



Securing Treasury

The Real Numbers Behind the State of Fraud

Craig Jeffery, *Managing Partner, Strategic Treasurer*

Ernie Humphrey, *CEO & COO, Treasury Webinars*

About the Presenter

Connect on [StrategicTreasurer.com](https://www.StrategicTreasurer.com)   

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.



Ernie Humphrey, CTP

CEO & COO

Treasury Webinars

Ernie Humphrey currently serves as the CEO of Treasury Webinars and the CEO of 360 Thought Leadership Consulting. Ernie is a proven strategy and financial professional with 20+ years of experience. He has diverse industry knowledge as a seasoned corporate finance practitioner, a leader at the largest association for financial professionals (the Association for Financial Professionals (AFP)), and as a driving force behind the development of what was formerly the largest online community for senior level financial professionals (Proformative). During his career he has supported and delivered thought-leadership in the arenas of finance, treasury, accounting, and related disciplines.. Ernie has a BS and MS in Economics both from Purdue University.



→ The Corporate Treasury Situation

- Overall Situation: Challenges & Responsibilities
- Sample Complexity Considerations
- Fraud in the Spotlight
- The Criminal's Playbook

→ Corporate Fraud Experience

- Overall Fraud Experience
- Losses & Criminal Payouts
- Corporate Fraud Concerns & Investment Plans

→ Structuring a Defense Posture

- The Fraud Battlefield: Areas of Exposure
- Corporate Shortsightedness: Security Training
- Technology vs Human Security Components
- Four Pillars of Treasury Security

→ Case Studies: Successful vs Unsuccessful Security Approaches

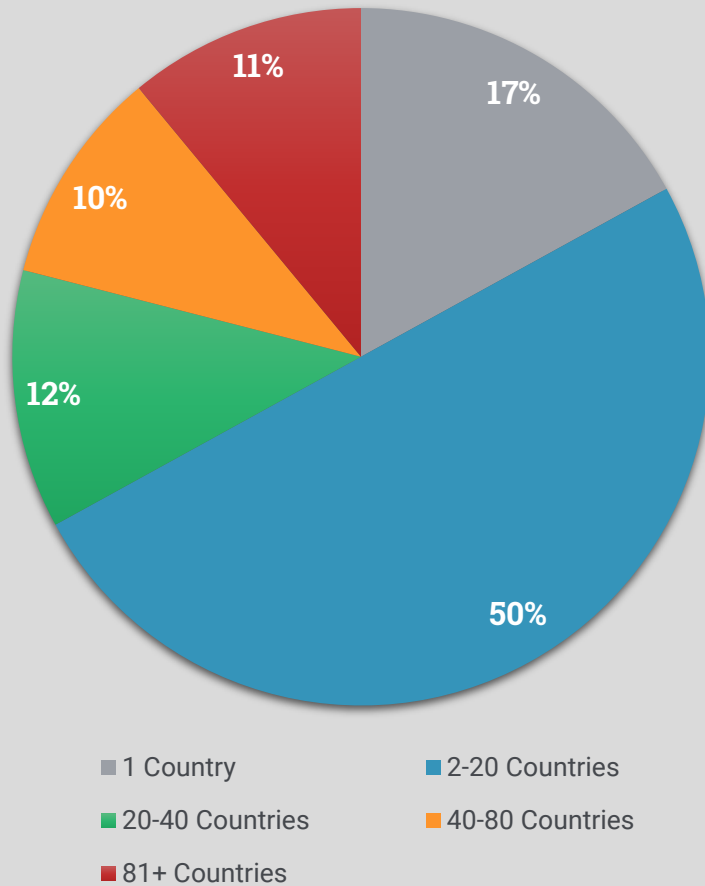
→ Key Technology Considerations for Treasury

Treasury's Situation: Responsibilities, Challenges, & Considerations

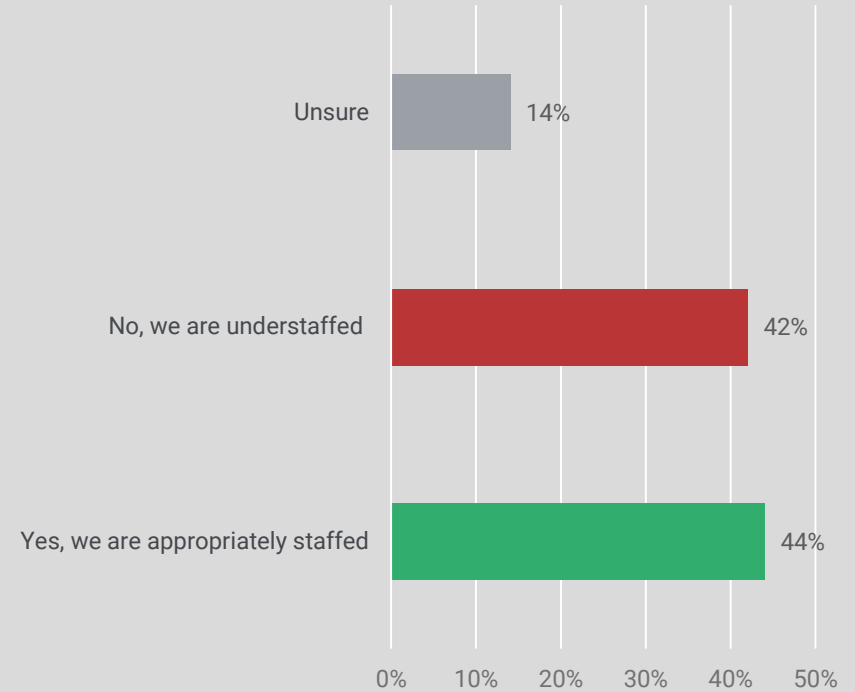


Sample Complexity: Globalization & Staffing

Our Business Operates in this many Countries: ¹



Are your staffing levels where they need to be now?²

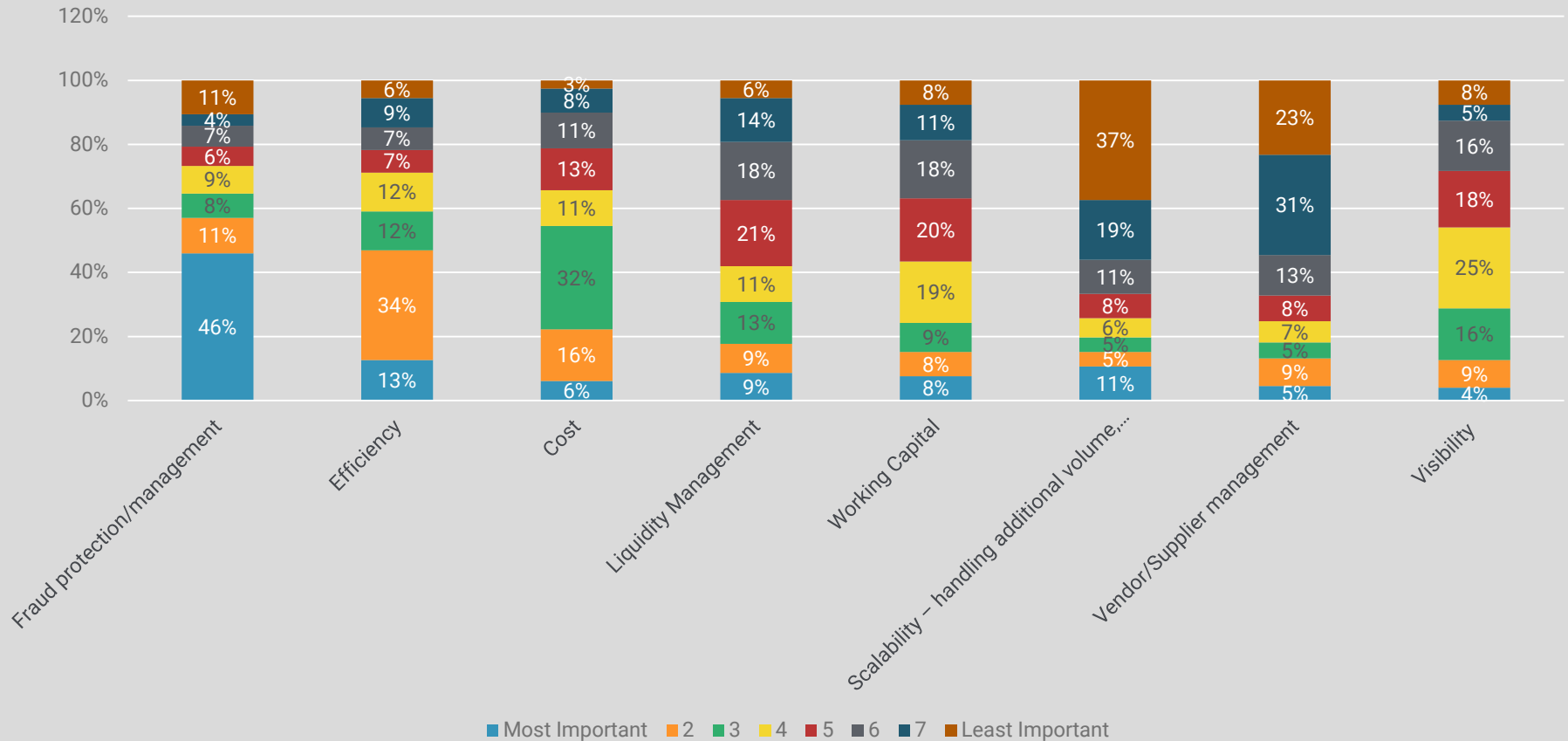


Lacking Numbers. When asked if their staff levels were where they needed to be, a sizeable portion of respondents to a 2017 survey saw themselves as understaffed.

Fraud: A Top Treasury Priority

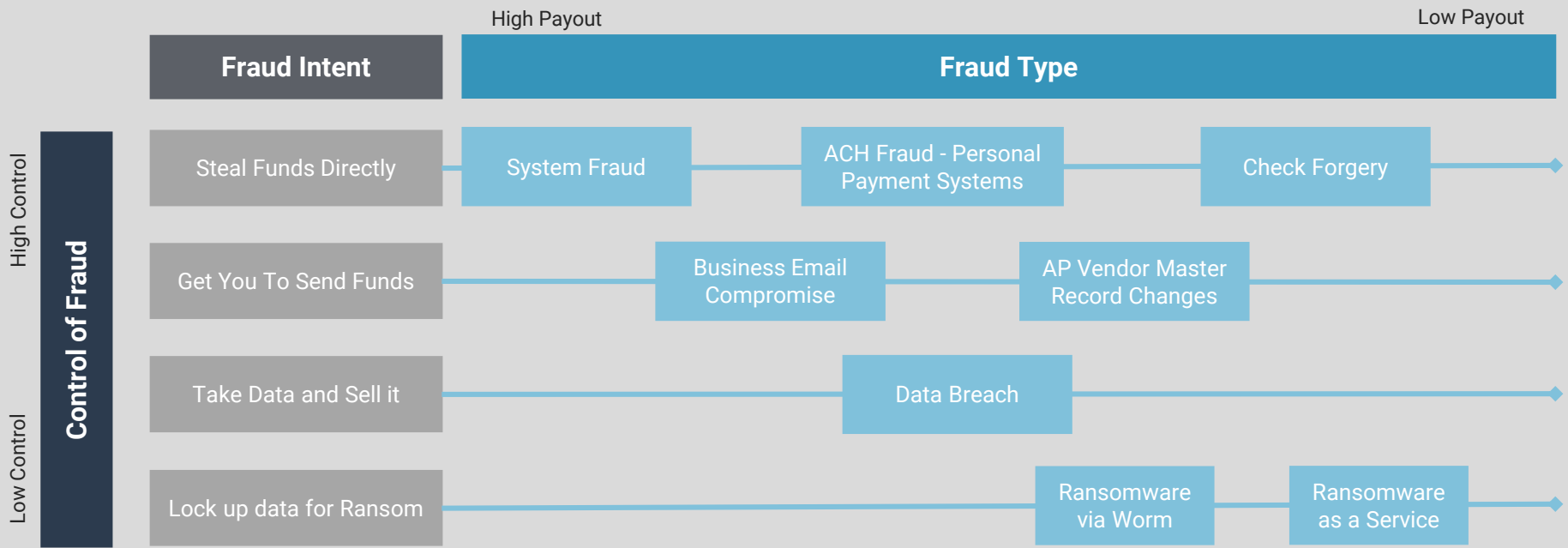
Connect on StrategicTreasurer.com   

Corporates: Rate the following payment initiative drivers on a scale from (1) most important to (8) least important. ³



Corporate Payment Drivers. In recent years, the growing threat of fraud has placed treasury’s security concerns at the top of their priority list. This is highlighted above when looking at corporate treasury payment drivers.

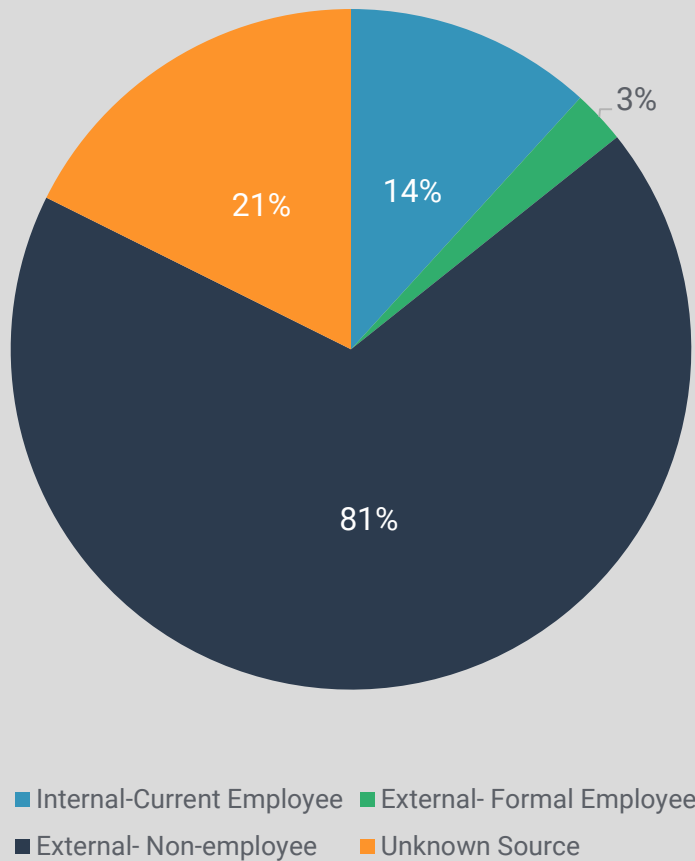
The Criminal's Playbook: Fraud Types & Associated Intentions



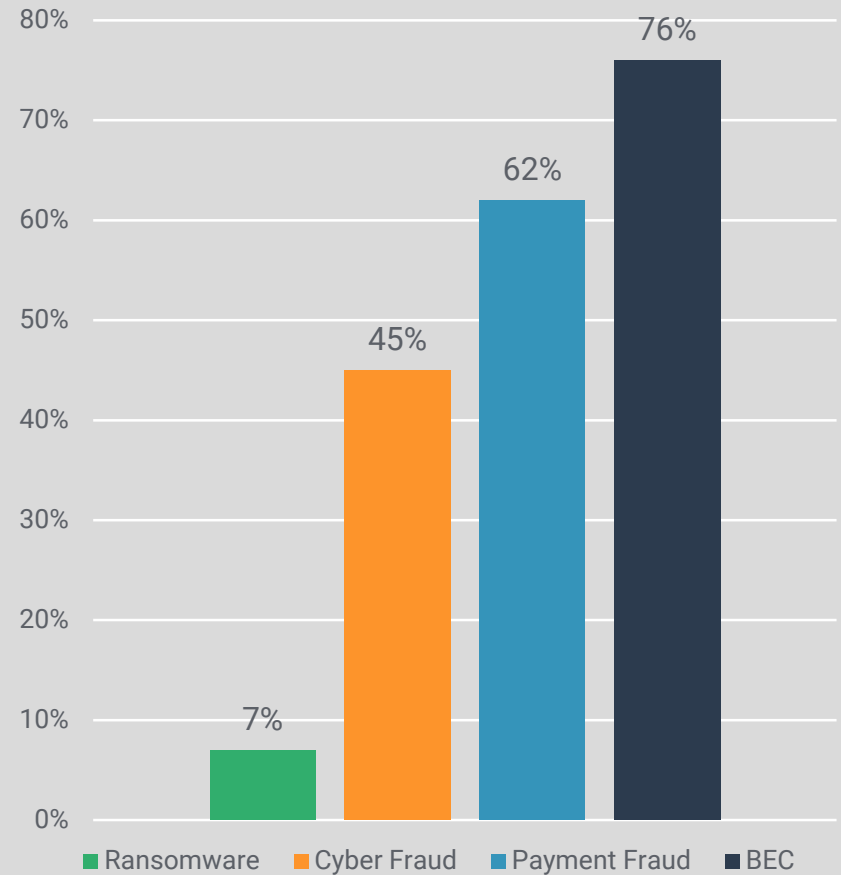
Surveying the Field: There are a wide variety of fraudulent methods for criminals to select from. If an organization is protected at one juncture, a criminal may move on to target them through another avenue or area of exposure. Due to the ever-evolving playbook of today's criminal, organizations must be constantly monitoring their operations to locate exposures and identify suspicious activity.

Corporate Fraud Experience

**Corporates: From Which Party did you Experience Fraud?
(Select all that Apply)⁴**



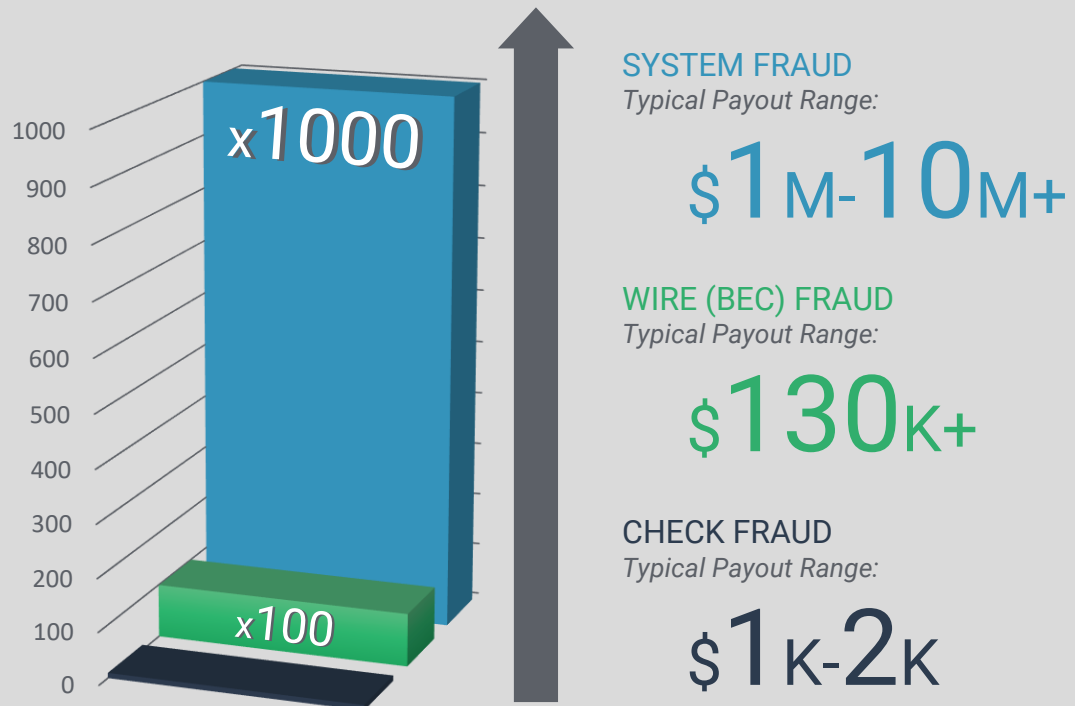
**Corporates: Fraud Experience by Type of Attack
(Over the last 1-2 Years (2016-2017))⁵**



Corporate Fraud: Criminal Payouts

Payouts are on the Rise

- Organizations are under constant attack from criminals trying to steal their funds through cybercrime, fraud, and other means . Over the past several years this has become a major concern for most firms, especially as the payouts associated with certain types of fraud increase.



*2017 Strategic Treasurer, Bottomline, Bank of America Merrill Lynch 2017 Treasury Fraud & Controls Survey

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

Fraud Concerns are Elevated

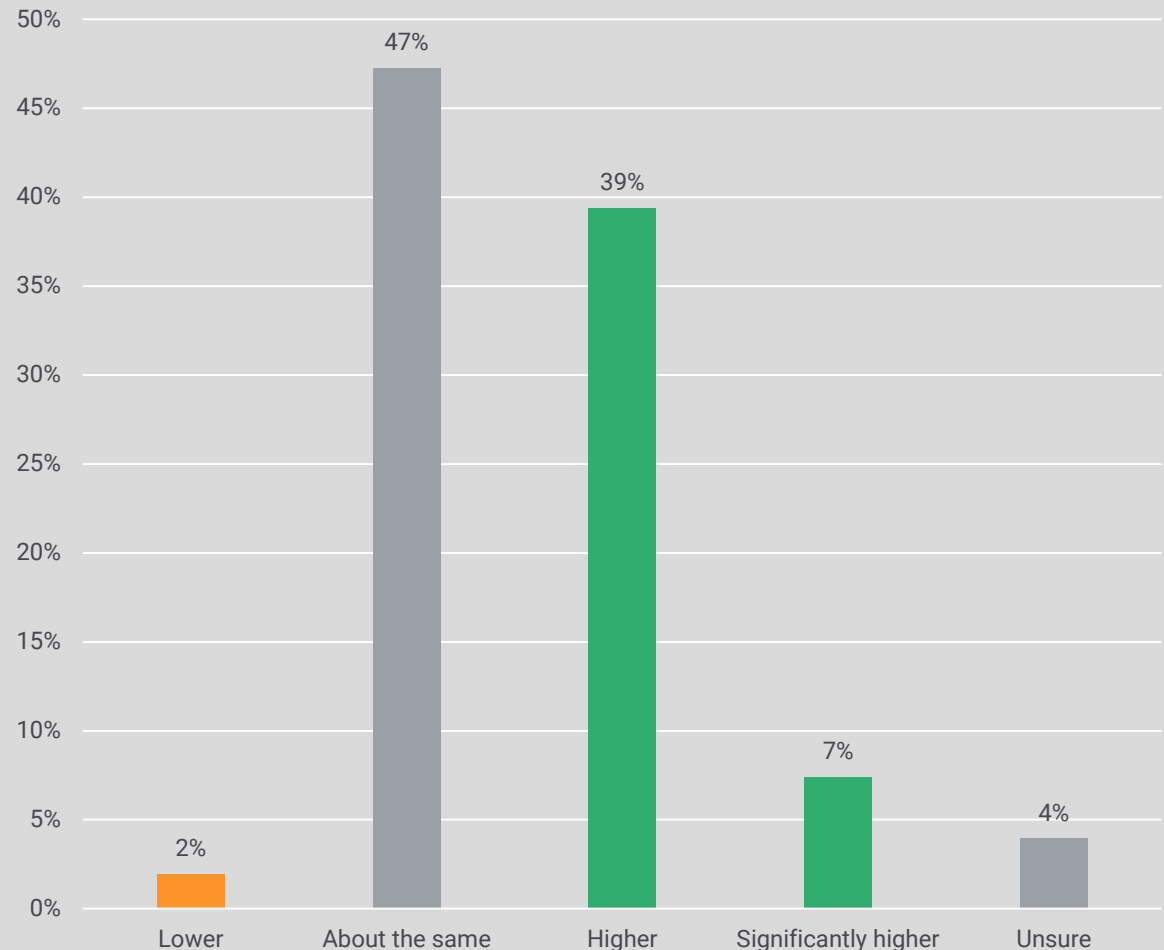
Connect on [StrategicTreasurer.com](https://www.StrategicTreasurer.com) [in](#) [v](#) [t](#)

Security Concerns Are Rising

- The frequency and severity in which fraud is striking the treasury environment has caused widespread panic amongst practitioners.
- 46% of respondents say that security concerns are higher or significantly higher than in previous years.
- Only 2% have lowered concerns.
- As security concerns rise, corporate practitioners must consider how they are going to prevent fraudulent attacks.

Payment Security Concerns ⁶

Our current payment security concerns, as compared to the prior year, are:



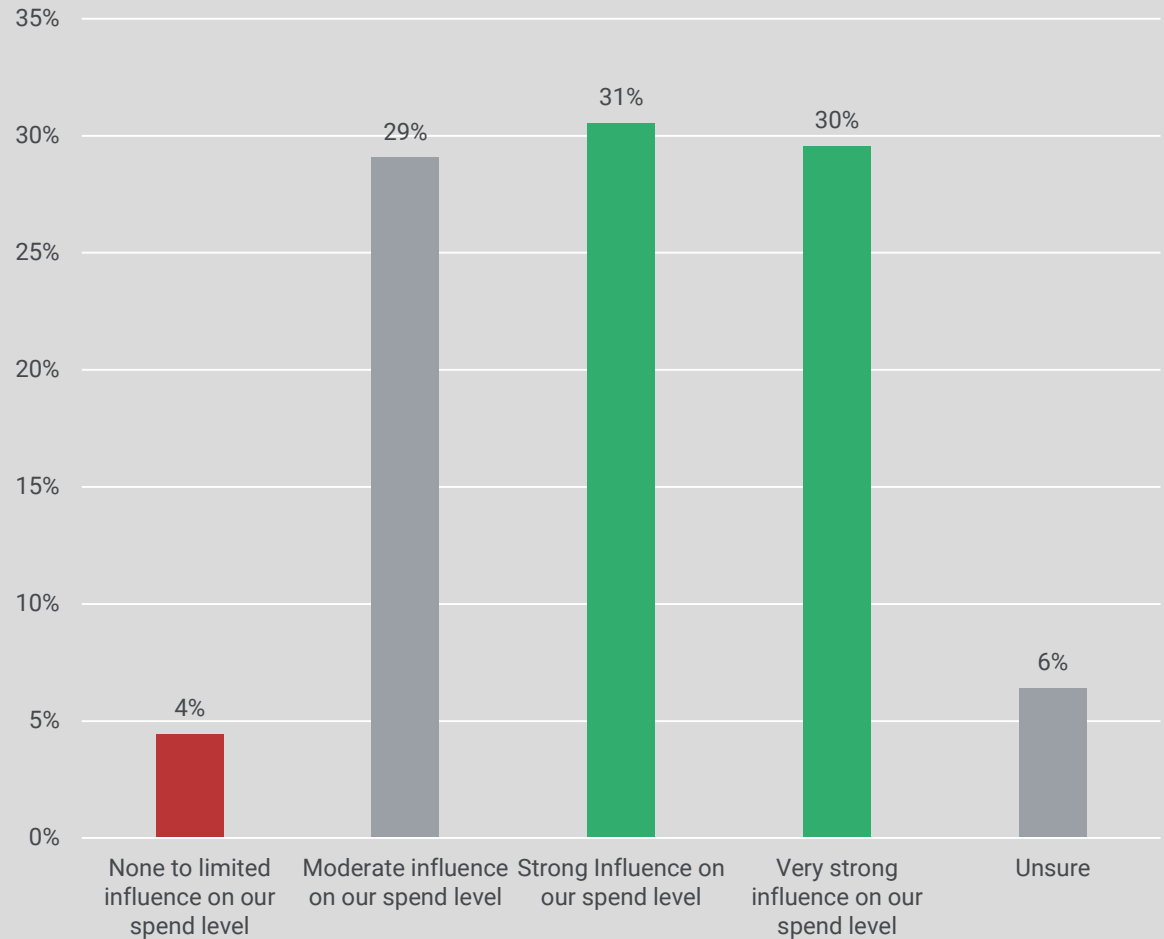
Fraud Concerns Influence Technology Spend

Security Concerns Influence Spending

- Not surprisingly, as fraud experience continues to climb, so to does the level of planned investment in security controls and technology.
- 61% of respondents say that security concerns have a strong or very strong influence on their technology spend.
- This shows that corporations are making serious investments in technology that enhances fraud detection and prevention.

Impact of Security on Spend ⁷

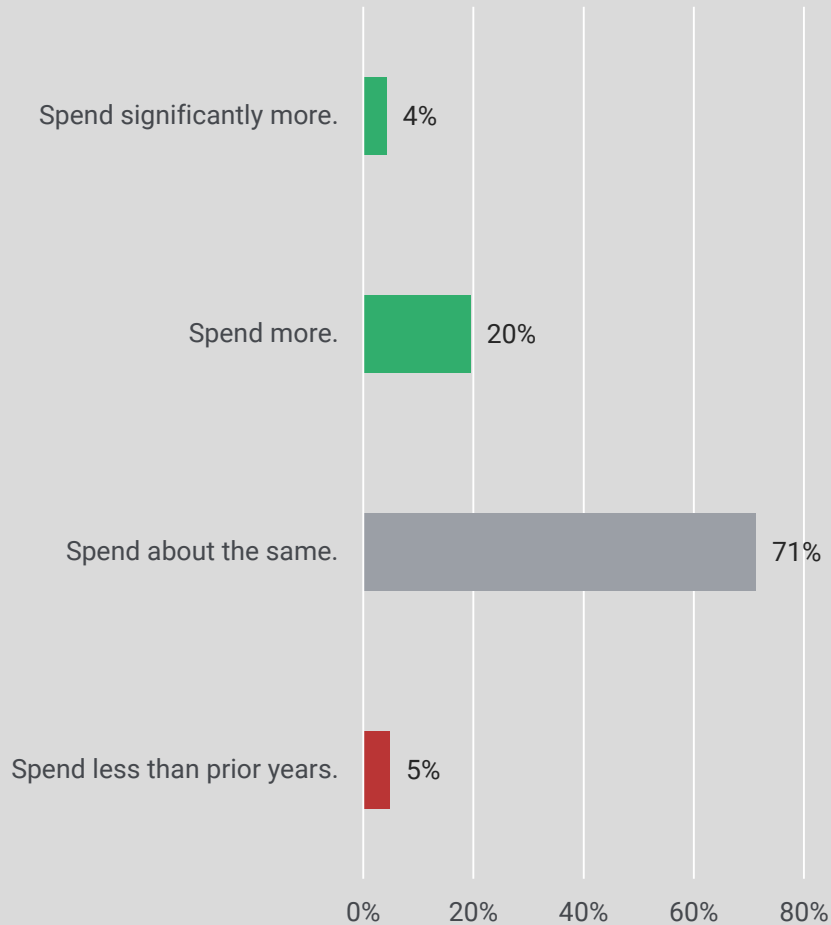
What influence do security concerns have on your current or planned technology spend?



Scope of Security Investments

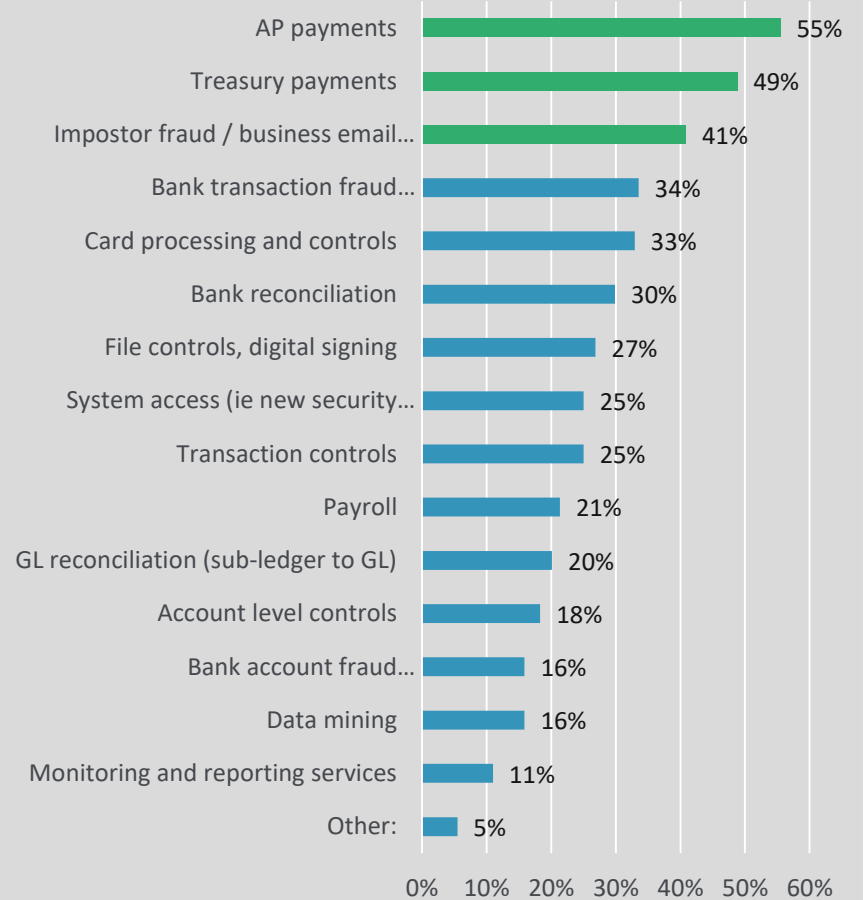
Spend Plans: Treasury Security Controls ⁸

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

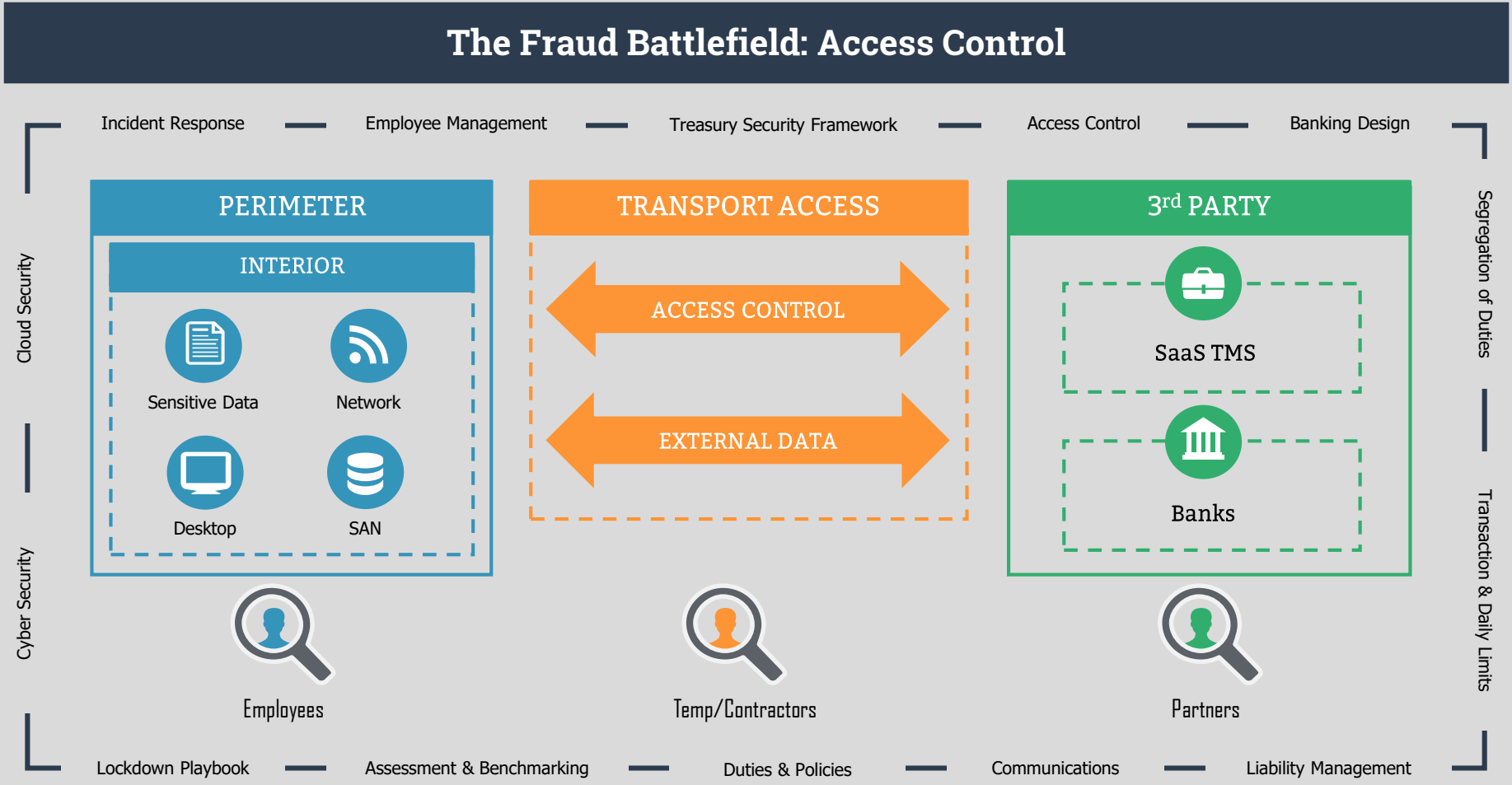


Spend Plans: Treasury Security Controls ⁹

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



The Fraud Battlefield



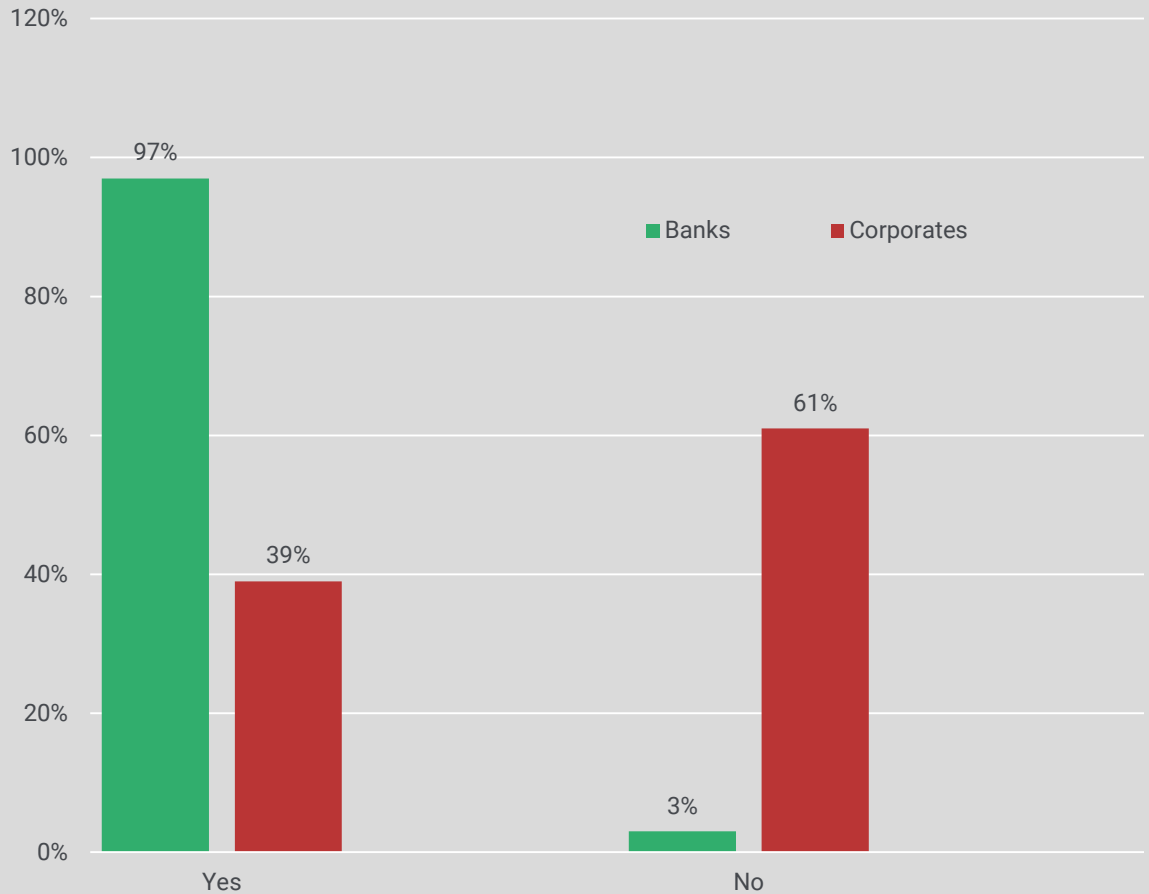
Exposure: Corporate Security Training

Corporate Security Practices

- Although corporates have indicated a willingness and intent to spend significantly on treasury security, there are still large areas of exposure.
- Currently, only 39% of corporates require employees involved in payments to take security training every year.
- This represents a major area of weakness and vulnerability.

Corporate vs Bank Security Training ¹⁰

Do you require employees involved in payments to take security training each year?



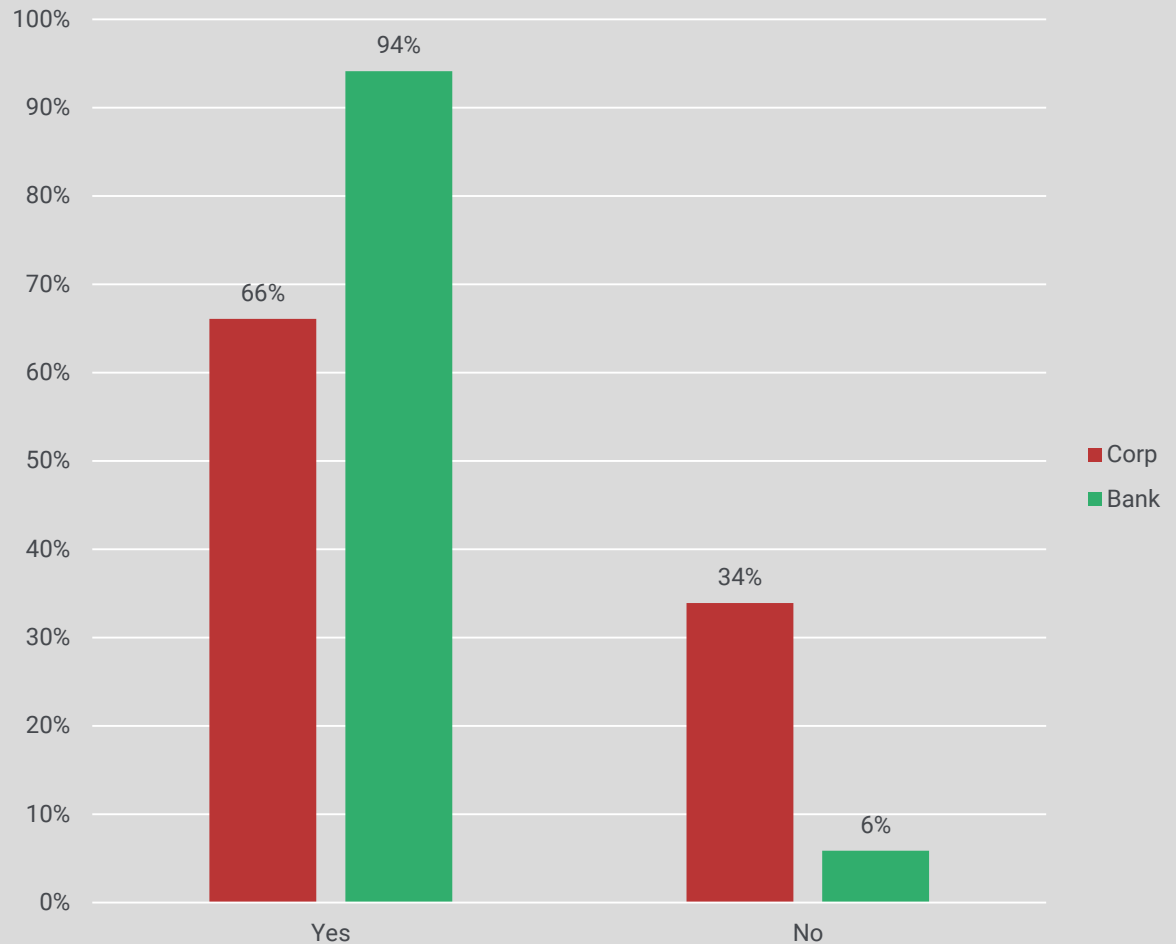
Strategic Treasurer & TD Bank Treasury Perspectives Survey

Bank vs. Corporate Security Testing

Corporate Security Practices









- Even when looking at those firms that *do* require regular training, the scope of their courses fall short compared to banks.
- Over 1/3rd of corporates that require regular training have not incorporated a testing component into their courses.
- Testing involves either a scored quiz/test, or may involve tests such as “fake” phishing emails sent to employees to see how they handle such messages.
- Corporates must learn to combine technology components of security with human elements.

Does this training have a reported testing component? ¹¹










Technology vs. Human Security Components

Technology Security Components

-  **Antivirus Software**
-  **Firewall**
-  **Multifactor Authentication**
-  **User Monitoring Tools**
-  **Biometrics**
-  **Encryption**
-  **Tokenization**
-  **SAML 2.0**

Human Security Components

-  **Security Training (Regularly)**
-  **Employee Testing (Phishing emails)**
-  **Whistleblower Policy**
-  **Clean Desk Policy**
-  **Dual Controls**
-  **Segregation of Duties**
-  **Principle of Least Privilege**

Case Study

Case Study: Fraud WITH Security Training



Fraudulent Activity Initiated. A criminal gained access to a corporate CFO's email address and initiated several payment requests via email to a treasury employee. The messages were made to sound urgent.



Suspicious Request Identified. The treasury employee noticed the unusually urgent language and did not recognize the payment details provided in the email. The employee did not post the payment and instead contacted his superiors for further verification.



Losses Prevented. Further analysis led to the discovery that the payments were indeed fraudulent and that the CFO's email credentials had been compromised. Due to the employee's training on how to identify suspicious requests, fraudulent losses were prevented.

Case Study: Fraud WITHOUT Security Training



Fraudulent Activity Initiated. A treasury employee receives an email from a current vendor requesting that future payments be sent to a new bank account.



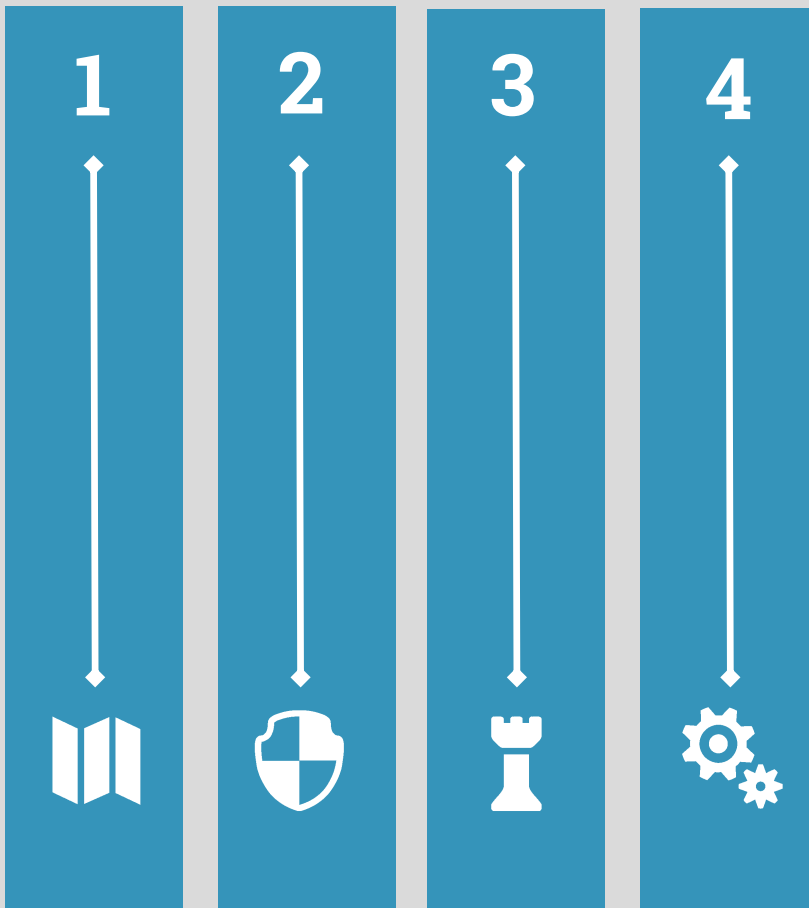
Suspicious Details Undetected. Although there were several minor typos in the message, the email address was correct and this vendor had changed their payment information before, so the employee follows through with the request.



Fraudulent Losses Sustained. As a result, the next two payments to the "vendor" are delinquent, and further analysis discovers that both payments were delivered to a fraudulent account instead of the vendor's actual account.

Developing a Security Framework

Four Pillars of Treasury Security



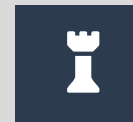
1. ASSESS & ARCHITECT

- Greater Awareness
- Assess Major Exposure Risks
- Understand Required Layers
- Regular Revision
- Ongoing Monitoring
- Market & Situations



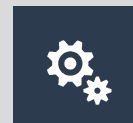
2. PREPARE & PREVENT

- Stronger Defense Posture
- Upgrade Processes
- Systems
- Staff Knowledge



3. MANAGE PROCESSES






- Maintain & Reinforce Position
- Ongoing Training
- Testing



4. REMEDIATION

- Respond & Recover
- Reporting
- Response (Fast, Appropriate)
- Rework (Restore to New Model)

Key Security Points for Treasury

-  Although corporate treasury faces a wide array of responsibilities and challenges, **fraud and security have become a top priority** as attacks increase in frequency and severity.
-  Innovations to techniques and methods by which criminals perpetrate fraud has resulted in a landscape where **criminal payouts can reach millions of dollars in some circumstances**.
-  As the threat of fraud is elevated, **corporates have indicated a strong intent to invest heavily in multiple areas of the technology components of their security infrastructure**.
-  Despite these technology investments, however, **many firms continue to leave themselves exposed by failing to implement staff security training and testing**.
-  **Treasury must learn to balance the technology components of their security infrastructure with human components** – failing to secure either sector can result in large and dangerous exposures.



Craig A. Jeffery, CCM, FLMI

Founder & Managing Partner

Strategic Treasurer

Email: craig@strategictreasurer.com

Direct: +1 (678) 466-2222



Ernie Humphrey, CTP

CEO & COO

Treasury Webinars

Email: Ernie@360thoughtleadership.com

Direct: +1 (260) 494-2210

Thank you for participating in this event!

Works Cited

1. 2017 Strategic Treasurer, Bottomline Technologies, & Bank of America Merrill Lynch B2B & WCM Strategies Survey
2. 2017 Strategic Treasurer Higher Ed Survey
3. 2016 Strategic Treasurer & Fides Global Payments Survey
4. 2017 Strategic Treasurer & Bottomline Technologies Treasury Fraud & Controls Survey
5. 2017 Strategic Treasurer & Bottomline Technologies Treasury Fraud & Controls Survey
6. 2017 Strategic Treasurer, Bottomline Technologies, & Bank of America Merrill Lynch B2B & WCM Strategies Survey
7. 2017 Strategic Treasurer, Bottomline Technologies, & Bank of America Merrill Lynch B2B & WCM Strategies Survey
8. 2017 Strategic Treasurer & Bottomline Technologies Treasury Fraud & Controls Survey
9. 2017 Strategic Treasurer & Bottomline Technologies Treasury Fraud & Controls Survey
10. Strategic Treasurer & TD Bank Treasury Perspectives Survey
11. Strategic Treasurer & TD Bank Treasury Perspectives Survey