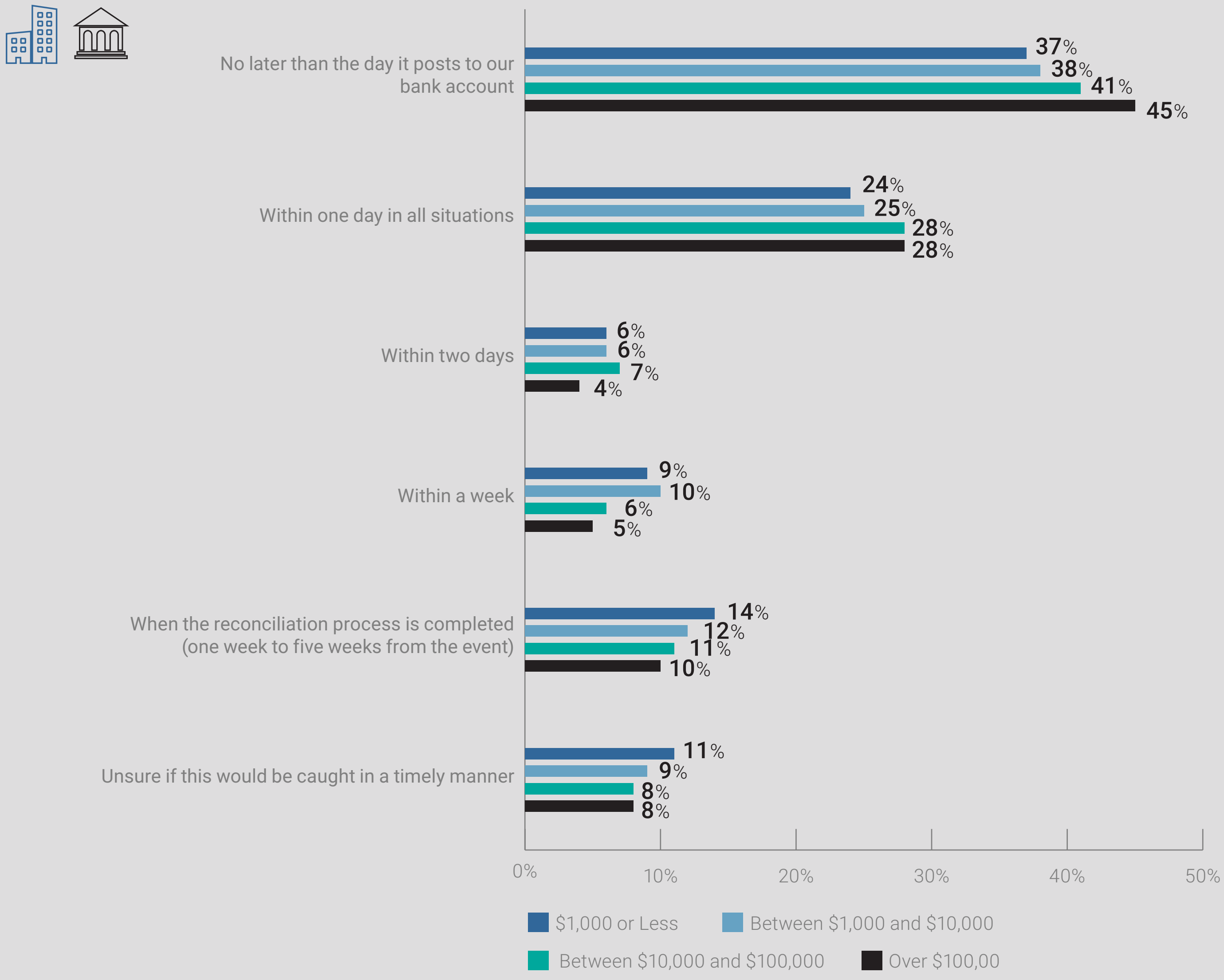
14% of the survey population does not allow the treasury department to remotely access their computers from unknown networks. Adversely, 11% allow remote access without any special requirements or controls.

Do you have technology implemented to proactively monitor anomalous or suspicious behavior within your system?



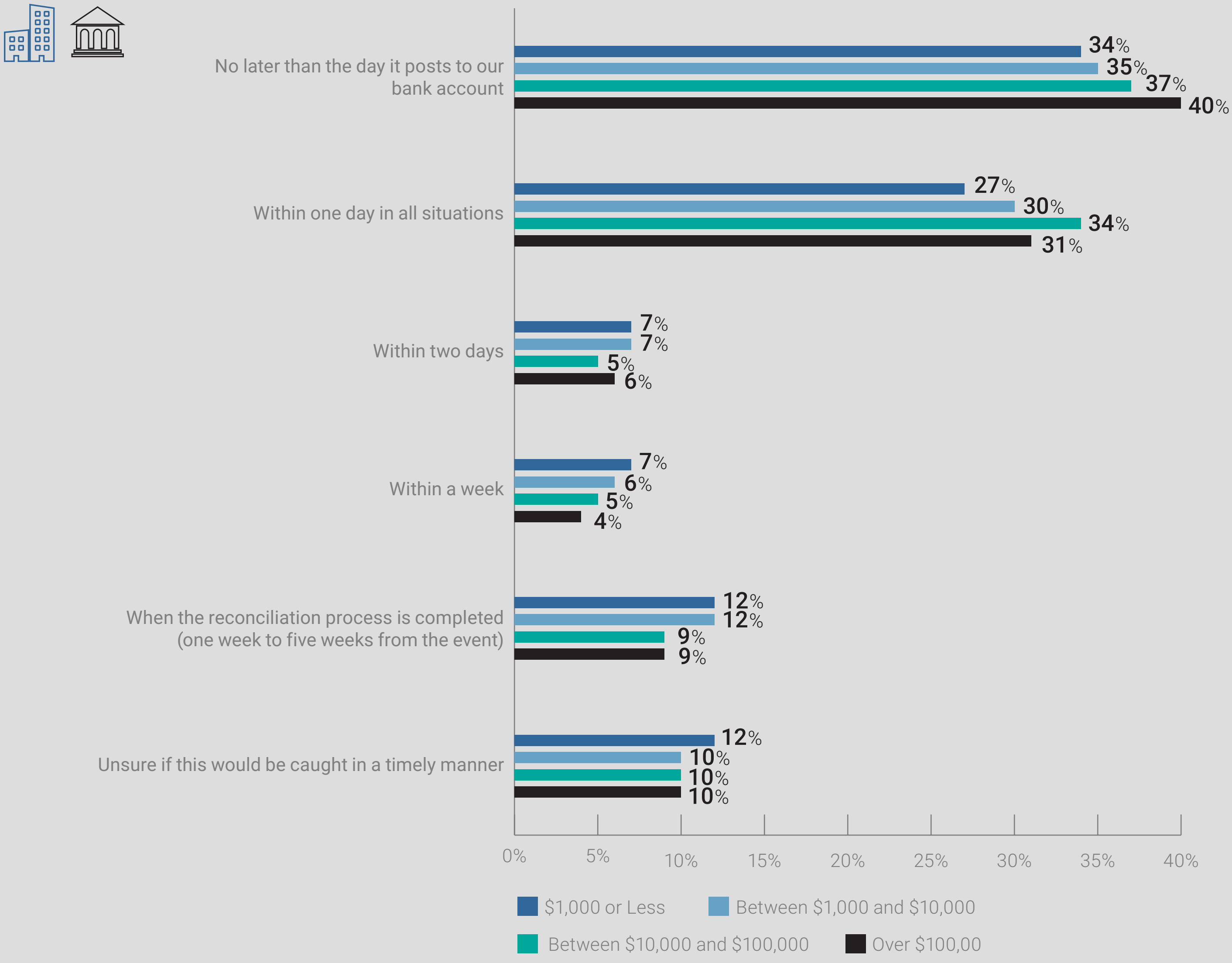
Respondents were split between having technology implemented to monitor anomalous behavior within their system and being unsure. Of those that had this technology, most had the ability to monitor in real-time.

How quickly will you detect and/or prevent Check/Cheque Fraud?



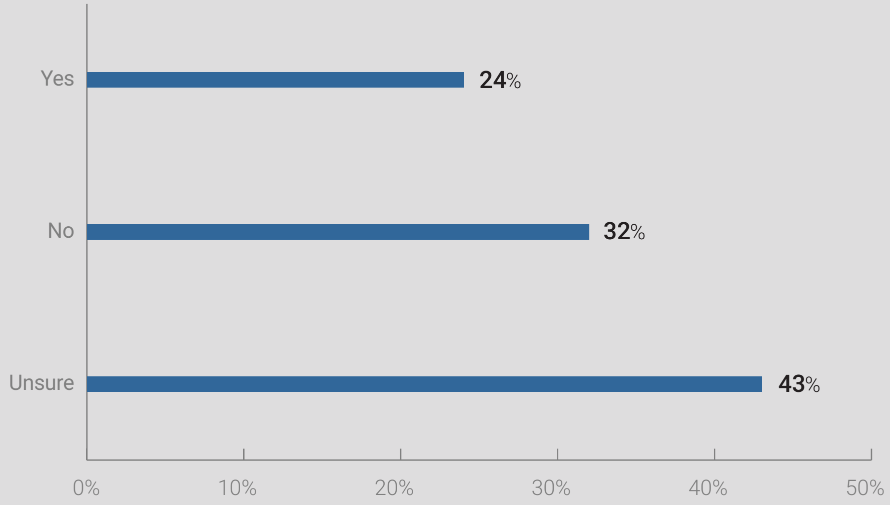
The majority of survey respondents were capable of detecting check fraud attempts within one day. However, nearly one in ten organizations were unsure if such attempts would be caught in a timely manner.

How quickly will you detect and/or prevent ACH or Wire Fraud?



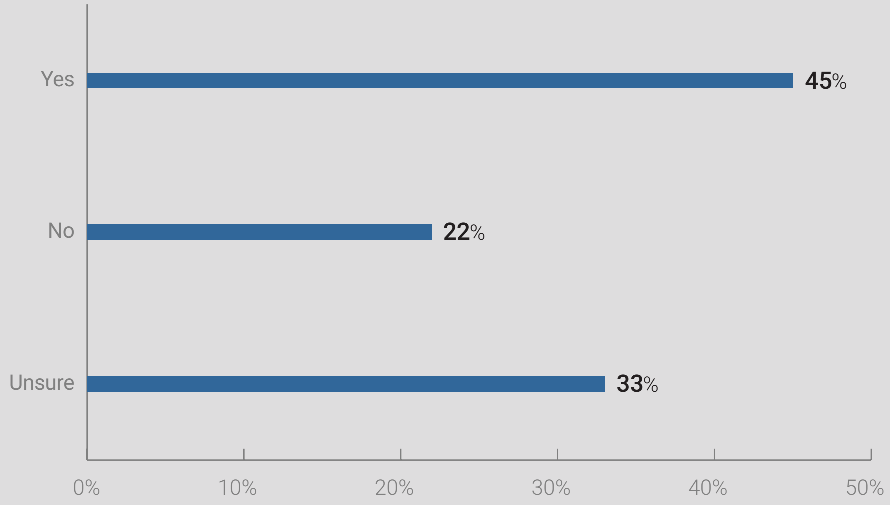
Similar to check fraud, while the majority of respondents were capable of identifying ACH/wire fraud attempts within one day, approximately one in ten firms were unsure if such attempts would be caught in a timely manner.

Do you require users with Bring Your Own Device (BYOD) to have remote wipe capability?



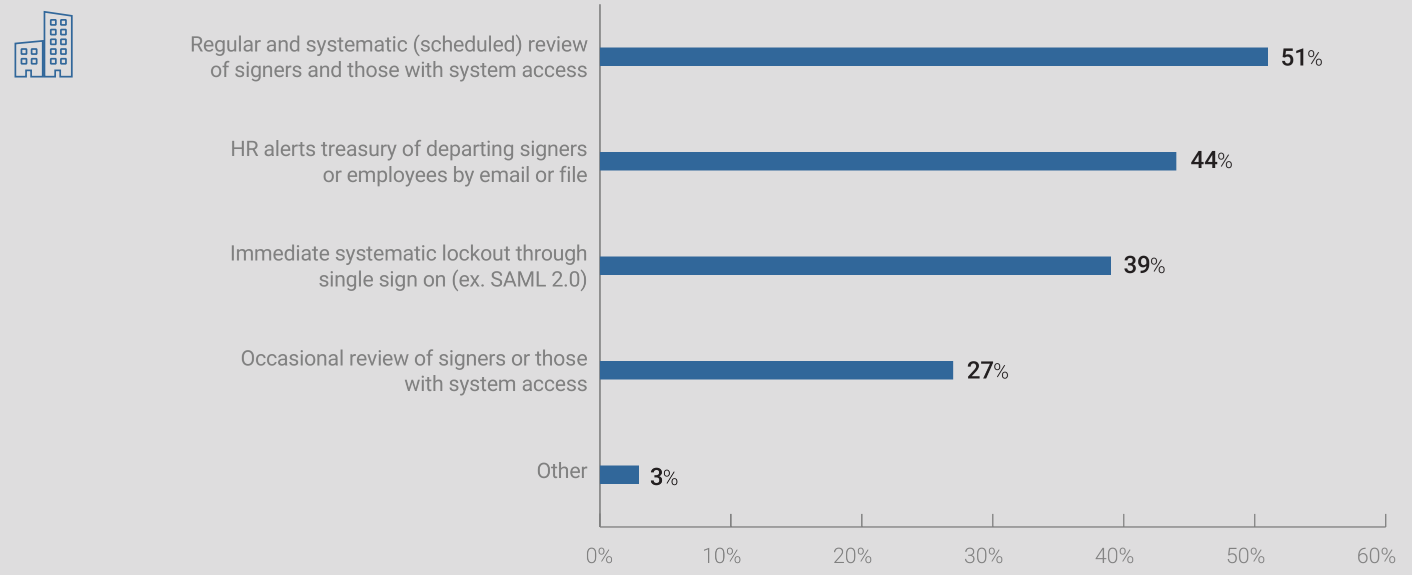
43% of the organizations were unsure if their company required them to have a remote wipe capability for their personal devices under BYOD policy.

Can you detect any ACH or Wire Fraud BEFORE it leaves the building?



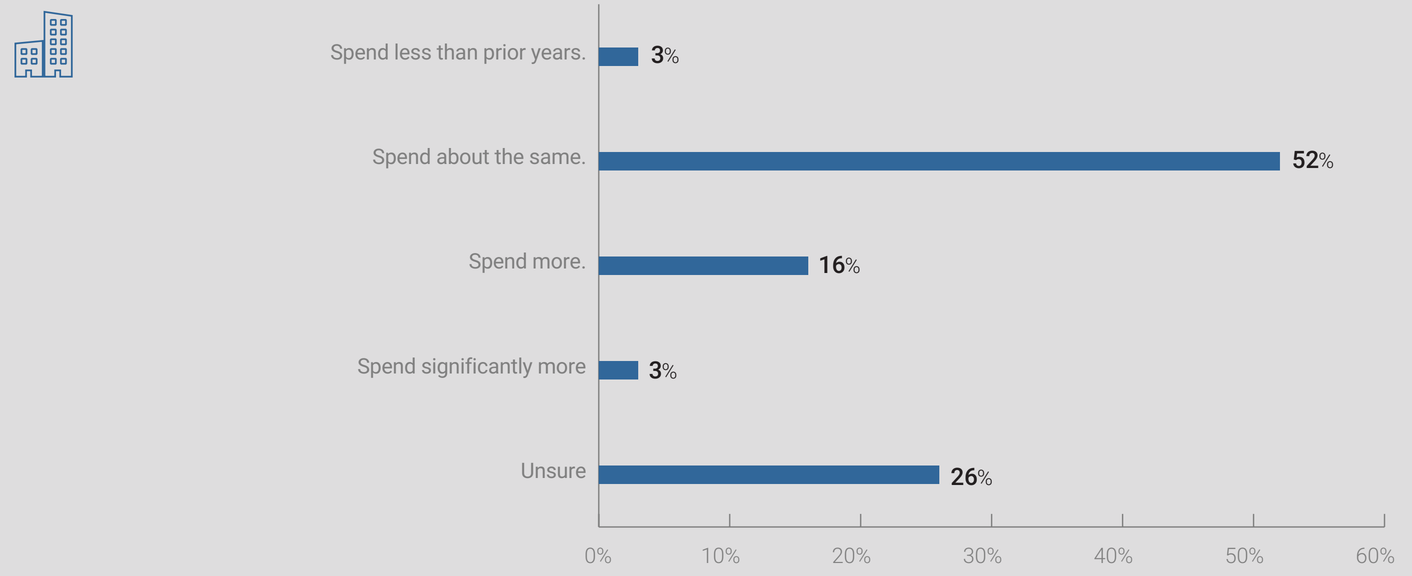
Detection of ACH fraud prior to leaving the building is a mix. 45% said they could detect this type of fraud, but 33% were unsure if this was possible.

If someone leaves the organization, then system access is removed from treasury / banking systems by *(Select all that apply)*



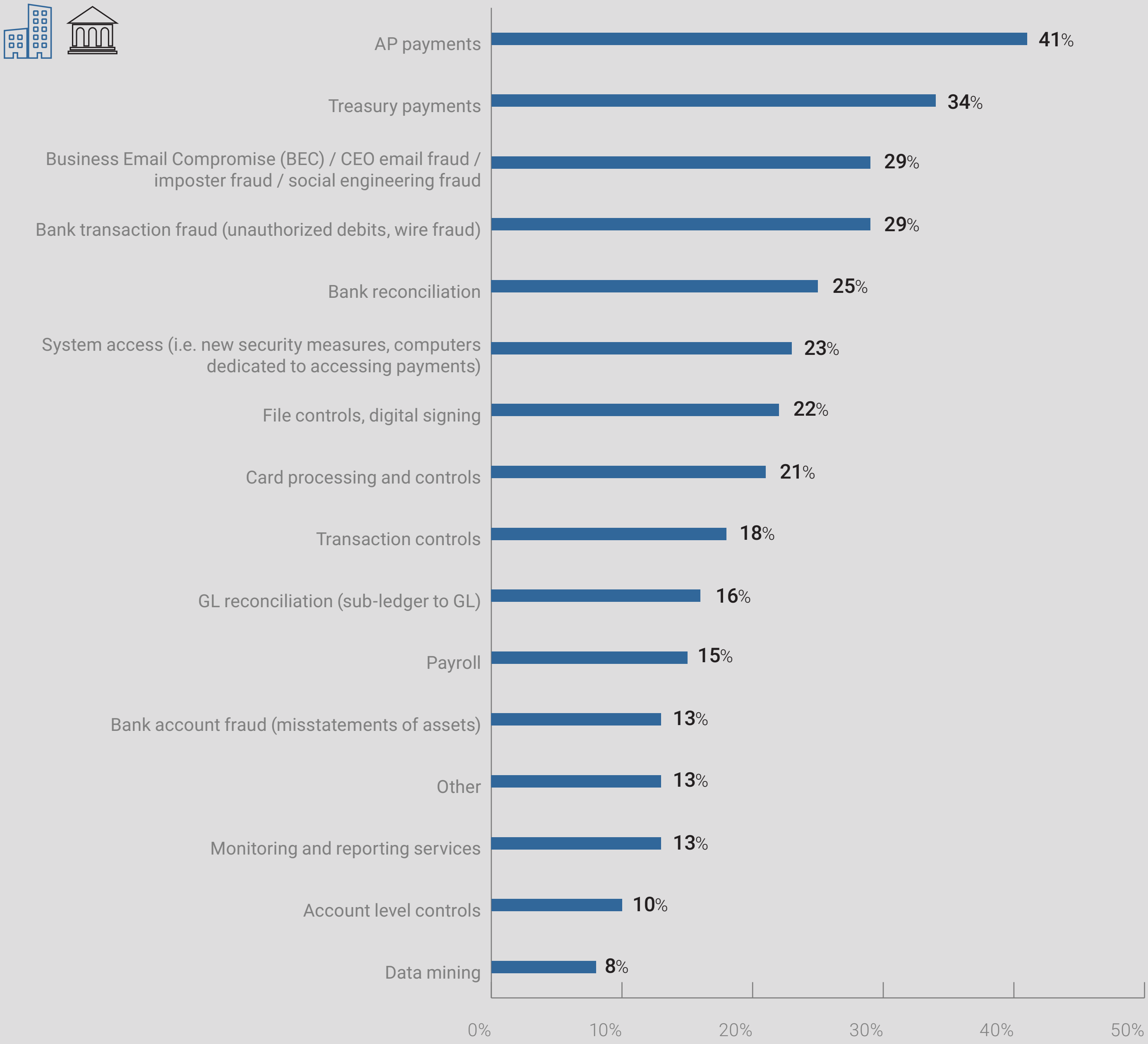
The most common way that corporates remove someone who has left their organization from their systems is through regular, scheduled system review. Only 39% have a plan in place for immediate system lockout.

What are your spending plans for treasury fraud prevention, detection, and controls?



Including "unsure" responses, 19% of corporations plan to spend more on preventing, detecting and controlling fraud. Only 3% plan to spend less.

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



The most common areas that the survey population plans to invest in is AP payments and treasury payments. However, there are a wide variety of security components being invested in and implemented.

About the Organizations

BOTTOMLINE TECHNOLOGIES

Bottomline Technologies (NASDAQ: EPAY) helps make complex business payments simple, smart, and secure. Corporations and banks rely on Bottomline for domestic and international payments, efficient cash management, automated workflows for payment processing and bill review, and state of the art fraud detection, behavioral analytics and regulatory compliance solutions. Thousands of corporations around the world benefit from Bottomline solutions. Headquartered in Portsmouth, NH, Bottomline delights customers through offices across the U.S., Europe, and Asia-Pacific. For more information visit *www.bottomline.com.*

Bottomline Technologies®

+1 800.243.2528
bottomline.com
info@bottomline.com

STRATEGIC TREASURER

Since 2004, Strategic Treasurer has helped hundreds of corporate clients face real world treasury issues. Our team of senior consultants is comprised of former practitioners with actual corporate treasury experience who have "hopped the desk" to support their former peers from the consulting side. Strategic Treasurer consultants are known not only for their expertise in the treasury space, but also for their responsiveness to client issues, thorough follow-through on each project, and general likability as temporary team members of your staff.

Our focus as a firm centers on maintaining true expertise in the treasury space. Through constantly refreshing our knowledge and intentionally learning about leading solutions, we ensure that our understanding is both global in scope and rich in detail.

STRATEGIC TREASURER
Consultants in Treasury

+1 678.466.2220
strategictreasurer.com
info@strategictreasurer.com