Treasury Fraud & Controls

2018 Survey Results Webinar

Craig Jeffery, *Strategic Treasurer*

David Levine, *Bottomline Technologies*

James Richardson, *Bottomline Technologies*

Thursday, April 26th, 2018

11:00 AM EST

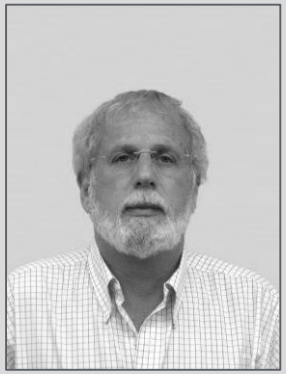
Today's Presenters

Craig Jeffery, CCM, FLMI

Founder & Managing Partner

Strategic Treasurer

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.



David Levine

Director of Product Marketing

Bottomline Technologies

David E. Levine has almost 40 years' experience in the Information Technology industry including almost 20 years in leadership positions in Europe and Asia Pacific. Mr. Levine joined Bottomline Technologies in 2008 to lead their Order-to-Pay Automation initiatives, and has been heavily involved in the expansion of Bottomline's payment and cash management product portfolio.

James Richardson

Head of Market Development, Risk & Fraud

Bottomline Technologies

James Richardson has worked in the Payments industry in an ever changing landscape for over 15 years, working with Financial Institutions and Corporates of all sizes. James helps organizations reduce their fraud risk and secure critical payments by sharing insights on industry, trend and technology offerings.

Topics of Discussion

- **About the Survey**
  - *Survey Components*
  - *Demographics*
- **Corporates Focused on Fraud**
  - *Firms Indicate that Cyber Fraud threat has increased*
  - *Heavy Investment in Cyber Security & Fraud Prevention*
  - *Investments Lead to Greater Confidence*
- **Security Controls Still Inadequate**
  - *A Piecemeal Approach to Security*
  - *Sanctions Violations: An Ignored Threat*
  - *Fraud Management Responsibilities Unassigned*
- **Losses Continue to Mount**
  - *Fraud Continues to Climb*
  - *Criminal Success Rates are High*
  - *New Threats Emerge: Ransomware*
- **Key Takeaways & Action Items**

About the Survey

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

At least 1/4th of respondents operated in each world region

Respondents primarily HQ'd in North America, Europe

TOP CORPORATE RESPONDENT ROLES

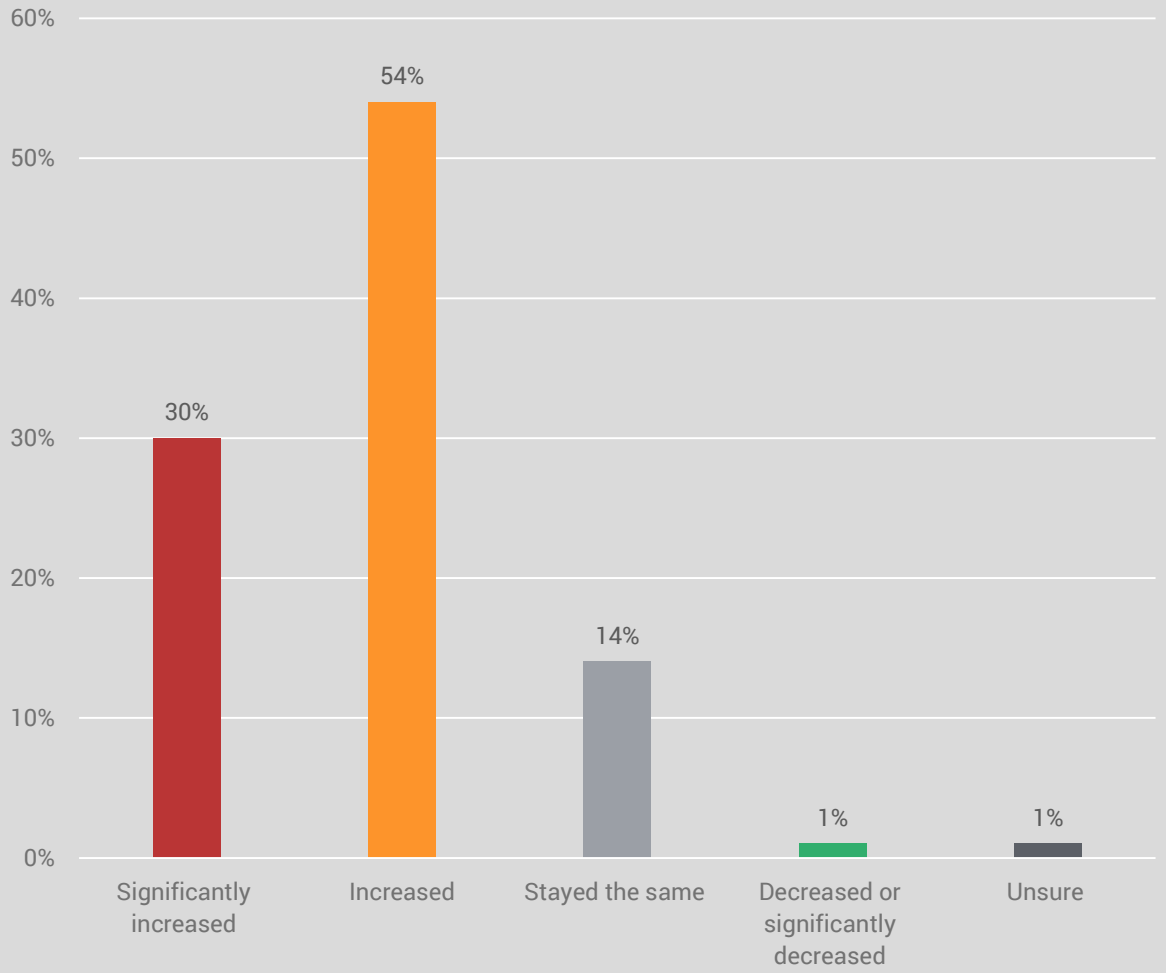
- 26% Treasury/Cash Manager
- 17% Treasurer
- 15% Assistant Treasurer
- 15% Treasury Analyst
- 4% CFO

Corporates Focused on Fraud

The Threat has Increased

- 84% of corporates believe the threat of cyber fraud has increased over the past year, 30% significantly.
- Only 1% saw a lower threat compared to the prior year.
- These elevated concerns, coupled with heightened spending and investment in security controls, suggests that fraud 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:"

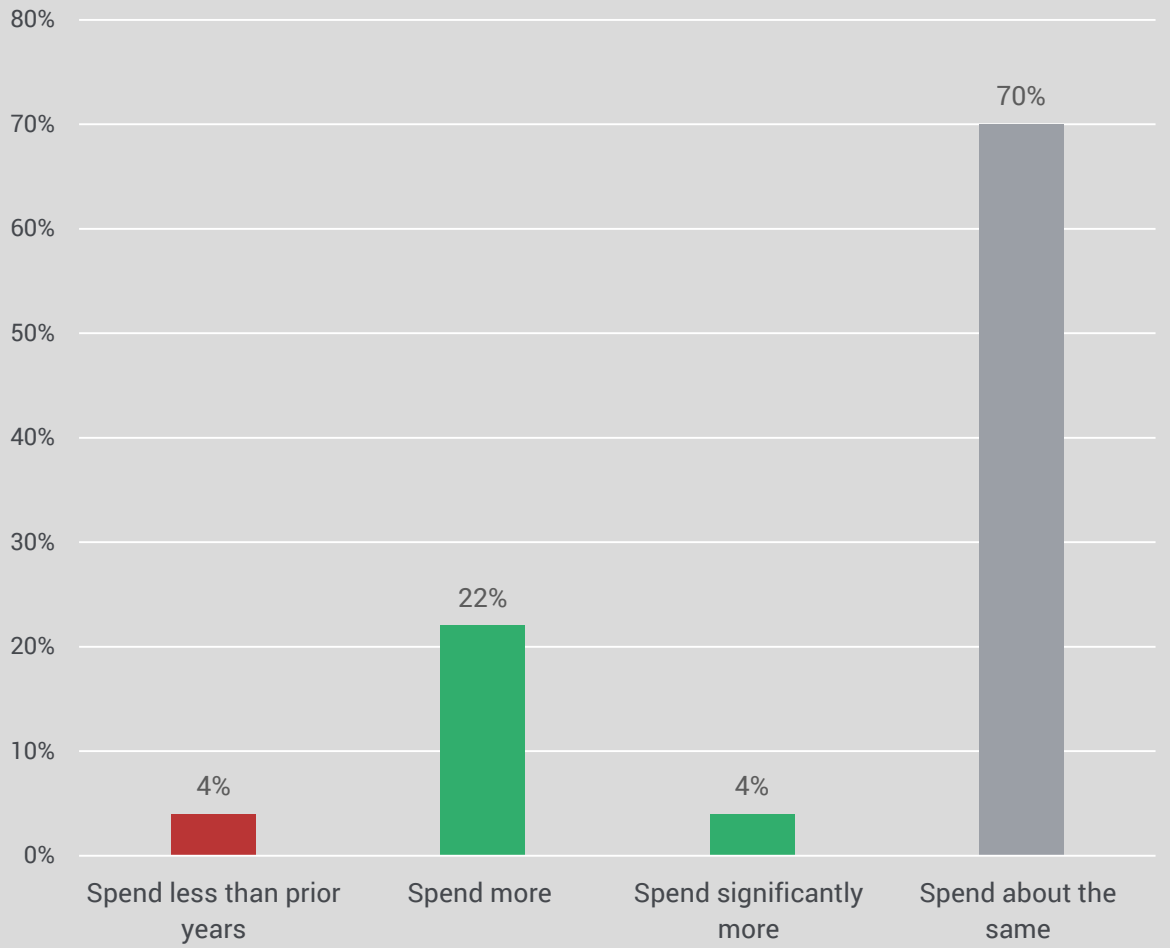


Corporates Focused on Fraud

Continued Intent to Spend on Security Tools

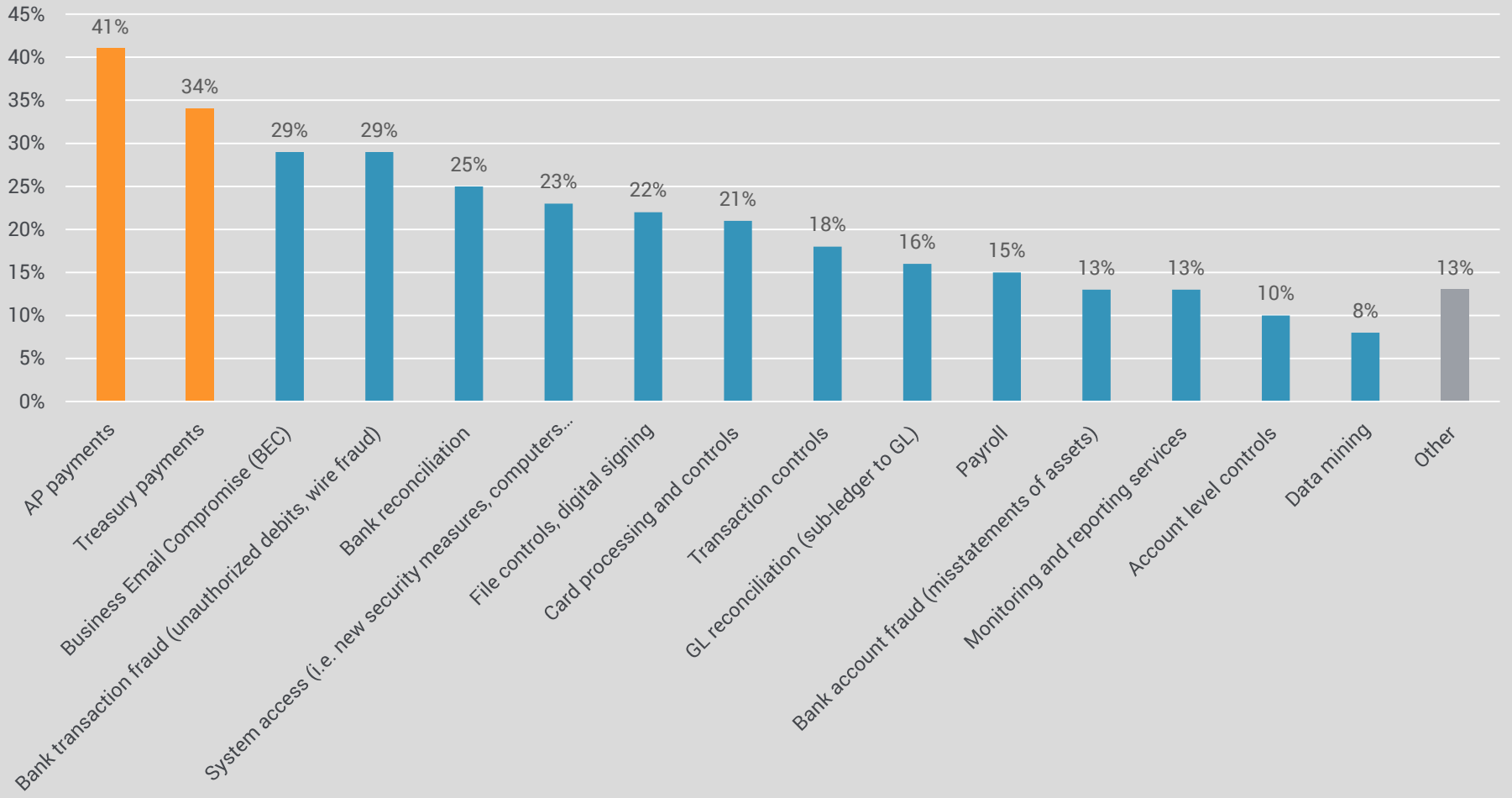
- As fraud concerns remain elevated, organizations continue to invest heavily in security controls.
- Over the past three years, approximately 25% of corporates have consistently spent more on security tools than in prior years.
- This elevated spend has targeted a wide variety of areas, ranging from AP and treasury payment controls to reconciliation features and fraud monitoring / reporting services.

Corporates: What are your spend plans for treasury fraud prevention, detection, and controls? *Data excludes "unsure" responses*



Corporates Focused on Fraud

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

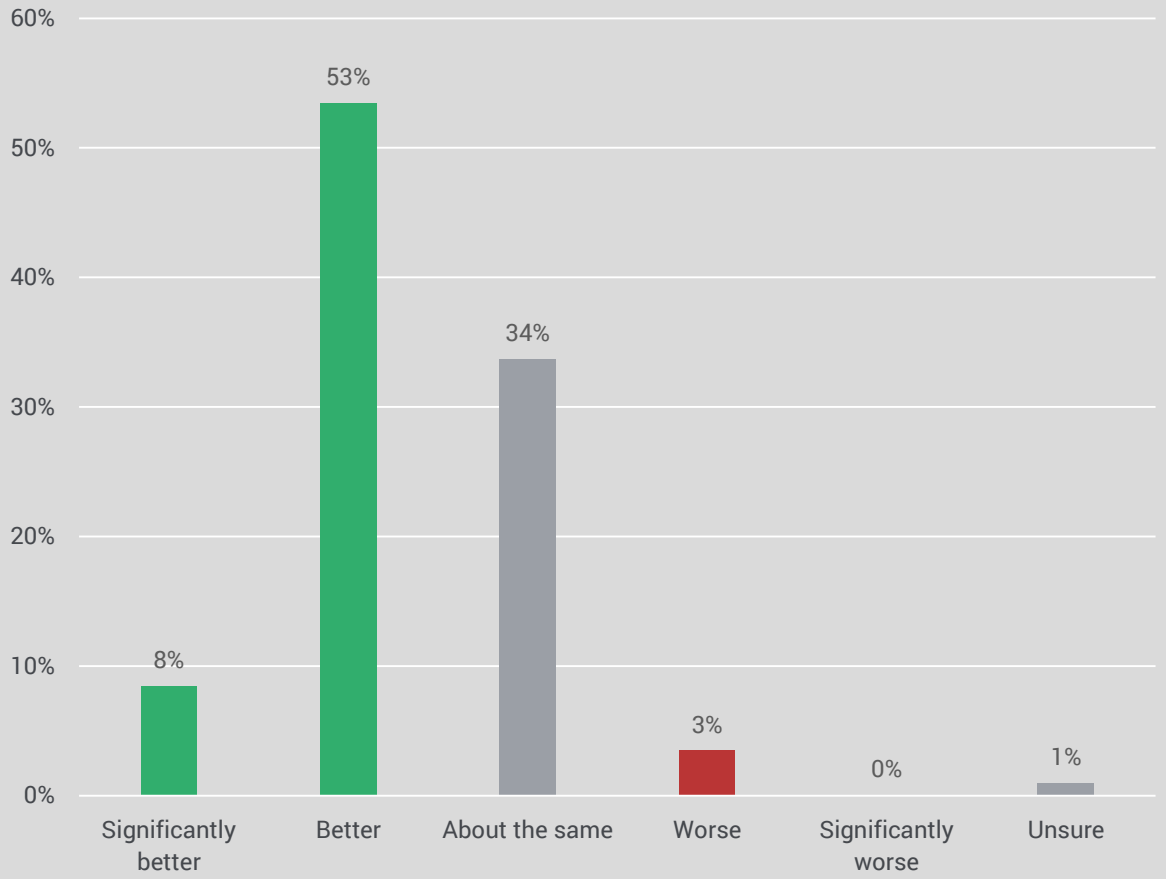


Corporates Focused on Fraud

Investments Lead to Corporate Confidence in Defensive Posture

- Continued investments in security have led to a higher degree of confidence for practitioners.
- In fact, **20x** more corporates believe they are in a better position to deal with fraud this year compared to those that believe they are worse off.
- This data highlights a belief within the corporate ranks that while fraud remains a significant threat, the security investments they have made means they can more effectively deal with attacks.

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.

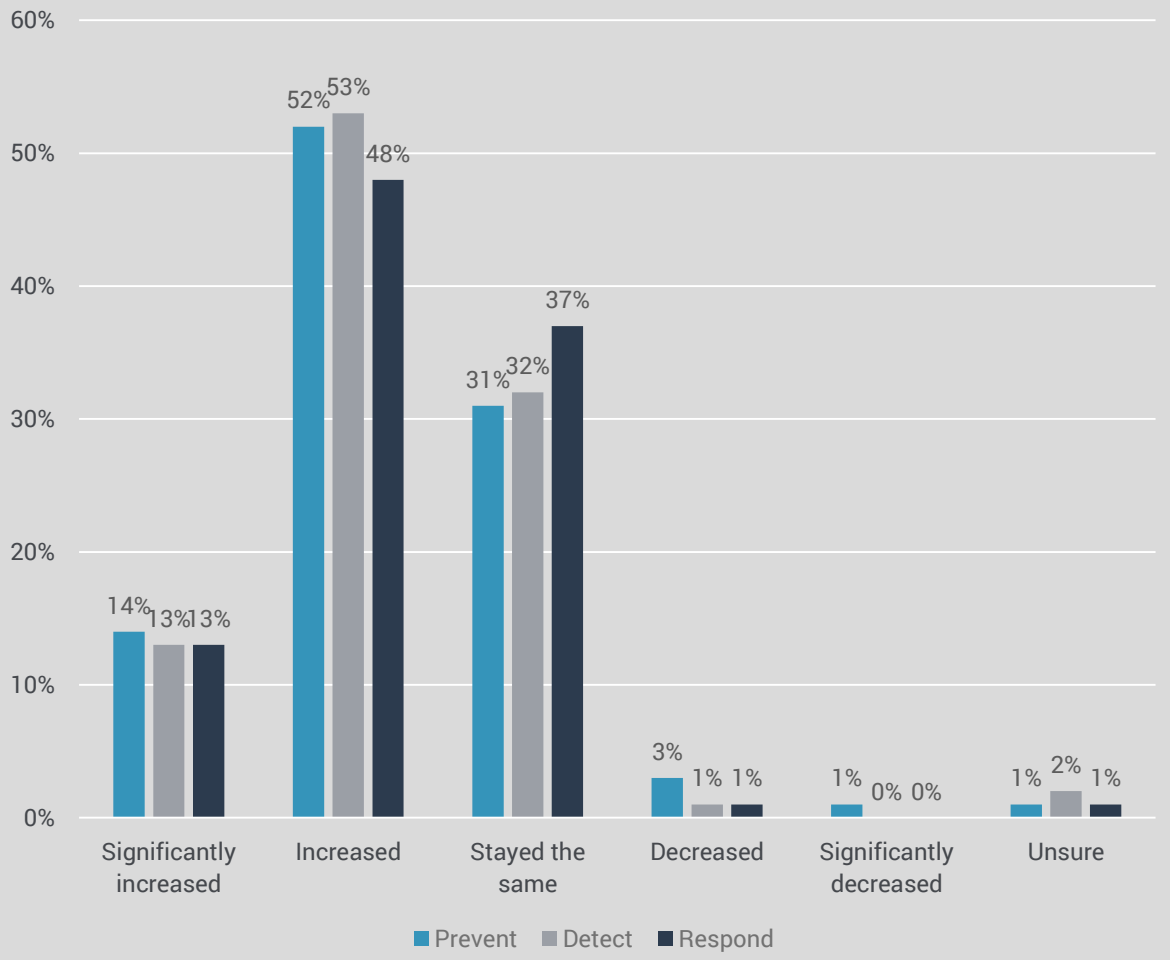


Corporates Focused on Fraud

Corporate Confidence Grows

- There are various stages of security that must be addressed in the fight against fraud.
- This includes:
  - The outright prevention of fraud
  - The detection of any anomalous activity
  - Response mechanisms in the event of a breach
- In the past year, the majority of corporate practitioners feel as though their firm's abilities in each of these areas has increased or significantly increased.

Corporates: In the past year, I think that our organization's ability to prevent, detect, and respond to fraud has:

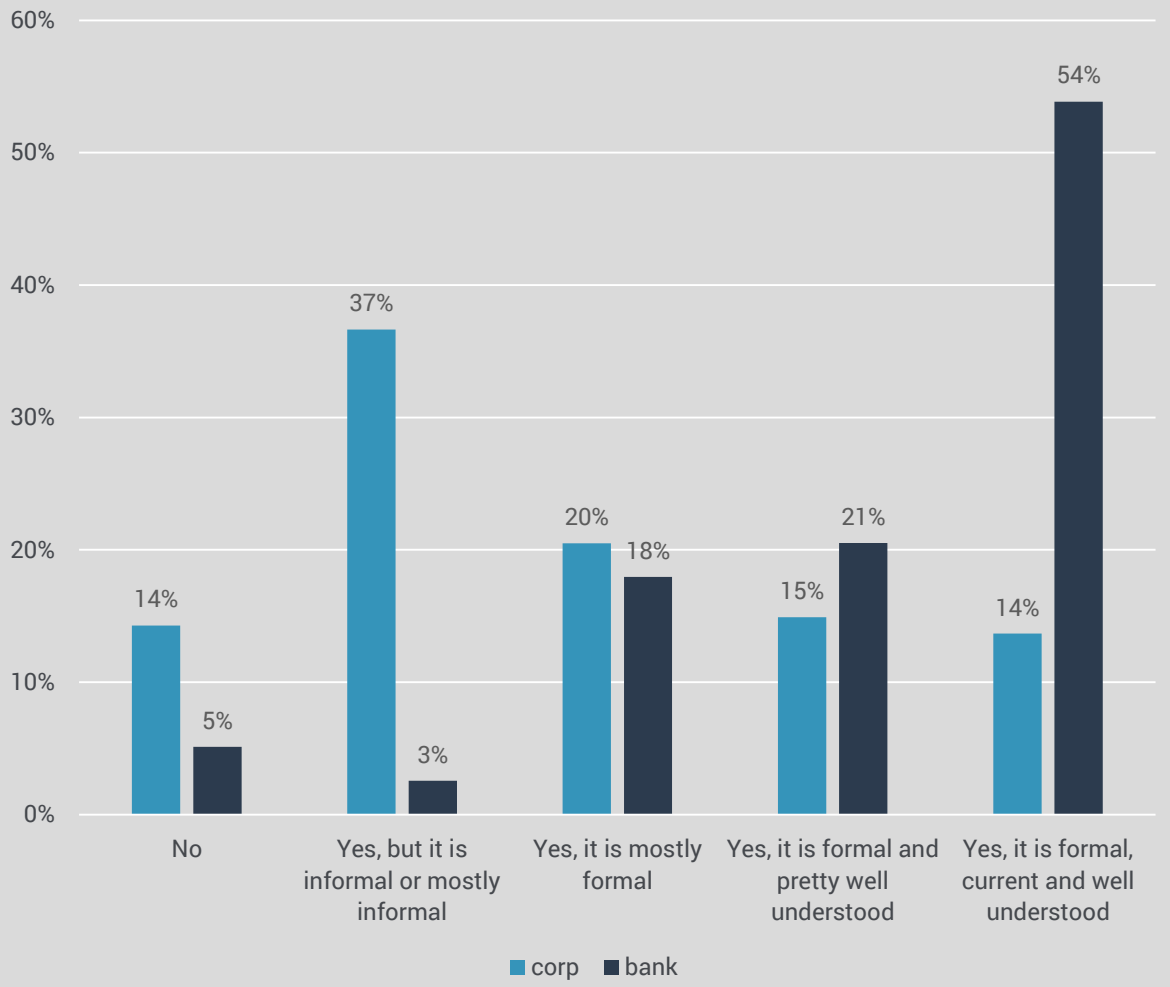


Security Controls Still Inadequate

A Piecemeal Security Approach

- When looking at corporate security controls compared to banks, over half of corporates have an informal control framework.
- This points to a lack of any definitive game-plan for fighting fraud and protecting organizational assets.
- This also means that corporate security investments are not always a part of a more holistic strategy.
- Instead, practitioners may address exposures as they arise, but other exposures or areas of weakness go unnoticed and unaddressed.

Do you have a treasury fraud and controls framework?

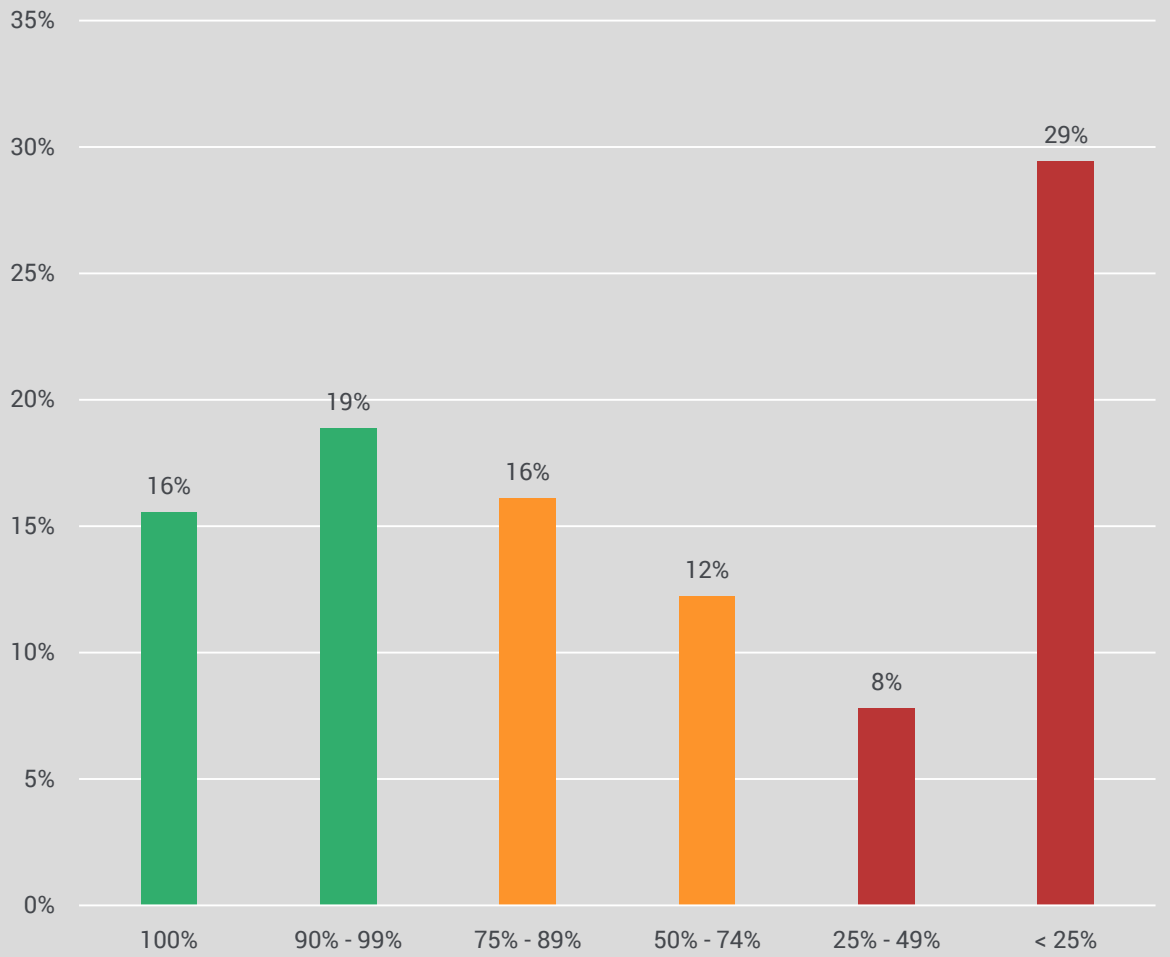


Security Controls Still Inadequate

Reconciliation Practices

- Over the past year, practitioners have indicated that reconciliation tools have been an area of focus.
- Currently, however, only 1/3rd of corporates reconcile 90%+ of their accounts daily.
- On the opposite end of the spectrum, over 1/3rd reconcile less than half their accounts daily.
- Speedy reconciliation capabilities play an important role in fraud detection; as such, this is an area in need of improvement.

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

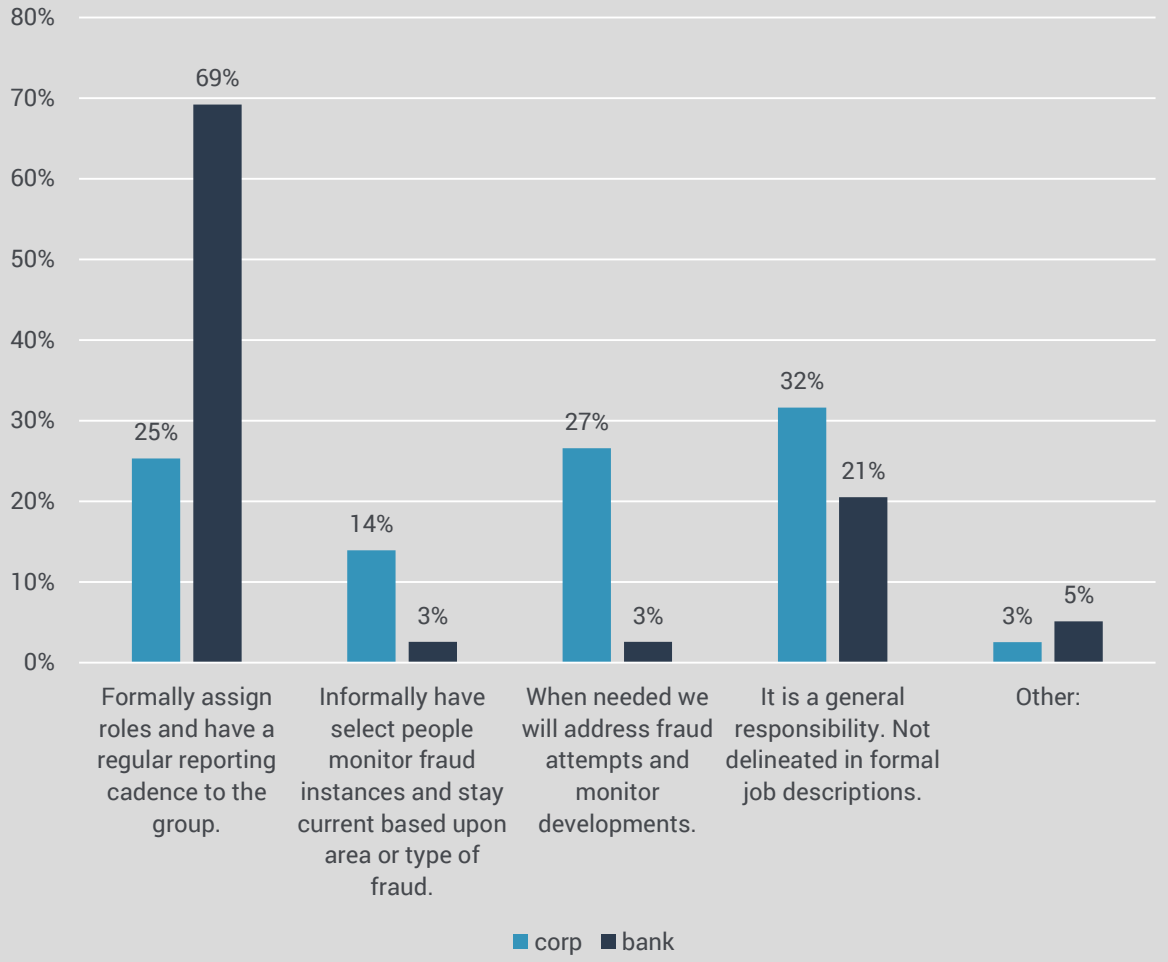


Security Controls Still Inadequate

Fraud Management Responsibilities Unassigned

- Survey results over the past three years have consistently shown a lack of focus by treasury teams on assigning formal security and fraud monitoring roles.
- Each year, approximately 1/4th of corporates have formally assigned roles.
- While corporates have invested heavily in security technology over the past few years, data shows that the human element of security is not as heavily emphasized.

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

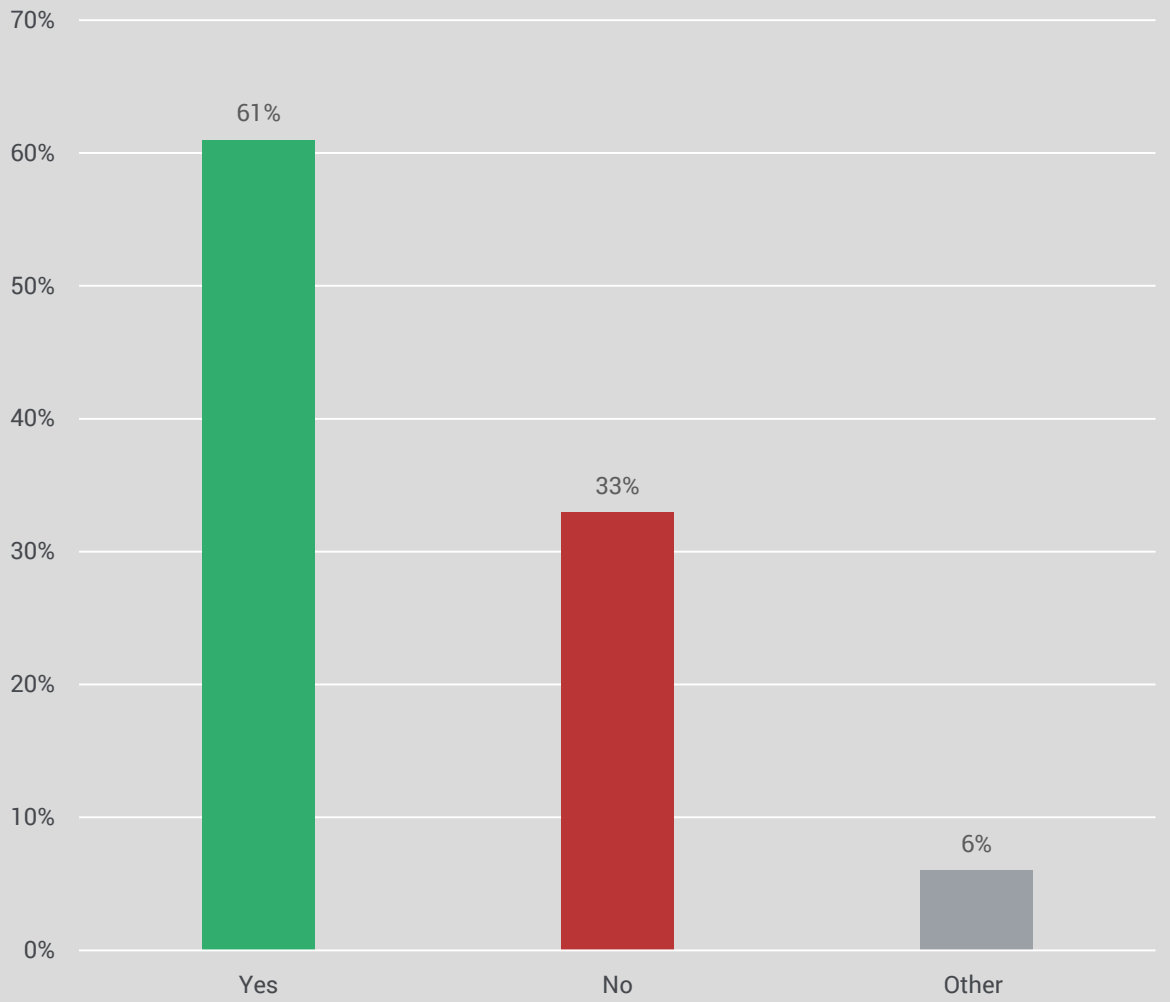


Security Controls Still Inadequate

Sanctioned Party Payments

- 1/3rd (33%) of corporates do not internally screen their payments for sanctioned parties at all.
- In the current environment, it is no longer just banks that are penalized for sanctions violations.
- In 2017, OFAC handed out $120 million in fines and penalties for sanctions violations, and many of these were levied against corporates rather than banks.
- Given the shifting compliance landscape and more responsibility on corporates, this is an exposure that must be addressed.

Corporates: (Regarding payments) Do you screen for sanctioned parties?



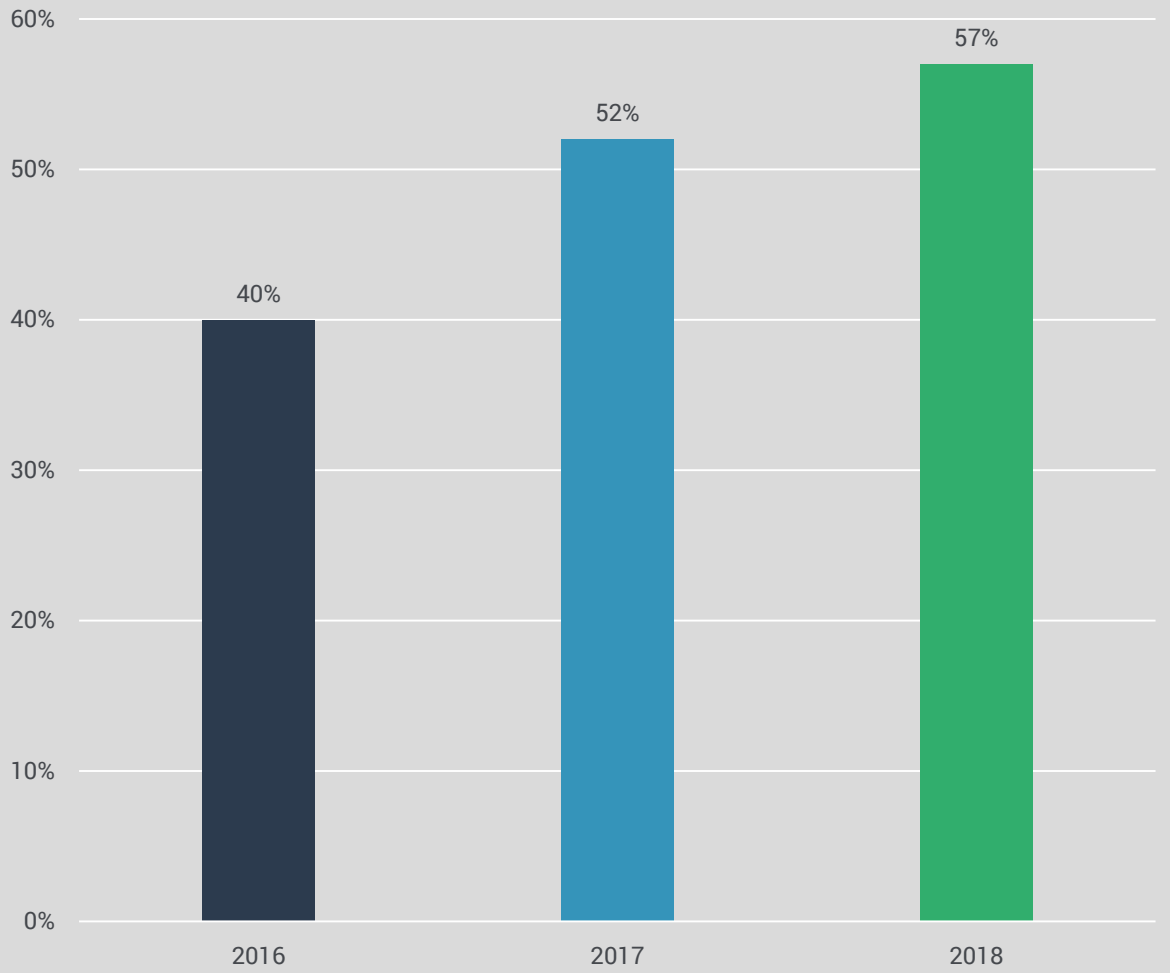
Fraud Experience

Fraud Experiences Rise

- In the three years that this survey has run, we have witnessed a dramatic rise in fraud activity perpetrated against the treasury environment.
- This represents a 40%+ year-over-year increase in just two years and drives home just how significant of a threat fraud has become.
- In today's world, more organizations experience fraud than those that don't; there is no excuse for firms not to have sophisticated control frameworks in place.

Have you experienced fraud in the last 12 months?

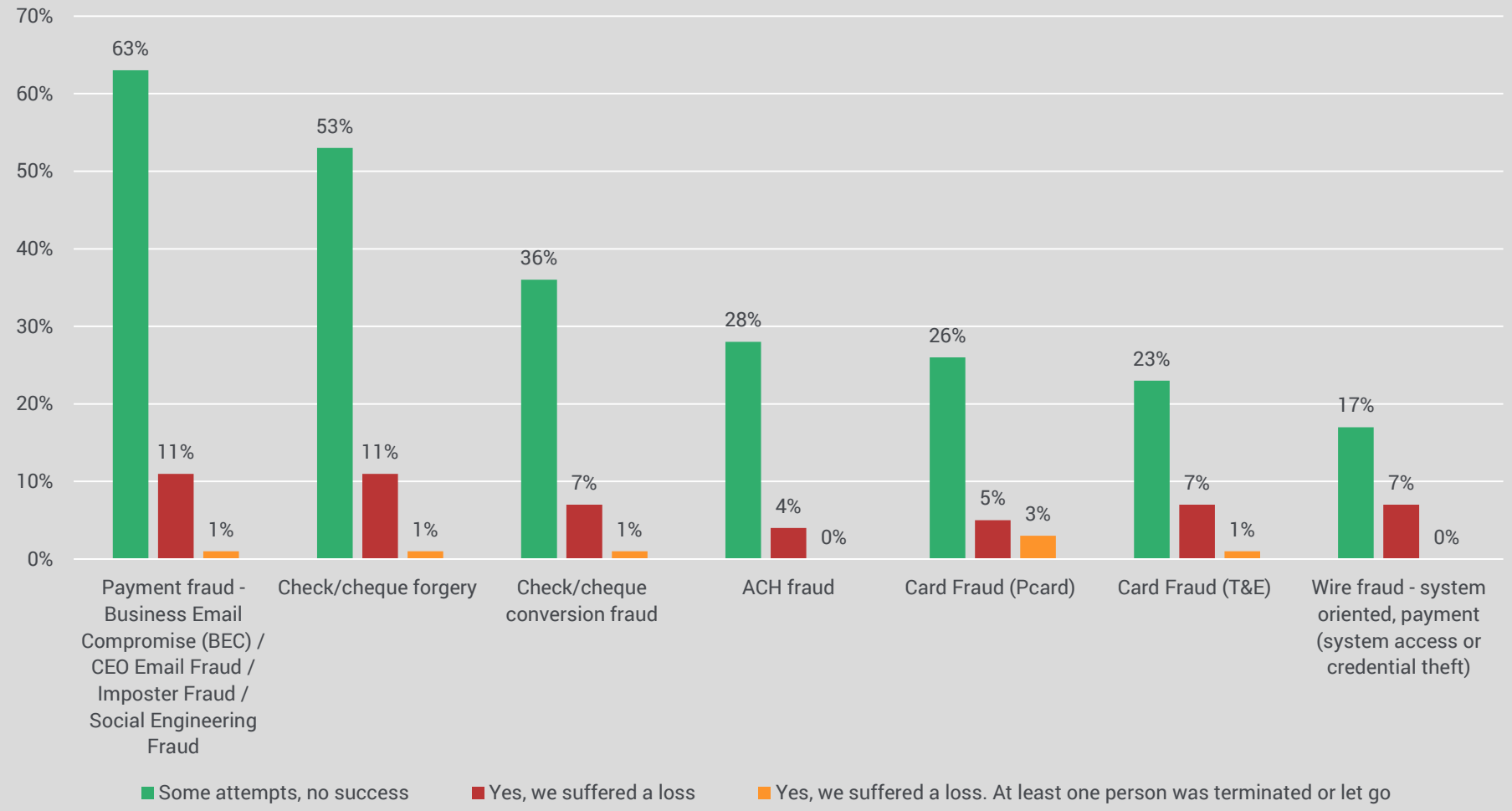
Data excludes "unsure" responses



Fraud Experience

Corporates: Have you experienced any of the following in the past two years?

Data excludes "unsure" responses

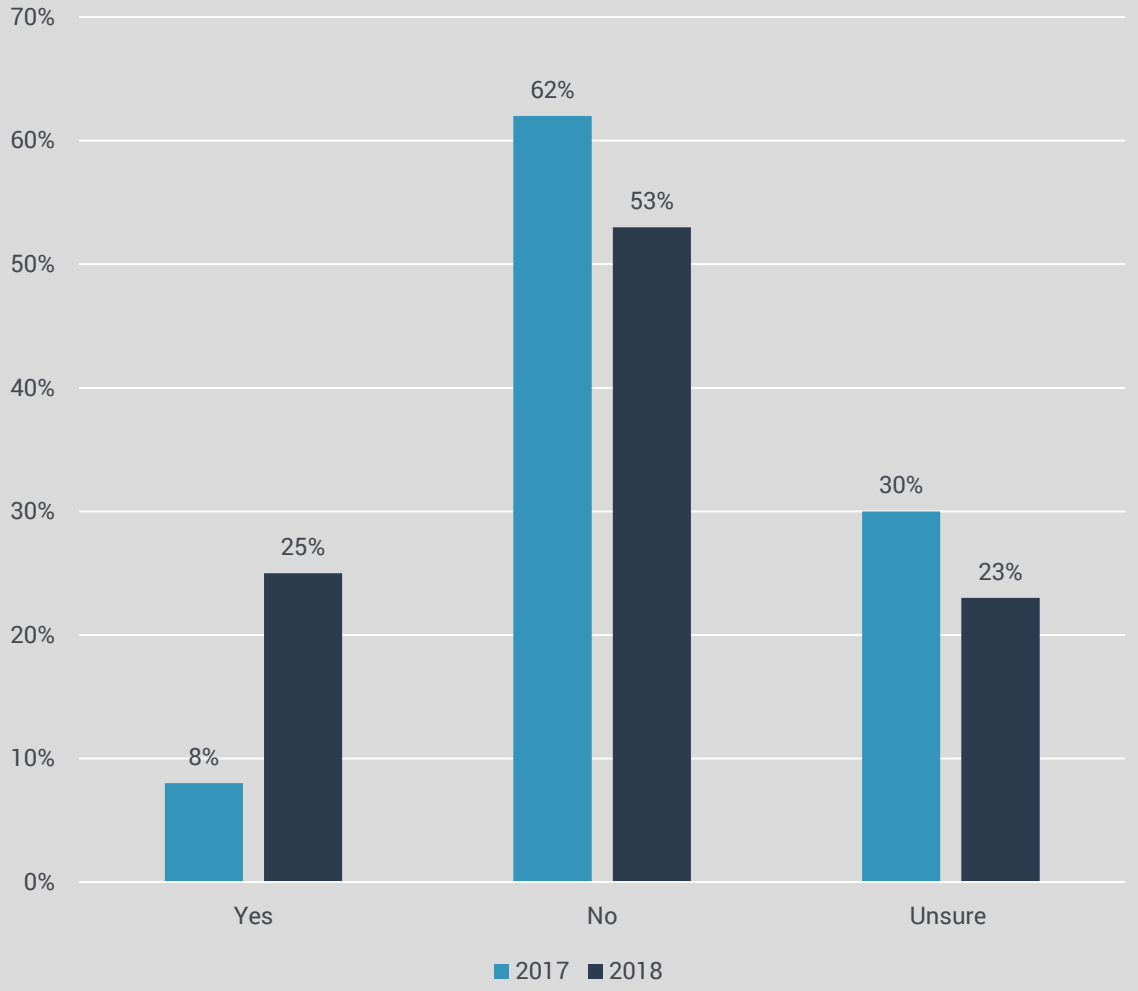


Fraud Experience

New Threats Surface: Ransomware

- In 2017, just before the massive Wannacry ransomware wave, only 8% of corporate practitioners had experienced a ransomware attempt.
- Today, 1 in 4 firms have experienced an attack. This represents a 300%+ rise growth in attacks in just a single year.
- This data pays testament to the fact that the criminal's playbook is constantly expanding and more sophisticated fraud techniques are regularly introduced to the fraud landscape.

Corporates: Have you experienced a ransomware attack in the past 2 years?

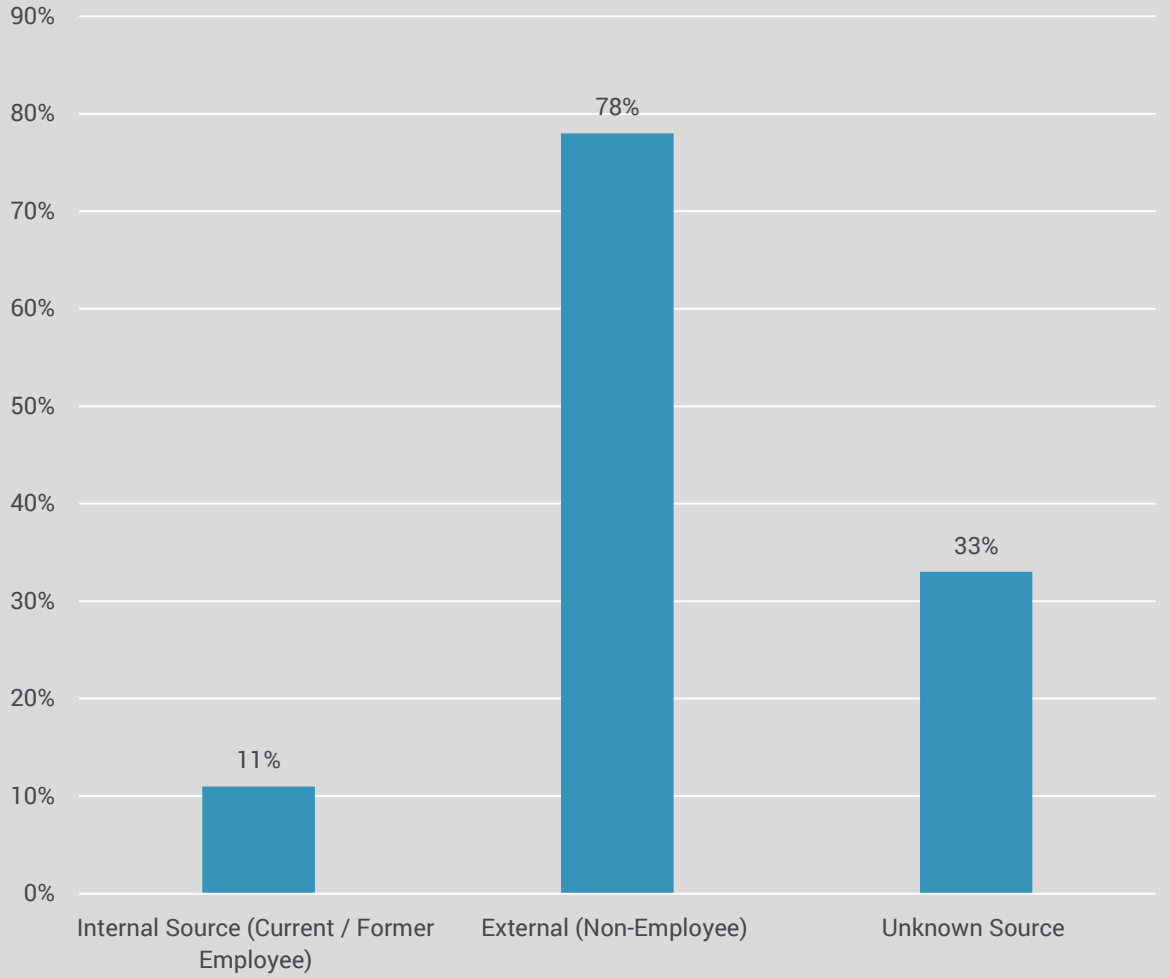


Fraud Experience

Where Did it Come From?

- Of those organizations that experienced fraud over the past year, 33% were not sure of the source for at least one of the attempts they experienced.
- One of the more concerning components associated with cyber fraud is that criminals can initiate attacks on corporations from entirely different world regions, which increases the difficulty of identifying the source.

Corporates: From Which Party Did You Experience Fraud? (Select all that apply)



Final Thoughts

Key Takeaways for Treasury

- **Weaknesses Still Exposed.** Many organizations have invested heavily in security tools and made decent progress. Yet, significant exposures remain.
- **Context, not Piecemeal.** Avoid the whack-a-mole response to fraud by examining all security layers within your framework and strategically implementing new controls as exposures arise.
- **No Time to Rest.** You are not done. Criminals are constantly learning and adapting; you should be too.

Action Items for Practitioners

Leverage your investments and defensive posture with security by :

1. ***Integrated**. Ensure enhancements are part of a comprehensive control framework.*
2. ***Both/And.** Update both human abilities and technology components of security. Get treasury and payment specific security training.*
3. ***Don't Overlook the Basics**. Items like cash visibility and reconciliations play vital roles in fraud prevention and detection.*
4. ***Anomalies Matter**. Monitor and manage system and processes for anomalous behavior.*

Contact Information & Survey Report Download

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

Email: craig@strategictreasurer.com
Direct: +1 678.466-2222

David Levine
Director of Product Marketing
Bottomline Technologies

Email: dlevine@bottomline.com
Direct: +1 603.501.5402

James Richardson
Head of Market Development, Risk & Fraud
Bottomline Technologies

Email: jrichardson@bottomline.com
Direct: +44 (0) 7595 241539

Link to Full Survey Report & Infographic

Thank you for participating in this event!