General Report

2019 TREASURY FRAUD & CONTROLS SURVEY REPORT

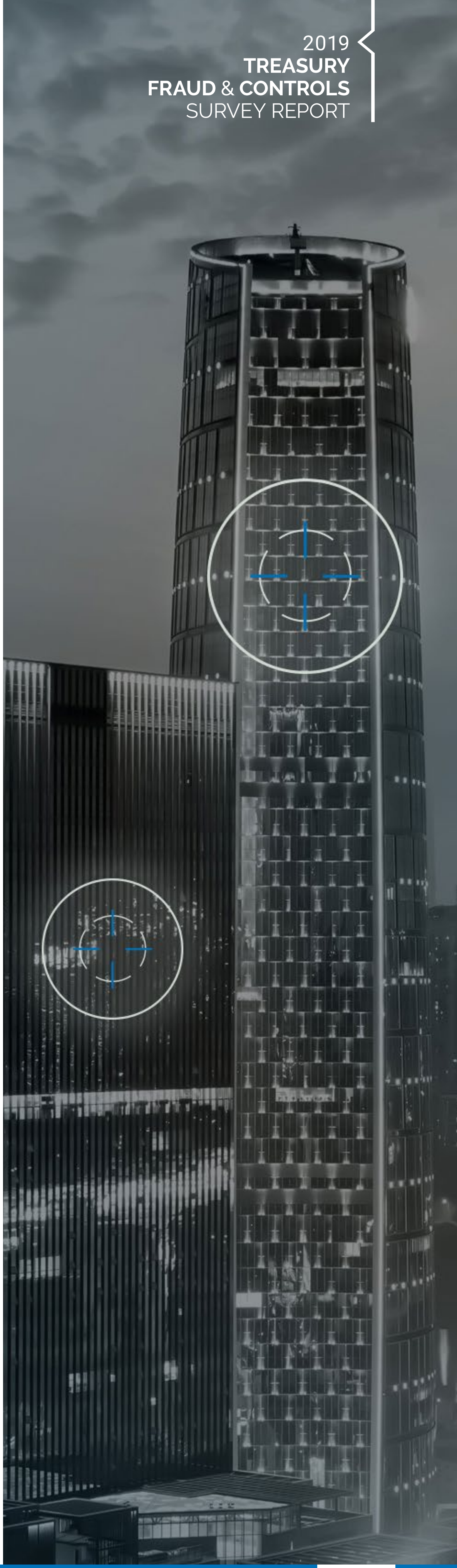
Fraud Experiences & Exposures • Security Controls & Spend • Bank Account Management

Sponsored by

Bottomline

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

KEVIN PEAK
Senior Consultant
kevin@strategictreasurer.com

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

Executive Summary

Today, protecting any organization against sophisticated, persistent, and changing fraud attacks falls heavily on treasury and IT. This responsibility is warranted, as liquid assets and financial data have become increasingly common targets for criminals. And given treasury's authority over a broad range of cash management, payment, and bank account operations, their leadership on security is vital.

For the 4th year running, Strategic Treasurer and Bottomline Technologies have partnered to develop a comprehensive market research initiative covering the realm of treasury fraud and controls. This year, our research has uncovered vital insights related to the fraud environment. While nearly a dozen specific findings are presented and analyzed within this report, the overall storyline of this year's study can be summarized in three quick points:

Heightened Security Spend Results in Greater Corporate Confidence

Despite practitioners' recognition that the threat of fraud continues to increase year-over-year, their elevated security spend and focus has resulted in improved levels of confidence regarding security controls and policies.

Fraudulent Activity Remains Widespread, But Losses Hold Steady

Although criminal activity remains elevated and more organizations experienced fraud over the past year than those that didn't, the number or percentage of firms that experienced losses has not increased from previous years.

Security Controls Have Grown Stronger, But More Work is Needed.

A multi-year trend of corporate investment and focus on security is positively impacting corporates' ability to prevent fraud. However, significant exposures remain. The fight against fraud is ongoing, and defenses must be fortified by strengthening both the technical and human elements.

While the above represents a consolidated view of the material covered in this report, we invite you to continue reading to explore a full range of specific insights and analysis. We thank Bottomline for their partnership in underwriting this survey and extend our deep appreciation to all who took the time to complete it. This data allows us to better gauge the impact of various fraudulent attacks and enables us to focus our investments and energy in order to increase our profession's effectiveness in protecting financial assets and information.

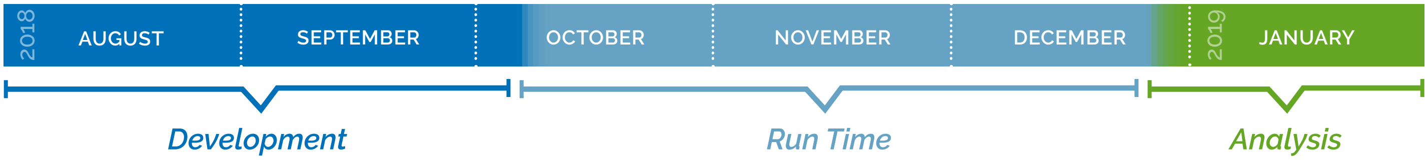
Craig Jeffery, FLMI, CCM
Founder & Managing Partner
Strategic Treasurer

James Richardson
Head of Market Development
Bottomline Technologies

Christopher Gerda
Risk & Fraud Prevention Officer
Bottomline Technologies

About the Survey

SURVEY PLANNING & ANALYSIS CYCLE



2018 AUGUST | SEPTEMBER | OCTOBER | NOVEMBER | DECEMBER | 2019 JANUARY

Development *Run Time* *Analysis*

SURVEY FACTS & FIGURES

~275 respondents

4th annual year of research

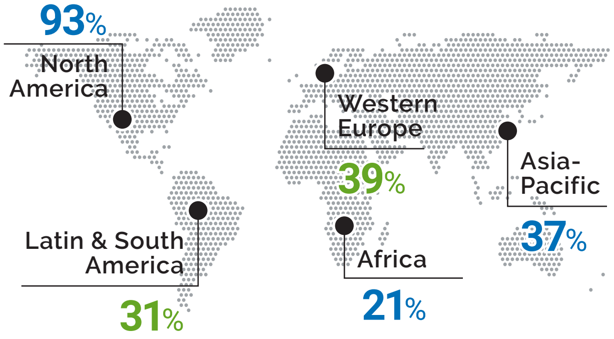
100+ questions

10 week survey runtime

TOP CORPORATE RESPONDENT ROLES

31%	Treasurer/AT/Director
27%	Treasury/Cash Manager
16%	Treasury Analyst
7%	C-Suite

RESPONDENT REGIONS OF OPERATION



North America	93%
Western Europe	39%
Asia-Pacific	37%
Latin & South America	31%
Africa	21%

KEY AREAS OF FOCUS

- What is the rate at which organizations are experiencing fraud?
- What types of fraud are most prominent?
- How and where are organizations investing in security, and what is the overall impact of these investments?
- What are the strongest and weakest areas of organizations' security?

QUICK STATS

73% of corporates believe the threat of fraud has increased in the past year.

64% of corporates train their employees on security at least annually.

26% of corporates reconcile 90%+ of their bank accounts on a daily basis.

12% of corporates currently leverage biometrics as a form of security.

Key Findings At-a-Glance

1 CORPORATE CONFIDENCE IN SECURITY GROWS *(Page 6)*

Although corporates have indicated for several years that they believe the threat of fraud is increasing, practitioners have still grown increasingly confident in their security controls.

3 WHAT TYPES OF FRAUD ARE MOST PROMINENT TODAY? *(Page 8)*

There are three specific types of fraud (Business Email Compromise, Cyber/Data Theft, and Check Forgery) that are initiated much more frequently than the rest.

5 WHAT AREAS OF SECURITY ARE CLEARLY LACKING? *(Page 10)*

Although we have witnessed dramatic improvements in corporate security over the past several years, exposures across areas such as data encryption and "principle of least privilege" policies still pose serious threats to organizations.

7 TIMELY BANK ACCOUNT VISIBILITY & RECONCILIATION ARE VITAL *(Page 12)*

With payments increasingly settled same-day if not in real-time, the need for enhanced bank account visibility and reconciliations features are more pronounced than they've ever been.

9 USER MONITORING SOFTWARE: WHAT IS IT & HOW DOES IT HELP? *(Page 14)*

User monitoring software has proven adept at detecting suspicious actions that occur within internal systems and alerting administrators of this activity before the organization experiences a data-related breach or financial loss.

2 MULTI-YEAR CORPORATE SECURITY FOCUS PAYING OFF *(Page 7)*

After a multi-year trend of significant corporate spend and focus on security, it appears that organizations are doing well to limit the success rates achieved by criminals.

4 WHAT SECURITY LAYERS ARE MOST IMPORTANT TO PRACTITIONERS? *(Page 9)*

The top three most important components of security in the eyes of practitioners are segregation of duties, firewall/antivirus software, and multi-factor authentication.

6 NEW SECURITY TECHNOLOGIES SEE PROMISING TRACTION EARLY ON *(Page 11)*

Technologies like biometrics and tokenization are not yet in widespread use amongst corporates or banks. Nonetheless, early traction is promising and adoption is expected to steadily rise over the next 3-5 years.

8 WHICH PARTIES ARE MOST SUSCEPTIBLE TO FRAUD? *(Page 13)*

Regarding internal parties/departments, practitioners viewed AP as the highest risk, followed by treasury and payroll. Externally, the majority of corporates believe their vendors/suppliers are the most susceptible targets, followed by banks and software providers.

10 CORPORATE SECURITY TRAINING IN NEED OF ENHANCEMENT *(Page 15)*

Although nearly two-thirds of respondents provide annual security training to staff and addressing the human element of security appears to be a growing focus for firms, the level and sophistication of this training is in need of further enhancement.

KEY TAKEAWAYS: Treasury Action Items

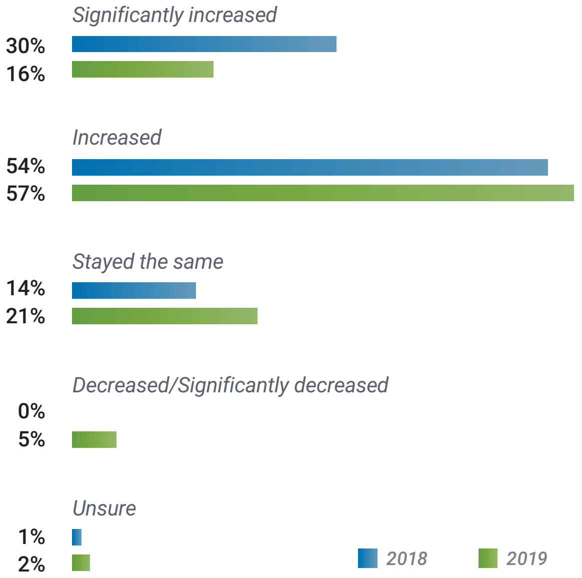
Key Findings Analysis

1| Corporate Confidence in Security Grows

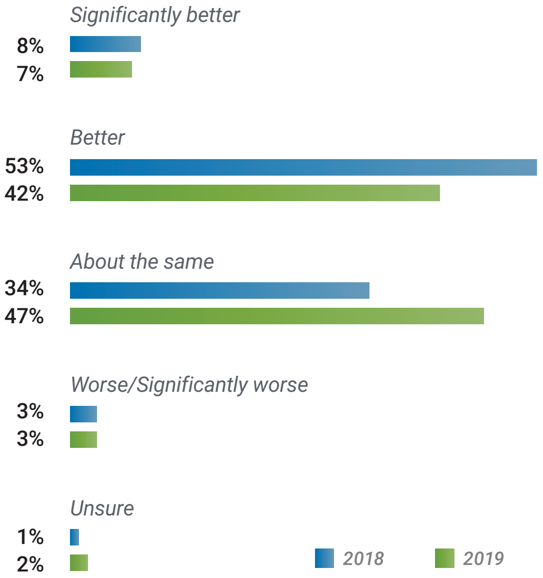
While practitioners consistently feel that the threat of fraud increases year-to-year, many also indicate increasing confidence in their security controls. However, this increased confidence has not always coincided with greater success in stopping fraud. In fact, despite widespread investment and focus on security controls by treasury groups over the past 3-5 years, there did not appear to be any noticeable shift in corporates' ability to prevent and detect fraud. Instead, many of the fraudulent attempts initiated by criminals were paying off.

In analyzing this year's results, a majority of practitioners again believed the threat of fraud had increased from the year before. Only 5% believed the threat had decreased. And also again, despite the fact that the overwhelming majority of respondents saw an elevated threat, practitioners were more confident in their ability to prevent and detect fraud than in prior years. In total, 50% believed they were in a better or significantly better position to fight fraud, vs. just 3% who believed they were worse off. However, while this heightened confidence has played out in prior years to the tune of continued criminal gains and corporate losses, data from this year indicates that corporate confidence in their security controls may finally be legitimate. With the percentage of successful fraud attempts in 2018 mostly holding steady from the prior year, corporates may finally be turning the tide back in their favor.

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



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

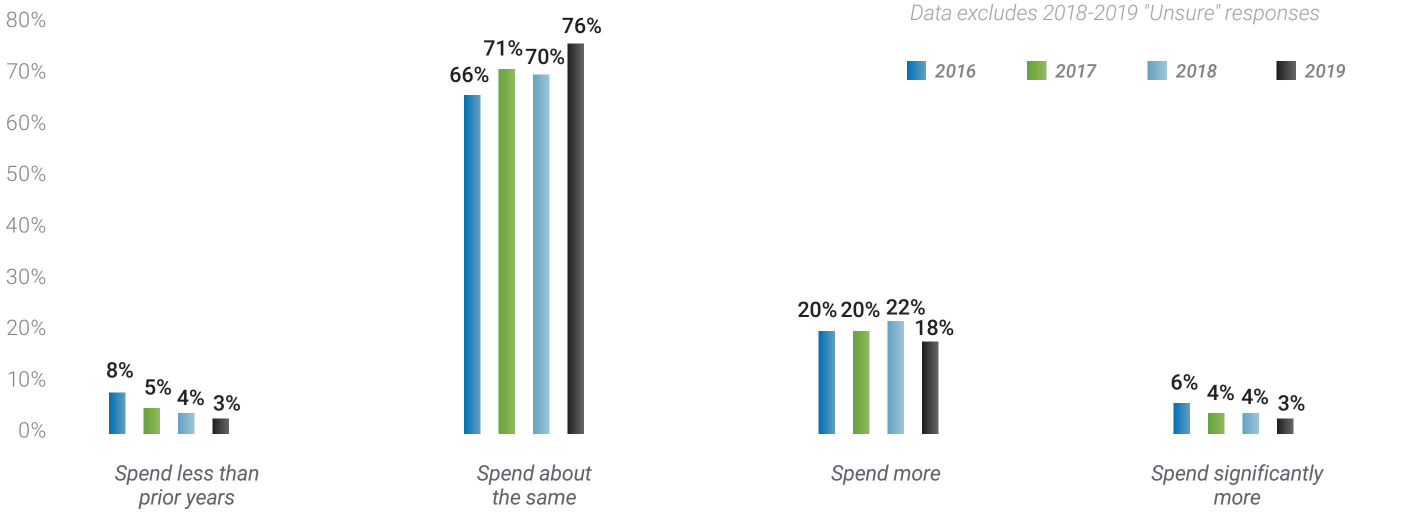


2| Multi-Year Corporate Security Focus Paying Off

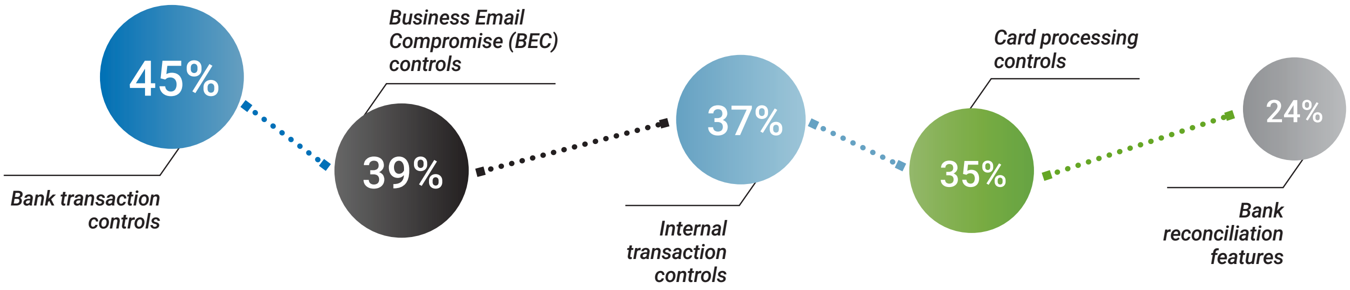
Since the 1st Treasury Fraud & Controls survey launched in 2016, we have seen significant investment in the security arena by firms of all sizes and industries. Typically, 20-25% of organizations spend more on security each year than in previous years, which makes for 3-6x more respondents planning to increase their spend versus those planning to spend less. This heightened security focus has also been captured in other recent Strategic Treasurer surveys, and in the *2018 B2B Payments survey,* 65% of corporates indicated that security concerns have a strong or very strong influence on their planned technology spend.

Looking now to 2019, approximately 7x more companies plan to increase their security spend compared to those reducing spend. Excluding "unsure" responses, 21% of corporates plan to spend more while just 3% plan to spend less. Much of this spend appears to be focused on AP/ Treasury payments, as well as on bank transaction controls and BEC fraud security components. However, while prior research has seen criminals continue to find success thwarting corporate defenses despite this spend, this multi-year trend of corporate investment finally appears to be paying off. While fraudulent activity remained widespread over the past year and more corporates experienced fraud than those that didn't, the number of successful attempts has not increased. After what has been witnessed across the financial environment in recent years, this is promising data. However, the fight against fraud is never over and companies must continue to be proactive in identifying and addressing exposures. Even a single criminal breach can be disastrous for an organization, and practitioners must not let their focus slide or grow overly confident in their controls. Criminals are always innovating their attack vectors, and corporates must continue to do the same with their defenses.

Corporates: What are your spending plans regarding treasury fraud prevention, detection, and controls?



2019 Planned Corporate Security Spend: Top 5 Areas of Focus



3| What Types of Fraud are Most Prominent Today?

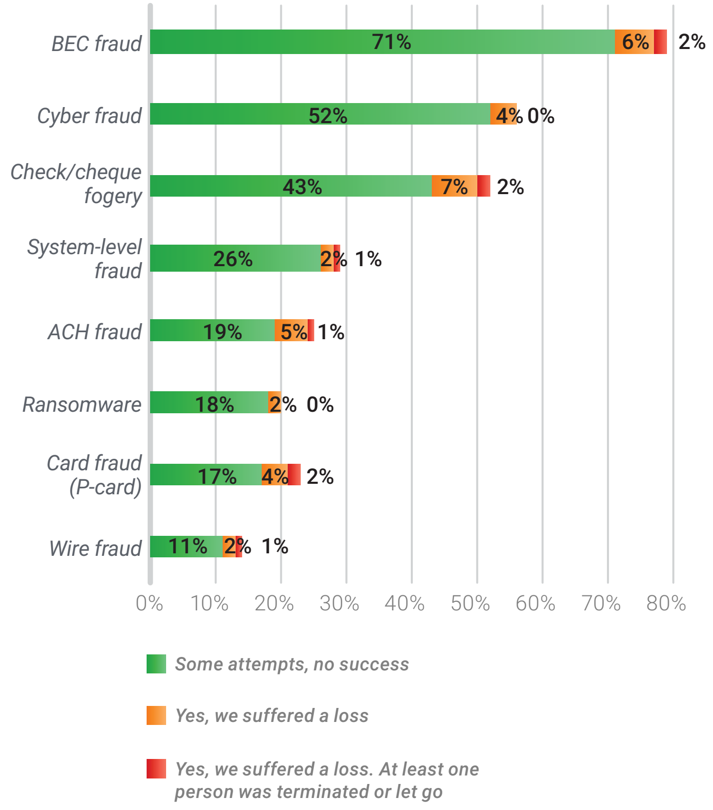
Looking across the full gamut of fraudulent activity, there are several types of fraud that were initiated or attempted much more frequently than others.

Business Email Compromise: BEC fraud has been the most common criminal tactic intitiated against treasury for several years now. But while the frequency of attempts in this area is high, the level of success experienced by criminals is relatively low (8% of the total population and 10% of those that experienced attempts actually suffered a loss). However, it is worth noting that because these attempts typically target large sums of money (tens of thousands of dollars per attempt in 2016[1]), there is more at stake than with other forms of fraud, such as check forgery.

Cyber Fraud/Data Theft: Cyber fraud (also known as data theft), the 2nd highest area of criminal activity, commonly involves phishing attempts or other malware being installed onto company servers or software with the intent of stealing sensitive data. This data is then either sold on the black market, or used to probe further into the company in hopes of eventually siphoning off actual funds. And while criminal success rates for this type of fraud appear low (4% of total population and 7% of those that experienced attempts), not every organization that suffers a breach in this area may be aware of it, as such attempts don't always result in an immediate dollar loss.

Check Forgery: Check forgery (the 3rd most frequently attempted type of fraud) is among the oldest forms of criminal trickery. However, the success ratio achieved by criminals carrying out check forgery is higher than both cyber fraud and business email compromise, with 9% of the total population and ~18% of those who experienced attempts suffering a loss. While this level of loss is high and somewhat concerning, the dollar-value associated with these attempts is much lower than for BEC or other mechanisms, and averaged just $1-2 thousand per loss in 2016[2].

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



Tips to Prevent:

BEC Fraud

1. Use multi-factor authentication on all email/messaging systems
2. Train employees on how to identify and respond to suspicious emails or requests

Cyber/Data Theft

1. Encrypt data, both at rest and in transit
2. Install & maintain updated antivirus & firewall software

Check Forgery

1. Stop using checks, convert to e-pay methods
2. Adopt Positive Pay
3. Reconcile bank accounts daily

*(1,2) average dollar-value of 2016 fraudulent losses for check fraud and BEC fraud are based off FBI, bank, and Strategic Treasurer data.

4| What Security Layers are Most Important to Practitioners?

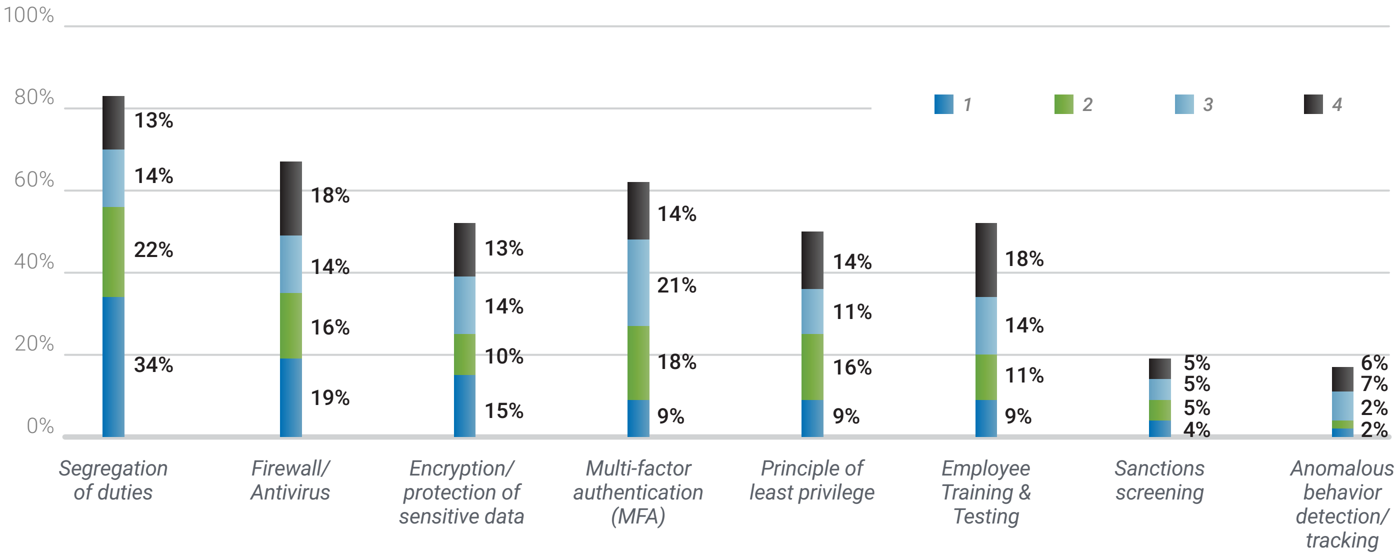
One of the questions contained in this year's survey asked respondents to rank, in order of importance, eight of the leading security practices/technologies currently in use across the treasury landscape. In analyzing the data, it appears the top three most-important techniques in the eyes of practitioners are:

i. *Segregation of duties*
ii. *Firewall & Antivirus software*
iii. *Multi-factor authentication*

The first two items on this list are core components of security that virtually every firm should have in place. In fact, any organization that has not implemented segregation of duties or that does not have firewall/antivirus software installed is far behind the rest of the corporate environment and is at serious risk of fraud, from both internal and external sources. However, while these first two items can be considered "minimal" requirements in the areas of security, the 3rd item (multi-factor authentication) is a more recent addition to many organizations' security infrastructures. As the threat from online and digital fraud becomes more significant, multi-factor authentication has proven to be a powerful form of defense. By requiring employees to present multiple forms of identification (i.e. username and password coupled with a key fob) before logging onto payment systems or executing funds transfers, the chances of a criminal being able to obtain each layer of authentication is drastically reduced.

Corporates: Please rank the importance of the following security principles at your organization from 1st to 8th.

***Note:** Only rankings 1-4 displayed*



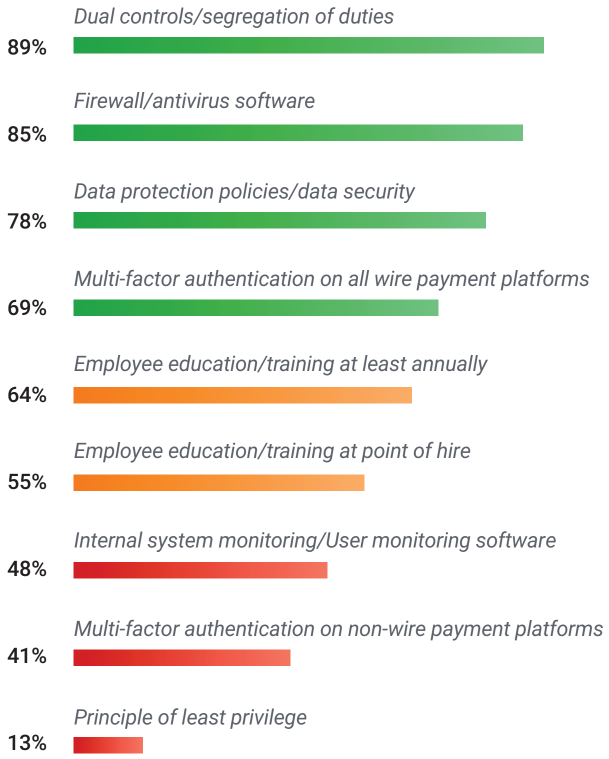
Focus on Multiple Layers: "*While certain security components may be ranked higher than others, corporates should remember that the best method of defense is to employ multiple layers of security, and not just focus on 1-2 core areas.*"

5| What Areas of Corporate Security are Clearly Lacking?

In evaluating the overall use and deployment of various security measures across the corporate environment, it is evident that while corporate adoption of security controls continues to rise, there are still a number of exposures to be addressed. This is true for both basic and advanced security practices and standards. Even when looking at common areas of security such as dual controls or antivirus/firewall software, 11% of companies did not leverage dual controls and 15% did not have antivirus software. Given that these items are considered minimal or "basic" standards of security, any firm that is not utilizing such policies is placing themselves at severe risk of fraud.

Although the majority of organizations leverage basic security elements like antivirus software, there appear to be much larger gaps in corporate adoption across other areas. For instance, while the "Principle of Least Privilege" ranked as a top four area of focus for 49% of practitioners, only 13% of respondents indicated they were officially leveraging such a policy internally. Given the proven benefits of implementing this type of policy, we would expect the number of firms utilizing it to be much higher. Another area where this rings true is with data encryption. While 52% of corporates listed data encryption as a top four area of focus, only 41% were knowingly encrypting data at rest and just 39% were encrypting data in transit. Given the prominence of data theft and cyber fraud in today's environment, this is a concerning discovery. In the event that unencrypted corporate systems or servers are actually jeopardized, the data contained within them is incredibly vulnerable and could be easily obtained by criminals during a breach. Although there are other more advanced forms of security that have yet to see major traction, firms that have yet to address these core areas or elements must take clear and quick action before they pay the price for their oversight.

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



Delineation of Corporate Security Practices:

Minimum Standards: If you do not employ these, you are FAR behind the industry and at severe risk of fraud.

1. Dual controls/segregation of duties
2. Firewall & antivirus software
3. Policy of least privilege

Standards of Good Corporate Conduct: If you do not employ these, you are behind the majority of the industry and need to reexamine your controls.

1. Multi-factor authentication (MFA)
2. Data encryption (at rest & in transit)
3. Annual employee security training

Leading Standards: Organizations should plan to employ these layers within the next 3-5 years.

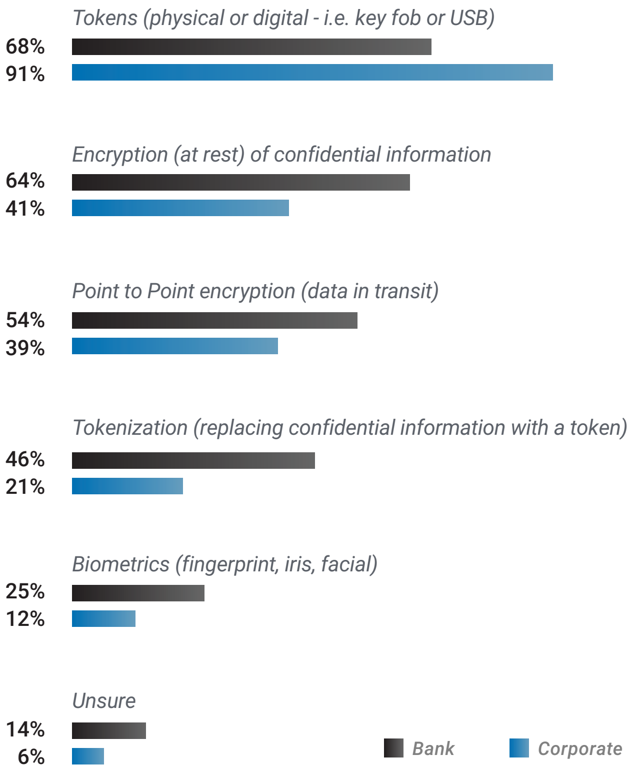
1. User monitoring software
2. Biometric software/scanners
3. Tokenization practices

6| New Security Technologies See Promising Traction Early On.

One of the forward-looking elements of this year's research was to determine which new or "emerging" security practices were seeing the most attention from corporates and banks. This included the use of technologies like biometrics and tokenization, as well as user monitoring software (which is addressed in more detail on page 14). Biometrics (the use of facial recognition, fingerprint scans, etc.) as a form of employee verification has garnered widespread attention in recent years, as has tokenization (replacing sensitive information with a "token" as it passes through certain systems). But how popular and widely-used are these techniques currently?

In analyzing responses, it is clear that traction is still (understandably) far behind more established security techniques. For example, while 91% of organizations were leveraging physical tokens such as key fobs or USBs when accessing payment systems, only 12% employed biometrics and 21% used tokenization. On the banking side, where new security practices tend to be implemented fairly quickly, biometrics saw use across 25% of the population and tokenization by 46%. But while the use of both biometrics and tokenization is subdued compared to other security techniques, keep in mind that these components are still relatively new entrants to the security landscape. In fact, this level of adoption is fairly promising given the short timeframe for which such technologies have been readily available. And as security continues to be a major focus for firms moving forward, we expect to see continued adoption of both components in the years to come.

Are you using any of the following access or security methods? (Select all that apply)



Banks Drive Adoption of New Security Technologies:

"While banks lead the way with adoption of new technologies like biometrics and tokenization, the use of these components is gradually filtering over to the corporate side as awareness spreads and the technology becomes more readily available."

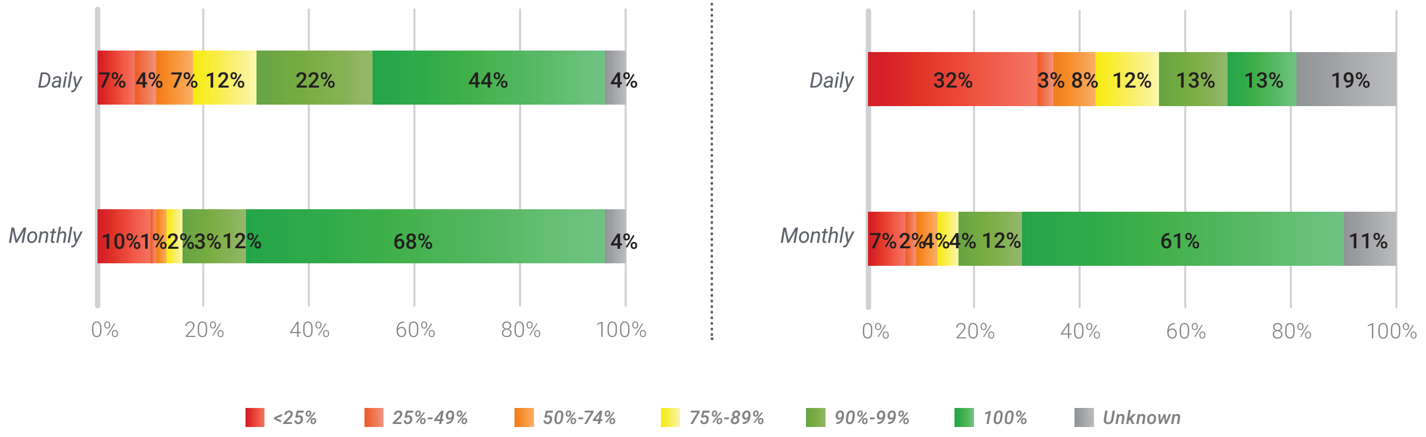
7| Timely Bank Account Visibility & Reconciliation are Vital.

Today, daily bank account reconciliation is not a widely leveraged feature in the corporate environment. Yet, it is a function that can go a long way in quickly identifying fraudulent activity and preventing future losses from occurring. Although many organizations are beginning to benefit from faster payments services, the downside to this speed is that criminal activity can be carried out much quicker than historically was the case. Whereas it may have taken several days for fraudulent checks to clear an account in the past (and thus provide several days for an organization to identify the anomalous payment), payments made via ACH, card, or RTGS (wire) clear much faster today. Thus, the need for enhanced bank account visibility and reconciliation features continues to escalate.

As highlighted by this year's survey, 44% of corporates currently have daily visibility to 100% of their bank accounts, and 66% have visibility to 90%+ of their accounts. Although this level of daily visibility is fairly substantial and is a great first step in quickly identifying errant or anomalous payments, there has been much less headway when it comes to actual account reconciliation. In total, just 13% of corporates reconcile all their accounts daily and only 26% reconcile 90%+ daily. Instead, data shows that the majority (73%) of corporates reconcile 90%+ of their accounts on a monthly basis. But in an environment where speed matters, this is simply not quick enough. While data from this survey has also shown that 24% of firms plan to spend significantly in the area of reconciliations during 2019, we hope to see similar (if not higher) levels of spend over the next 2-5 years until this issue is rectified.

Corporates: What percentage of your accounts do you have **VISIBILITY** to within the following timeframes?

Corporates: What percentage of your bank accounts are **RECONCILED** within the following timeframes?



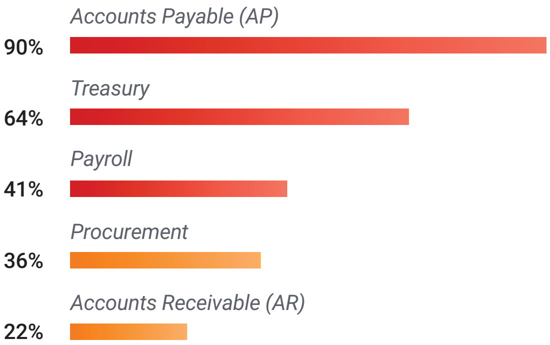
Faster Reconciliation Required: *"While the fact that 2/3rds of corporates have daily visibility to 90%+ their bank accounts is promising, just 1/4th reconcile 90%+ of their accounts daily. This lack of timely reconciliation represents a large exposure when it comes to quickly identifying fraudulent transactions."*

8| Which Parties are Most Susceptible to Fraud?

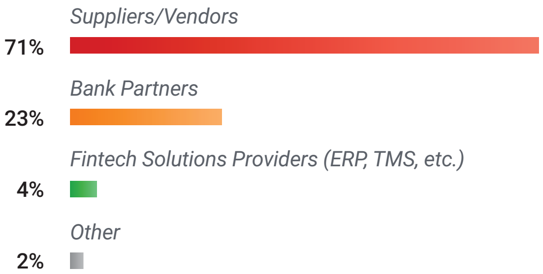
Internal Party Susceptibility: When asked to select the three departments (out of nine potential choices) that were most susceptible to fraud, the vast majority of respondents (90%) listed Account Payable (AP). Treasury was listed by 61%, and 41% selected payroll. Other departments like procurement, AR, and C-Suite (executives) were seen as less susceptible. Given that AP, treasury, and payroll are responsible for the vast majority of funds transfers generated by companies, it makes sense that practitioners would view these areas as the primary targets for fraud.

External Party Susceptibility: Looking at external parties, practitioners view their suppliers/vendors as way more vulnerable to fraud than other parties like banks or fintech providers. In fact, when asked to select the one segment of their partner network they believed was most susceptible, 71% of practitioners listed their suppliers/vendors, compared to just 23% that listed their bank and 4% that listed their tech provider (TMS, ERP, etc.). In evaluating the security landscape as a whole, corporates are probably less concerned about their banks and technology providers because these organizations are held to rigorous standards regarding their security infrastructure, due to the various regulations and requirements in place for managing sensitive client data. Also, as banks and fintech providers are evaluated by clients, their security practices come under intense scrutiny and as a result, corporates may just be more familiar and confident in their controls. And while some of these requirements and inspections are levied onto vendors/suppliers also, they are nowhere near as stringent as those within the FI/Fintech space. Finally, smaller vendors and suppliers commonly lack the budget or capital necessary to invest in advanced security technology and other controls, and also may have lower internal standards regarding their security infrastructure.

Corporates: Which THREE departments internally do you feel are most susceptible to fraudulent attacks? (Only top 5 choices shown)



Corporates: Which segment of your partner network do you feel is the most susceptible to fraudulent attacks?



Tips for Reducing Exposure:

Internal Departments

1. Deploy user monitoring software to detect anomalous user actions
2. Train employees on how to monitor and identify suspicious emails, behaviors, etc.
3. Use multi-factor authentication (MFA) on all systems and platforms

External Suppliers/Vendors

1. Develop a thorough onboarding process that includes security checks
2. Assign clear policies and workflows for managing bank account details/records
3. Establish clear processes and points of contact for changing vendor details/bank accounts

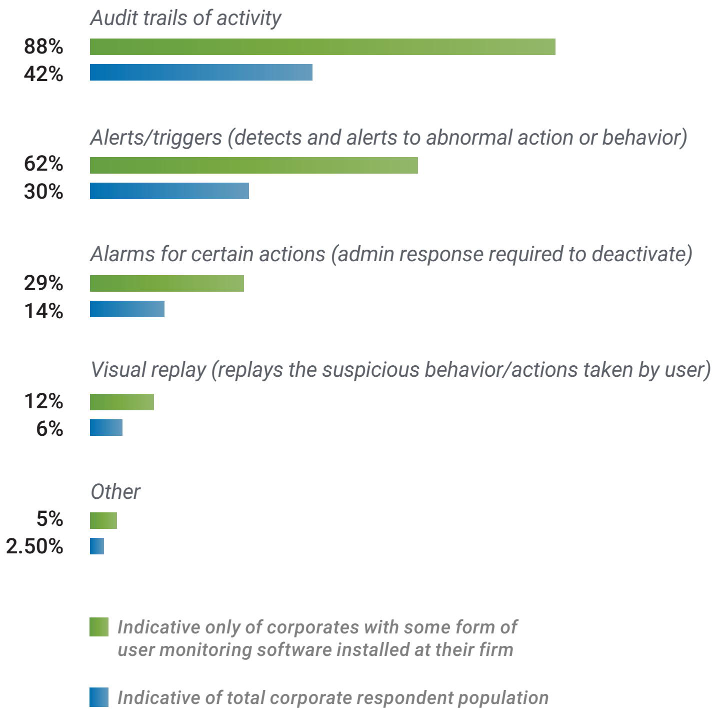
9| User Monitoring Software: What is it & How Does it Help?

What would the current fraud environment look like if organizations could detect suspicious activity occurring through their systems in real-time? This ability may soon be a reality for many companies, as technology vendors and banks have begun incorporating user monitoring software into their various solutions and offerings. These functionalities are designed to monitor user activity within financial systems and send alerts to administrators if anything unusual is detected. For instance, if a company user logs in at an abnormal hour or attempts to enter a module that they would typically not have access to, the system would identify these actions and alert administrators of the issue. The system may even be capable of providing visual replays or detailed summaries of what actions were taken by the user to further understand the nature of the suspicious behavior. Other types of activity that may generate alerts include suspicious payment amounts, volumes, or recipients.

While user monitoring software is not currently at the top of many corporates' security priorities, certain variations of the software are in use amongst nearly half (48%) of the corporate environment. Such software was also used by 82% of bank respondents. However, most of the functionality leveraged through this software currently revolves around simple audit trails of activity or basic alerts, rather than more sophisticated features like visual replays of user activity. But, given that user monitoring software has seen steady investment by software firms and FIs over the past 3-5 years and its development continues to advance, we expect rising traction and use within the corporate environment.

Corporates: We have these capabilities to monitor anomalous or suspicious behavior within our system(s): (Select all that apply)

***Note:** This question asked only to the 48% of corporates with user monitoring software installed at their organization.*



Benefits of User Monitoring Software:

Despite limited adoption so far, user monitoring software has proven adept at providing several key benefits to organizations:

- ✓ Be alerted of suspicious activity in real-time
- ✓ Have complete visibility into suspicious user actions
- ✓ Ability to provide complete audit trails/system replays in event of breach
- ✓ Protects against rogue employee actions internally, as well as external fraud perpetrated via compromised user accounts.

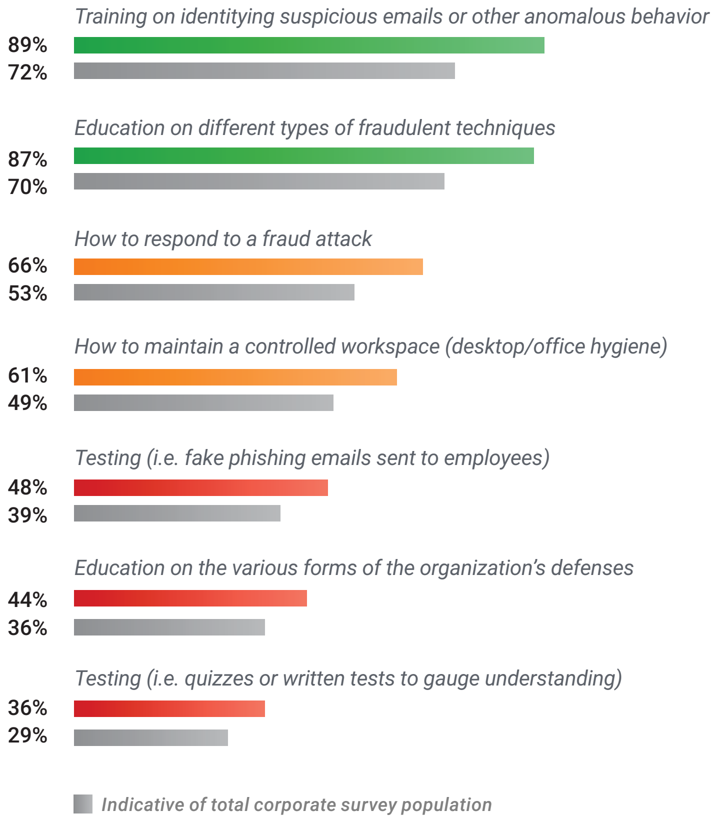
10 | Corporate Security Training in Need of Enhancement

During the initial years of our research in the security arena, one area that was regularly highlighted as lacking in focus centered around employee training. While enhancements to security technology and controls are very crucial (especially in today's digital age), the importance of the human elements of security (i.e. training and educating employees on how to identify and respond to fraudulent attacks) cannot be underestimated. Even if the most advanced security systems are implemented by an organization, employees that are not aware of how the systems work or that are ignorant of the protocols to follow in the event of a breach can be the reason losses occur.

Although past surveys have shown that most corporates offer some form of annual security training to their staff, the robustness of these training sessions varies from firm to firm. For instance, 81% of organizations in this year's survey trained their employees on security (64% annually and 55% at point-of-hire). However, only 66% of these firms (53% of the total population) were trained on how to respond to a fraud attack, and only 48% tested their employees with fake phishing emails. An even smaller portion (36%) provided written tests to their employees as a method of gauging actual understanding. Thus, even though a majority of corporates provide security training, the level of preparation and understanding obtained through many of these sessions is not optimal. Moving forward, instead of providing a basic "101" overview of security, we would like to see a greater portion of corporates implement more advanced training courses that not only cover a greater breadth of topics, but that also include tests and follow-up procedures to ensure that employees are legitimately cognizant of their security situation.

Corporates: Our security training includes: (Select all that apply)

***Note:** This question asked only to the 81% of organizations that trained their employees on security either annually or at point-of-hire*



Security Training Tiers: Range of Practices

☠ **No Training:** If you are not training your employees at all on security, you are at severe risk. Untrainined employees represent a large exposure.

⚠ **Training at Point of Hire ONLY:** While some training is better than none at all, only training employees once means that any subsequent changes to the fraud environment go unnoticed and unaccounted for by your staff.

✓ **Annual Training:** Annual training is the best way to ensure your employees are up-to-date. These sessions should include training on:

1. How to identify suspicious activity
2. Various forms of fraud
3. How to respond to an attack
4. How to maintain a hygienic workspace
5. Testing employees with fake fraud instances
6. Testing employees with written quizzes

Treasury Action Items

While the corporate treasury environment as a whole is continuing to make advancements in the area of security and fraud prevention, there is no time to rest. Just as new security controls and techniques are added to defend against one form of attack, criminals are simultaneously innovating new methods. And although practitioners can take encouragement from the gains they have made over the past several years, there is always room for improvement. Looking ahead, the following actions can be considered a list of most pressing items that practitioners should consider moving forward.

1 APPLY LEAST PRIVILEGE

In order to ensure that sensitive information or system access does not fall into the wrong hands, apply the principle of least privilege. Having a clear policy that limits the level of information employees can obtain, especially where payment processes or financial data is concerned, can significantly reduce the exposure points that result in fraud.

2 MONITOR ANOMALIES

With a vast proportion of today's financial operations conducted electronically, the need for systems and software that can monitor user behavior is vital for quickly identifying suspicious or anomalous actions. These systems should also keep clear logs of user activity in case certain actions or circumstances need to be reviewed.

3 FORMALLY TRAIN PERSONNEL

While nearly 2/3^{rds} of the corporate environment train their employees at least annually on fraud, many of these sessions lack the substance necessary to adequately prepare staff. And while some training is better than none, testing employees and expanding training programs to include advanced subjects is highly recommended.

4 CONSISTENTLY ENCRYPT DATA

While some organizations may rely on external providers for encrypting data, there are typically instances where information is stored on internal hard drives or servers as well. In either case, ensuring that both data at rest and in transit is encrypted across all business processes can significantly limit the impact that a cyber breach has on a company.

5 DEPLOY MULTI-FACTOR AUTHENTICATION

Whether it's for email accounts or payment systems, multi-factor authentication introduces a vital new layer of protection for companies and drastically increases the difficulty for criminals to steal credentials. Chiefly, requiring a username and password in addition to a randomly generated passcode, biometric scan, or other element means that even if certain credentials are compromised, a criminal still could not gain access to corporate systems.

6 RECONCILE BANK ACCOUNTS DAILY

In the event that fraudulent transactions are initiated, it is pivotal that organizations identify them as quickly as possible. Recognizing a fraudulent charge on the day it occurs may provide a chance at blocking the transaction before funds are withdrawn, and also ensures that future losses do not occur through the same breach or exposure.

7 VET SUPPLIERS PRIOR TO ONBOARDING

With ~3/4^{ths} of practitioners viewing their suppliers as highly susceptible to fraud, establishing proper due diligence, KYC, and other screening/onboarding steps prior to conducting business with a new partner is essential for ensuring your processes are not jeopardized through an external breach.

8 AUTOMATE BANK ACCOUNT PROCESSES

Today, 60% of organizations still manage bank account operations manually. Given the sensitive nature of bank account information, having a clear defined and secure process for managing this data can go a long way in ensuring such details are not illegitimately tampered with.

Have a question?
Contact an expert!

Bottomline
info@bottomline.com

Strategic Treasurer
Consultants in Treasury
info@strategictreasurer.com

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.*

+1 800.243.2528 (US)
+44 118 925 8250 (EMEA)
bottomline.com
info@bottomline.com

STRATEGIC TREASURER

Strategic Treasurer was founded in 2004 by Craig Jeffery, a financial expert and trusted advisor to executive treasury teams since the early 1990s. Partners and associates of Strategic Treasurer span the US, the UK, and continental Europe.

This team of experienced treasury specialists are widely recognized and respected leaders in treasury. Known for their expertise in treasury technology, risk management, and working capital as well as other cash management and banking operations, they efficiently identify issues, creatively explore ideas and options, and provide effective solutions and implementations for their valued clients. For more information visit *www.strategictreasurer.com.*

+1 678.466.2220
strategictreasurer.com
info@strategictreasurer.com

Bottomline

+1 800.243.2528 (US)
+44 118 925 8250 (EMEA)
bottomline.com
info@bottomline.com

Strategic Treasurer
Consultants in Treasury

+1 678.466.2220
strategictreasurer.com
info@strategictreasurer.com