



# Fraud & Security in 2018

The Why & How of Securing Treasury & Payments

**Craig Jeffery, Strategic Treasurer**

Tuesday, September 11<sup>th</sup>, 2018

2:00 PM EST

# 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.



**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 issues, they efficiently identify issues, creatively explore ideas and options, and provide effective solutions and implementations for their valued clients.



# Topics of Discussion



## ↳ Treasury's Situation

## ↳ Treasury's Experience with Fraud

- *Escalating Fraud Activity*
- *Types of Fraud Experienced*
- *Success Rates & Losses Sustained*

## ↳ Assessing the Fraud Environment

- *The Fraud Battlefield*
- *The Criminal's Playbook*

## ↳ Security Considerations for Treasury

- *IT vs. Treasury Considerations*
- *Human vs. Technology Components*
- *12 Key Security Principles*
  - *Dual Controls & Multi-factor Authentication*
  - *Principle of Least Privilege*
  - *Awareness, Testing, & Training*

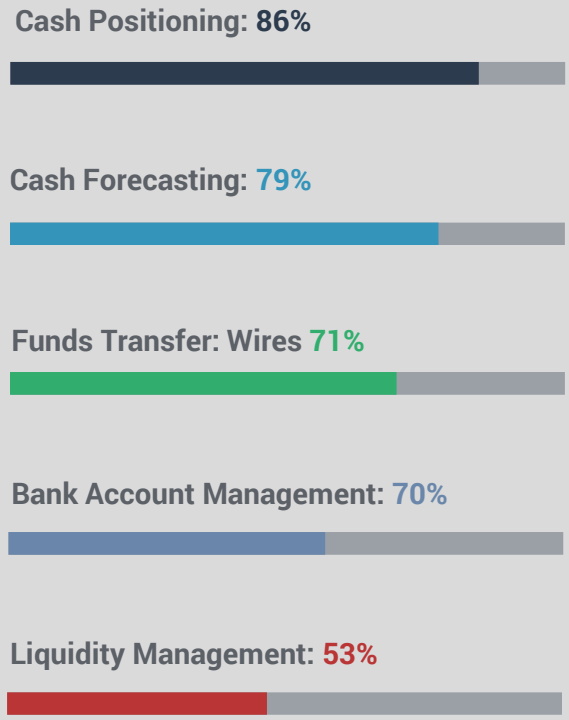
## ↳ Final Thoughts, Key Takeaways

# Treasury's Situation

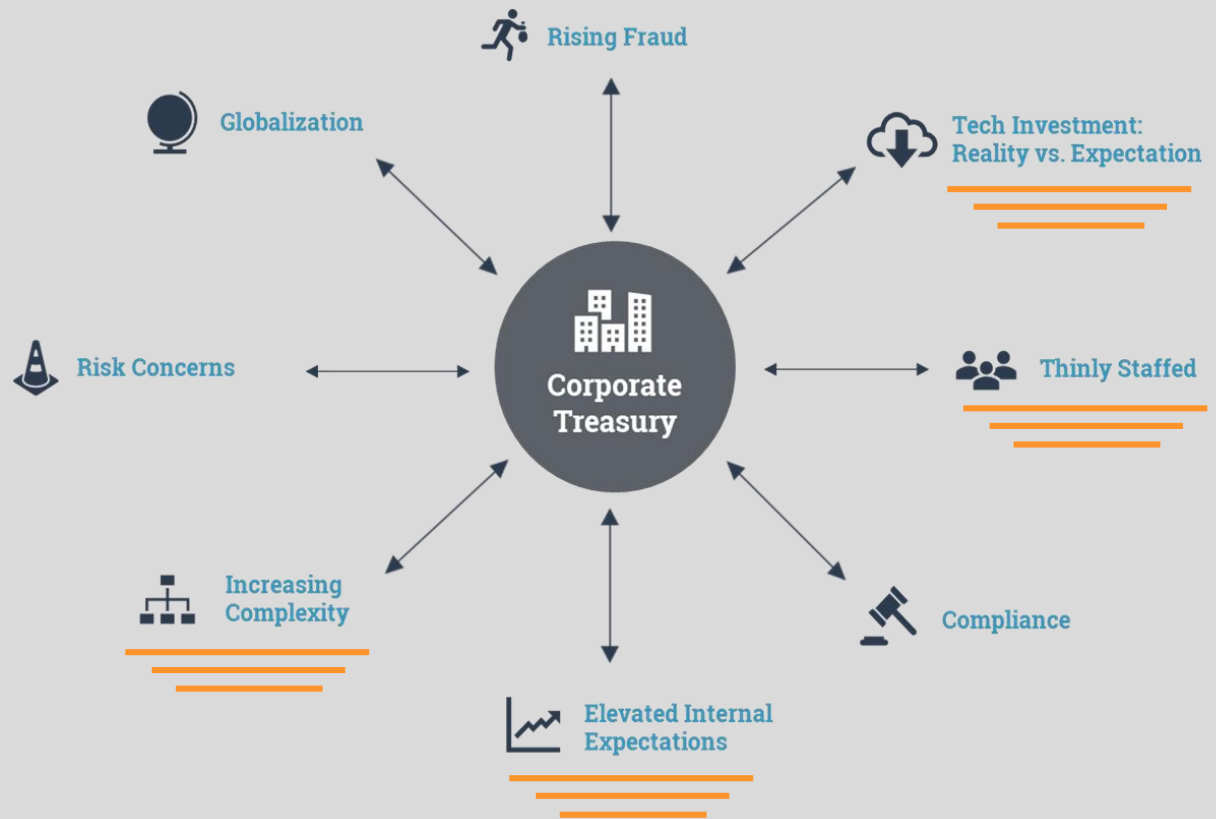
## Top Treasury Responsibilities

What functions do you use or need in treasury? (Select all that apply)

*\*Not all answer choices shown below*



## Treasury's Situation: Challenges & Considerations

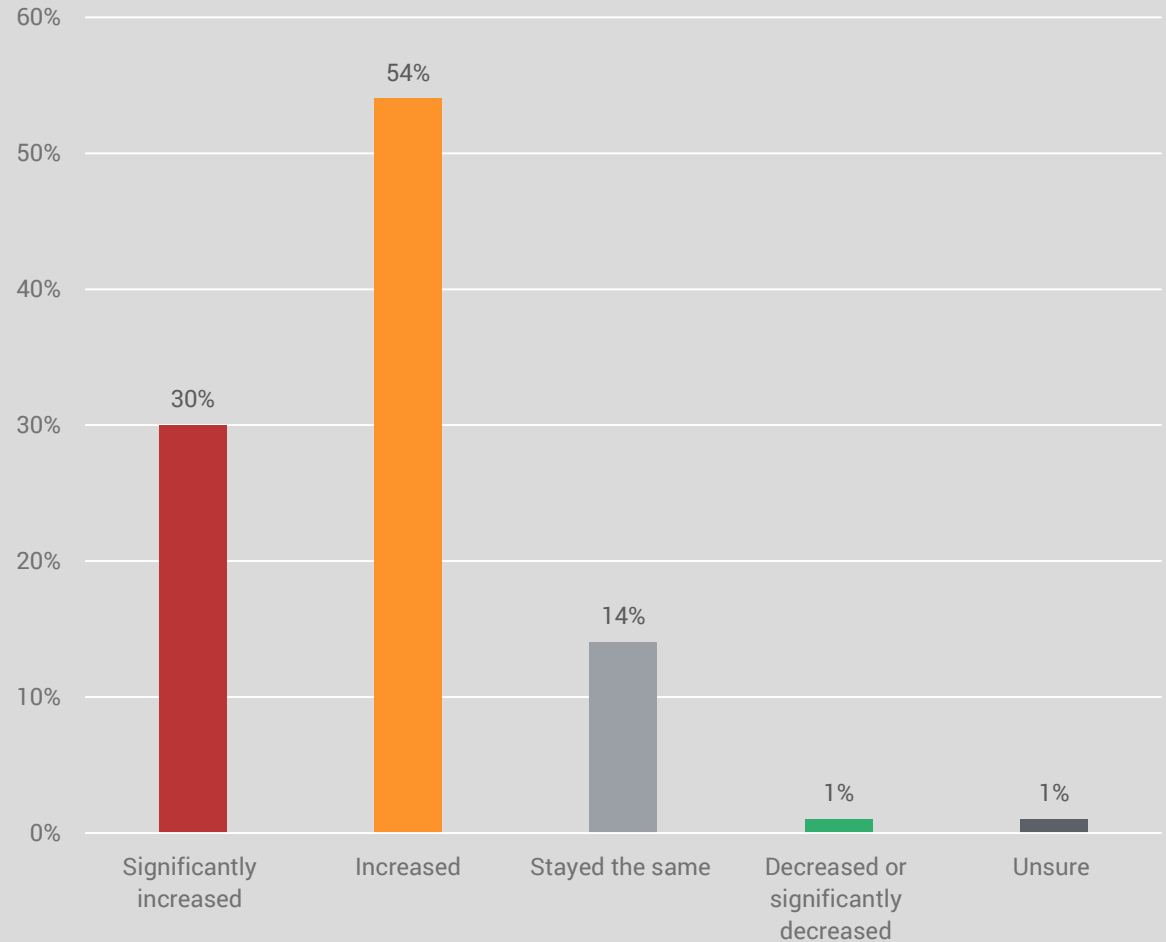


# Treasury Experiences with Fraud

## Escalated Threat

- Comparing 2018 to 2017, the vast majority (84%) of treasury practitioners believe the threat of cyber and payments fraud has increased.
- Only 1% believe that the threat has decreased.
- These figures highlight the extreme levels of concern towards fraud within the treasury environment.

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



2018 Strategic Treasurer & Bottomline Technologies Treasury Fraud & Controls Survey

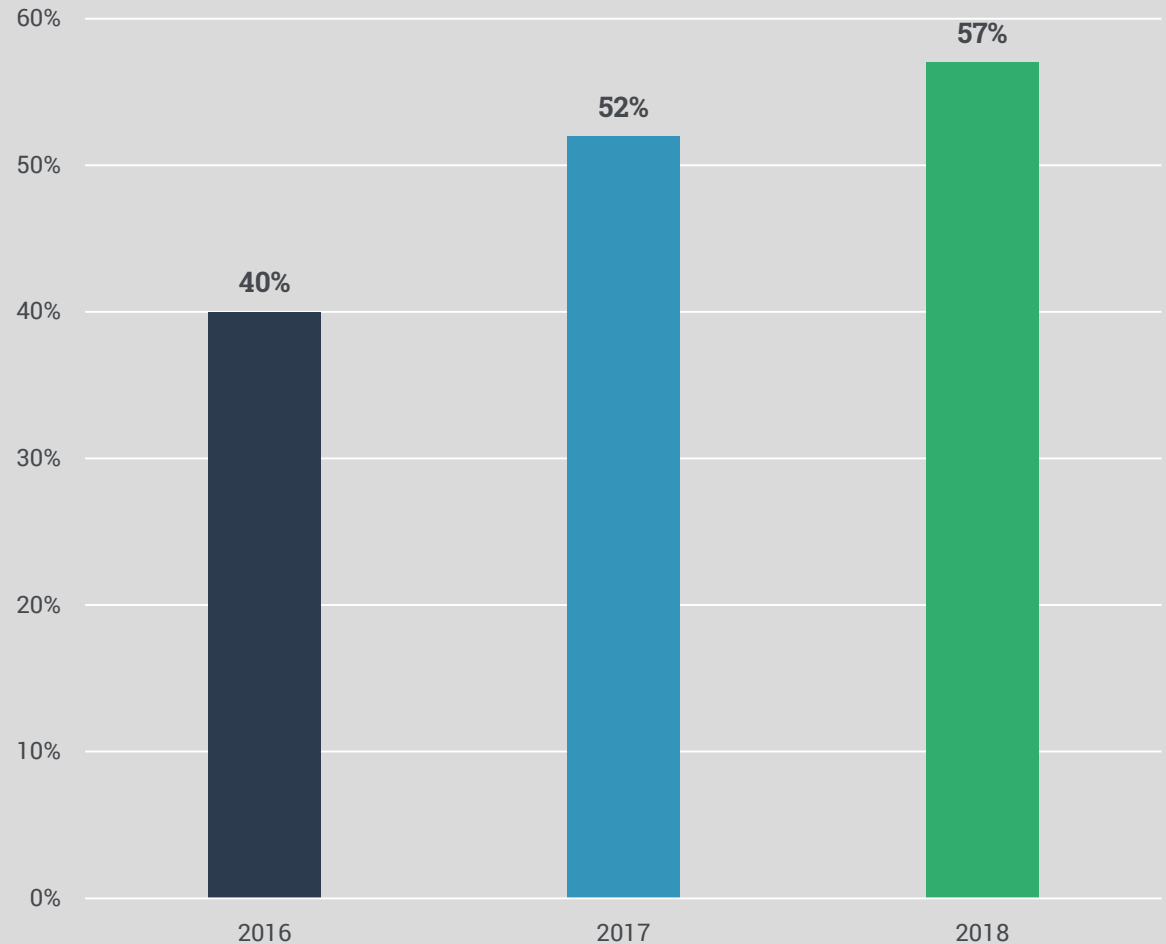
# Treasury Experiences with Fraud

## Fraud Experiences Rise

- Looking at organizations' fraud experiences, it appears that practitioners are correct in their beliefs that fraudulent threats have increased.
- These figures represent a 17% overall increase (40%+ year-over-year) in fraud experience since 2016.
- Today, more organizations experience fraudulent attacks than those that don't.

## Have you experienced fraud in the last 12 months?

Data excludes "unsure" responses



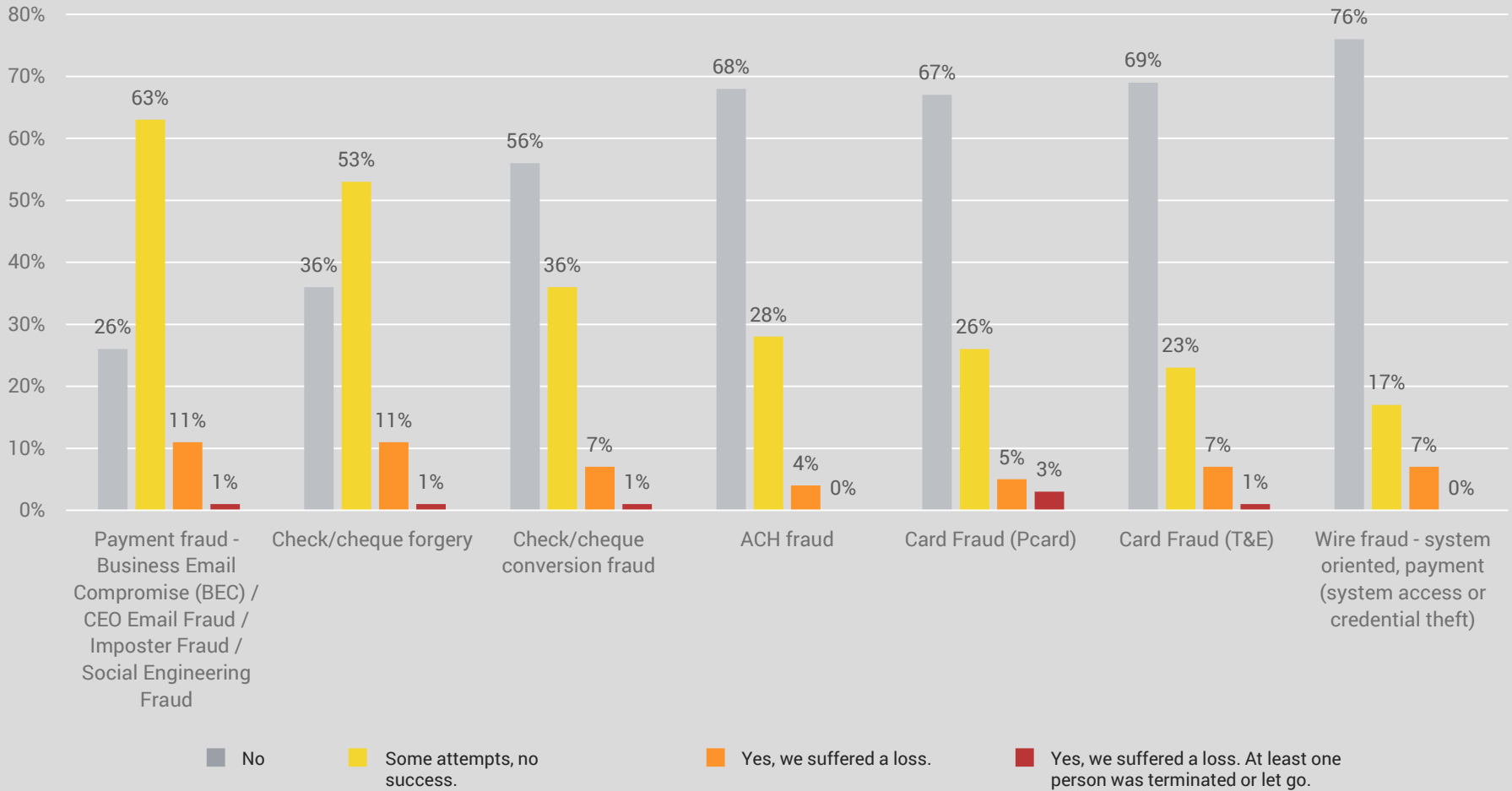
2018 Strategic Treasurer & Bottomline Technologies Treasury Fraud & Controls Survey

# Treasury Experiences with Fraud

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

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

Data excludes "unsure" responses

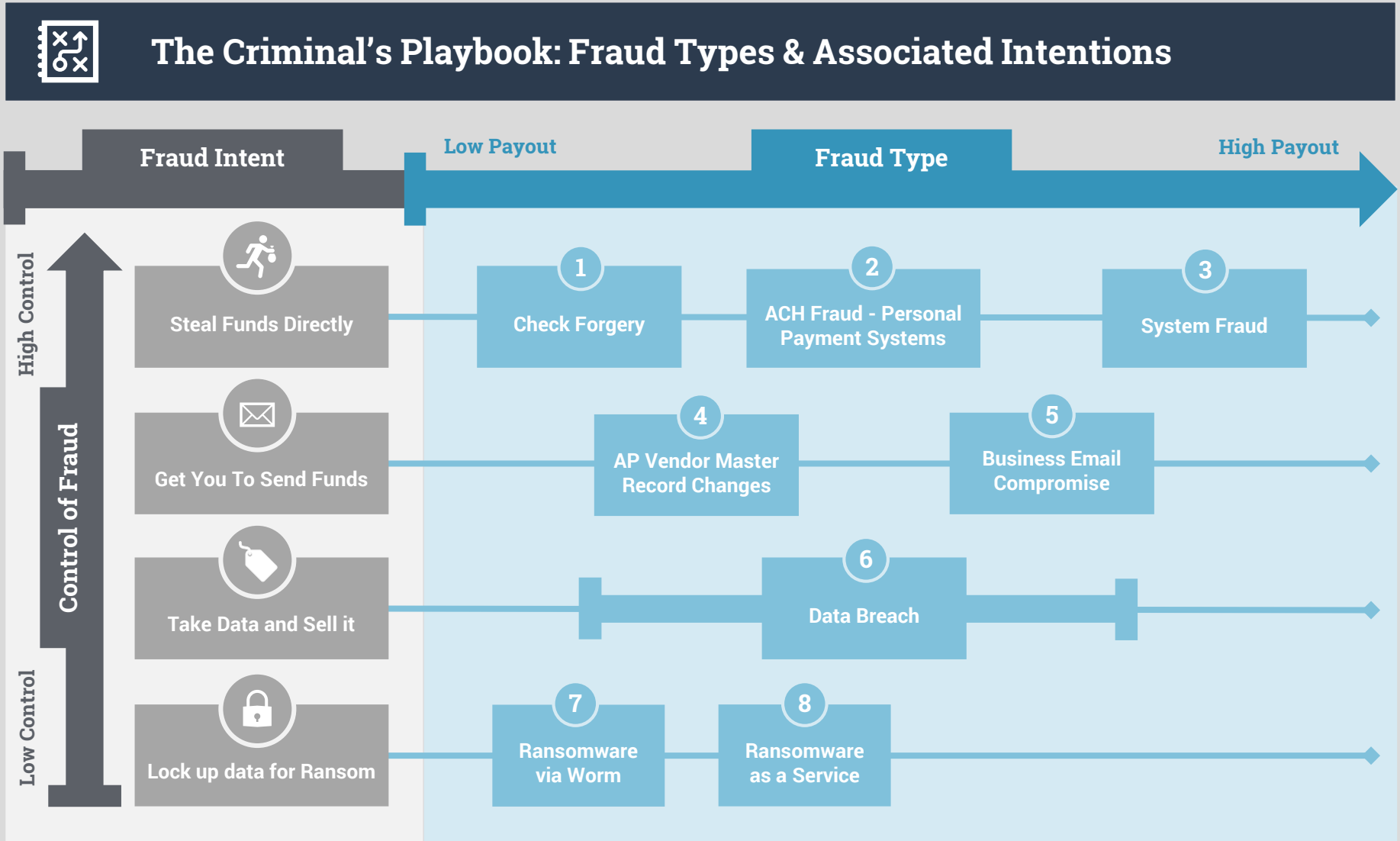


2018 Strategic Treasurer & Bottomline Technologies Treasury Fraud & Controls Survey



# The Criminal's Playbook

Connect on [StrategicTreasurer.com](http://StrategicTreasurer.com)   

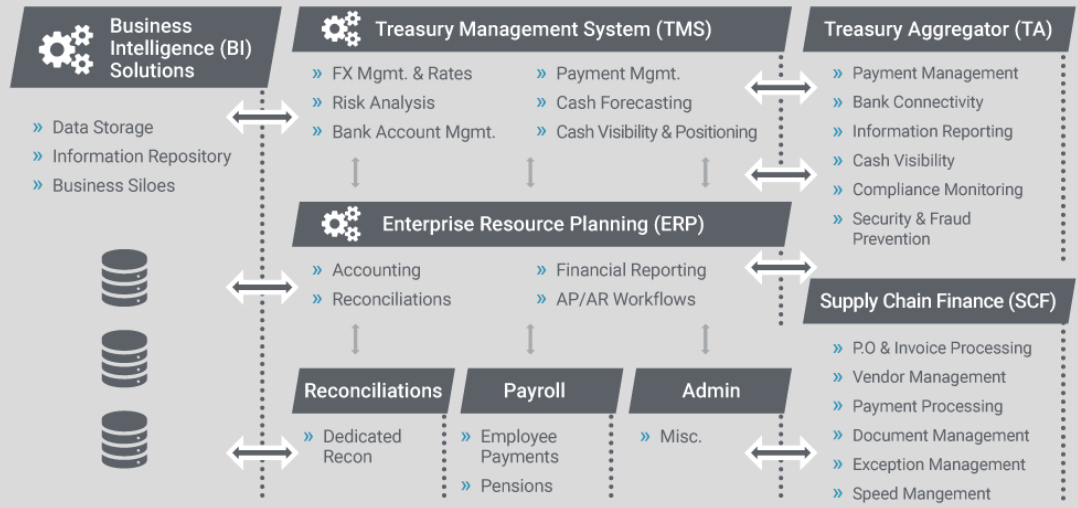




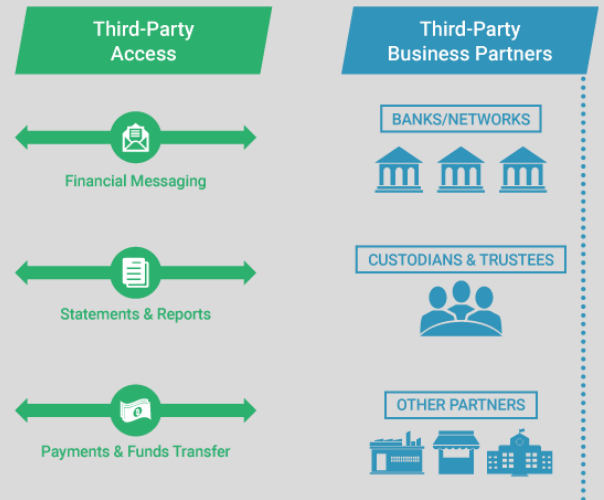
# The Fraud Battlefield

## The Fraud Battlefield: Access Control

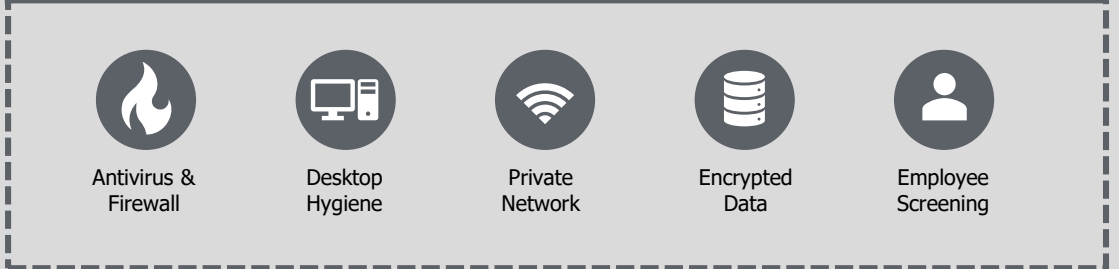
### Organization Perimeter / Interior



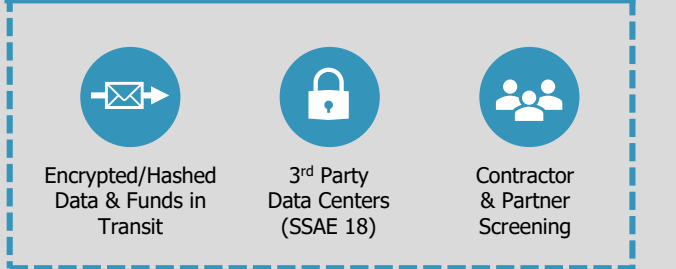
### Exterior Environment



### Security Elements











### Security Elements










# Human vs. Technology Components of Security

## Technology Security Components

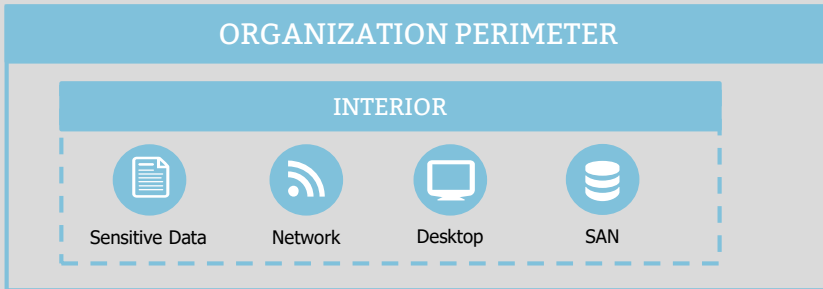
-  Antivirus Software
-  Firewall
-  Multifactor Authentication
-  User Monitoring Tools
-  Biometrics
-  Encryption
-  Tokenization
-  SAML 2.0

## Human Security Components

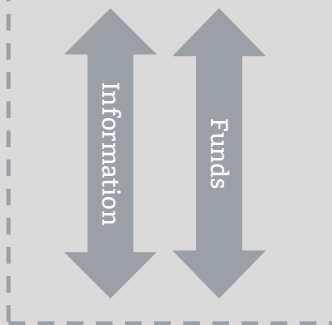
-  Security Training (Regularly)
-  Employee Testing (Phishing emails)
-  Whistleblower Policy
-  Clean Desk Policy
-  Dual Controls
-  Segregation of Duties
-  Principle of Least Privilege

# Security Considerations: IT vs. Treasury

## Information Technology (IT)



### TRANSPORT ACCESS

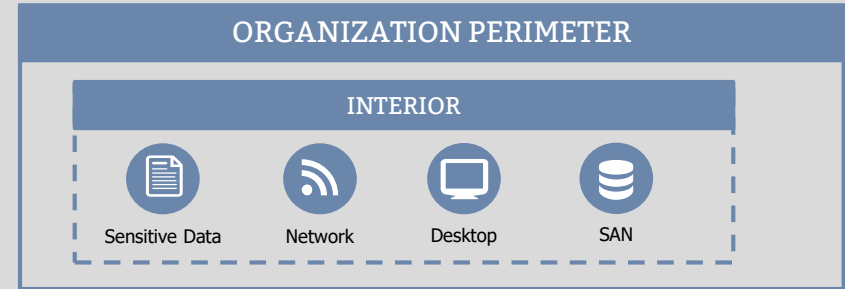


When it comes to security, IT's focus will be primarily on securing the "perimeter" of the organization and as such, may not factor in all exposures, particularly those arising through external sources.

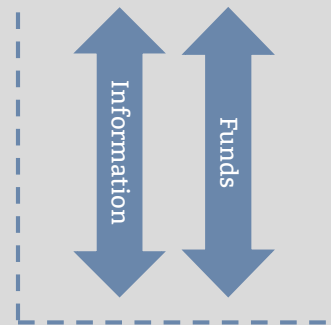
### 3<sup>rd</sup> PARTY



## Treasury

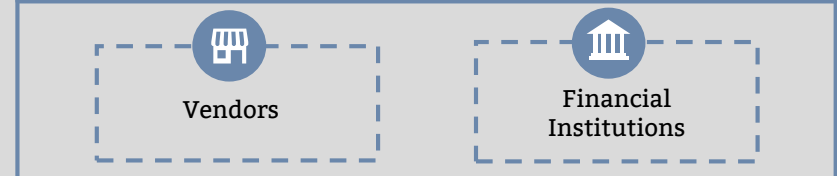


### TRANSPORT ACCESS



Treasury must have a broader view of security that addresses funds/information in transit, as well as information/funds stored or managed externally. This includes 3<sup>rd</sup> party data servers, bank systems and data siloes, etc.

### 3<sup>rd</sup> PARTY



# 12 Key Security Principles

## A Strategic Approach to Fraud Prevention & Security

- In the modern environment, the best way to fight fraud is to develop a comprehensive controls framework that considers each element of security.
- Strategic Treasurer's 12 security principles expand on the vital elements of security that must be considered for any organization to effectively protect against fraudulent activity.
- The following slides will focus on 4-5 of these principles and what their effective utilization looks like within a treasury setting.

## Strategic Treasurer's 12 Security Principles (S.E.C.U.R.E. C.L.A.M.P.S.)

1. Speed Matters
2. Encryption and Control of Keys
3. Challenge / Verify
4. Update Continuously
5. Readiness / Response
6. Exact and Specific Accountability Management
7. **Control / Dual Controls**
8. **Layers**
9. **Awareness / Understanding / Testing**
10. Monitoring
11. **Privilege**
12. Secure Removal / Deletion of Data

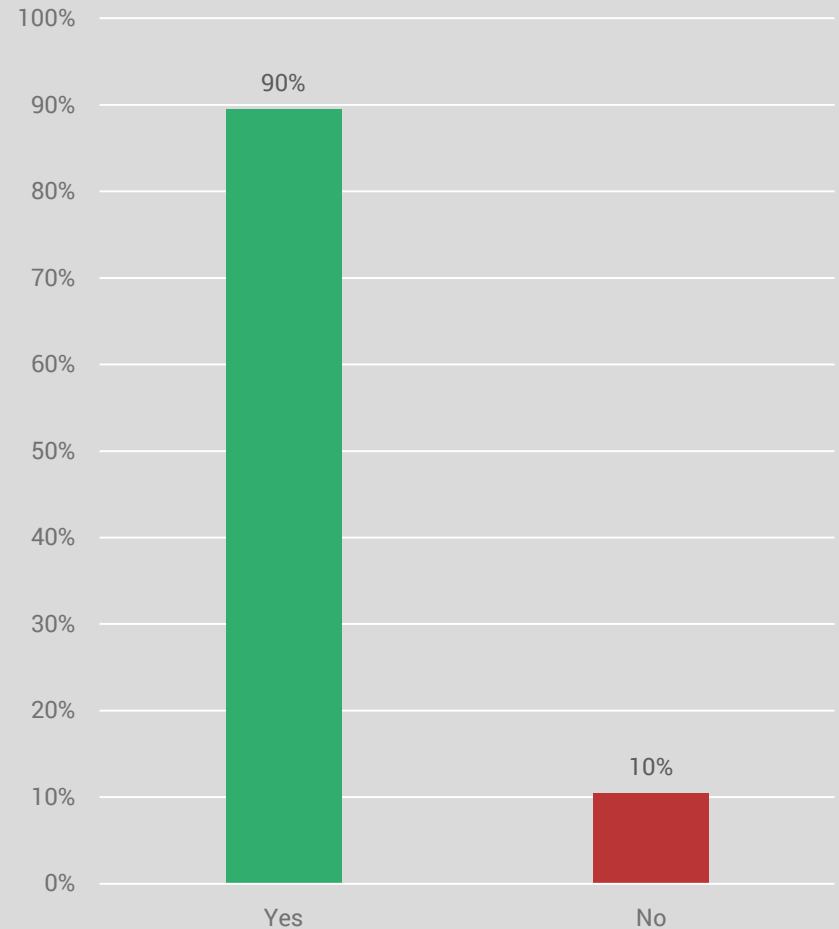
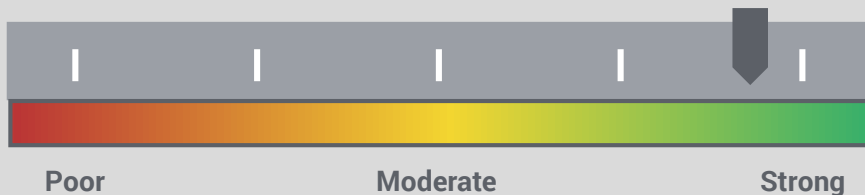
# Dual Controls

## Dual Controls

- Dual controls refers to the practice of requiring more than one employee to approve/generate a payment.
- Makes it harder for criminals to steal funds by requiring multiple employee credentials/approvals.
- Currently, a significant majority of organizations are actively using this security practice (see graph on right)

## Does your organization require dual controls for all transactions?

### Industry Use: Current State



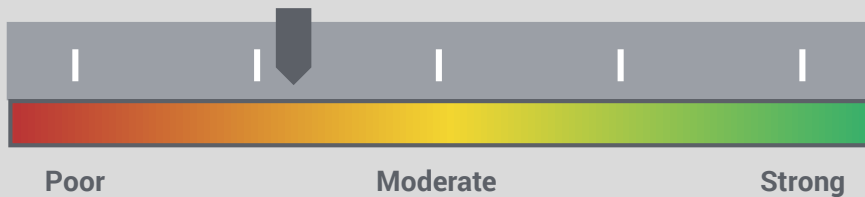
2018 Strategic Treasurer & Bottomline Technologies Treasury Fraud & Controls Survey

# Layers & Multi-Factor Authentication

## Layers

- The term “layers” in the context of security refers to the practice of implementing multiple tiers of controls across a given process or area of operation, such as payments.
- The intent is that if one layer is compromised, the additional layers will still prevent an attack from succeeding.

### Industry Use: Current State



- While multifactor authentication is still a relatively new practice, it has seen promising adoption throughout the treasury environment.

## Sample Layers: Multifactor Authentication



### Fraudulent Transfer

In order for a criminal to steal funds, they must possess:



### Employee Credentials

The individual credentials of an employee with authority over payment generation.



### Physical Key Fob

A physical key-fob or token that is unique to each specific employee.



### Multiple Sets of Information

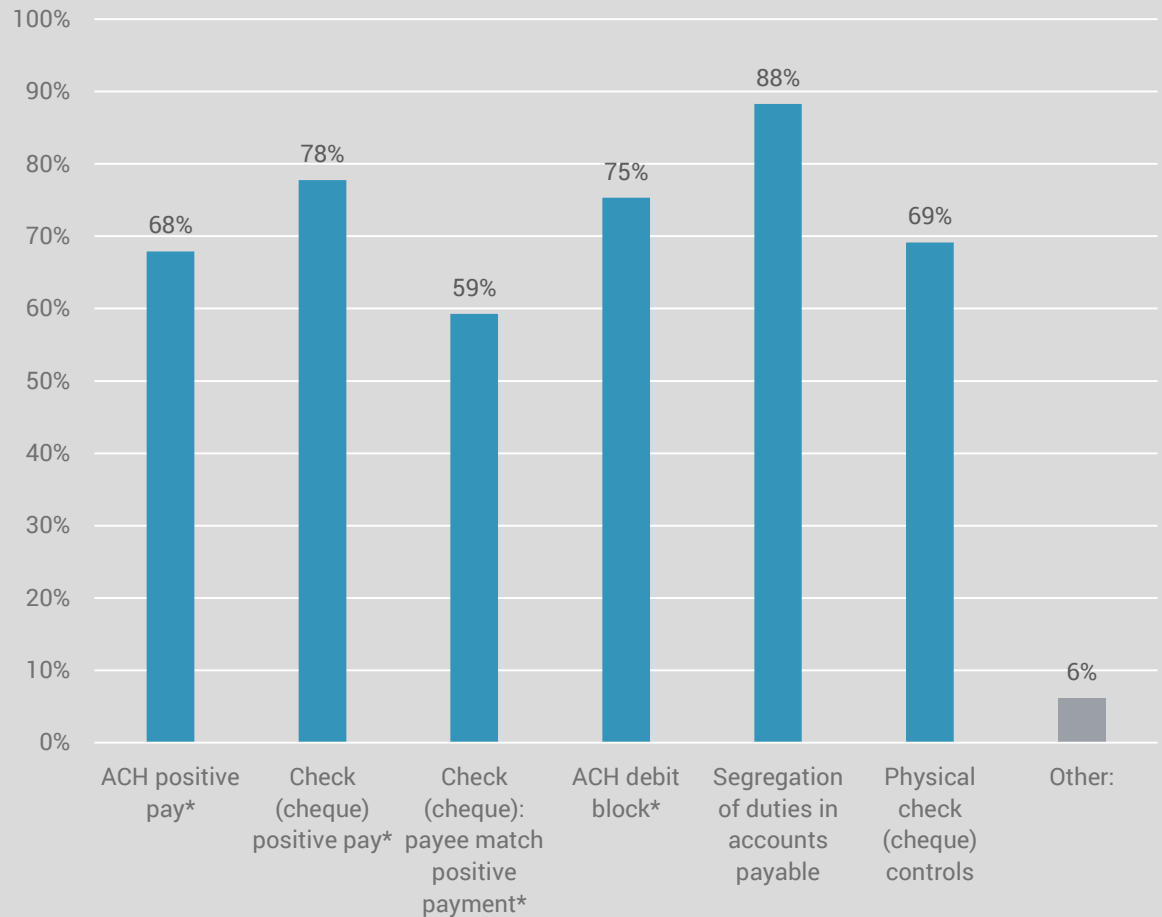
If dual controls are involved, the criminal would have to possess this information for TWO employees in order to control the entire process.

# Layers & Multi-Factor Authentication

## Security Layers

- Besides multifactor authentication, a “layered” approach to security could consist of other elements.
- Combining segregation of duties with positive pay services and other security tools provides a fresh layer of security at each “junction” in the payments process.
- This practice results in multiple points where fraud can be identified and thwarted.

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



2018 Strategic Treasurer & Bottomline Technologies Treasury Fraud & Controls Survey

# Principle of Least Privilege

## Principle of Least Privilege

- The principle of least privilege involves restricting access to any sensitive information to only those employees that **MUST** have it, and **ONLY** for as long as they must have it.
- If such information is not critical to the day-to-day functioning for a specific employee, they should not be granted access.

### Industry Use: Current State



- Most organizations today employ some form of this principle, though in limited measure. Some of these practices are undefined or informal.

## Sensitive Information to Withhold



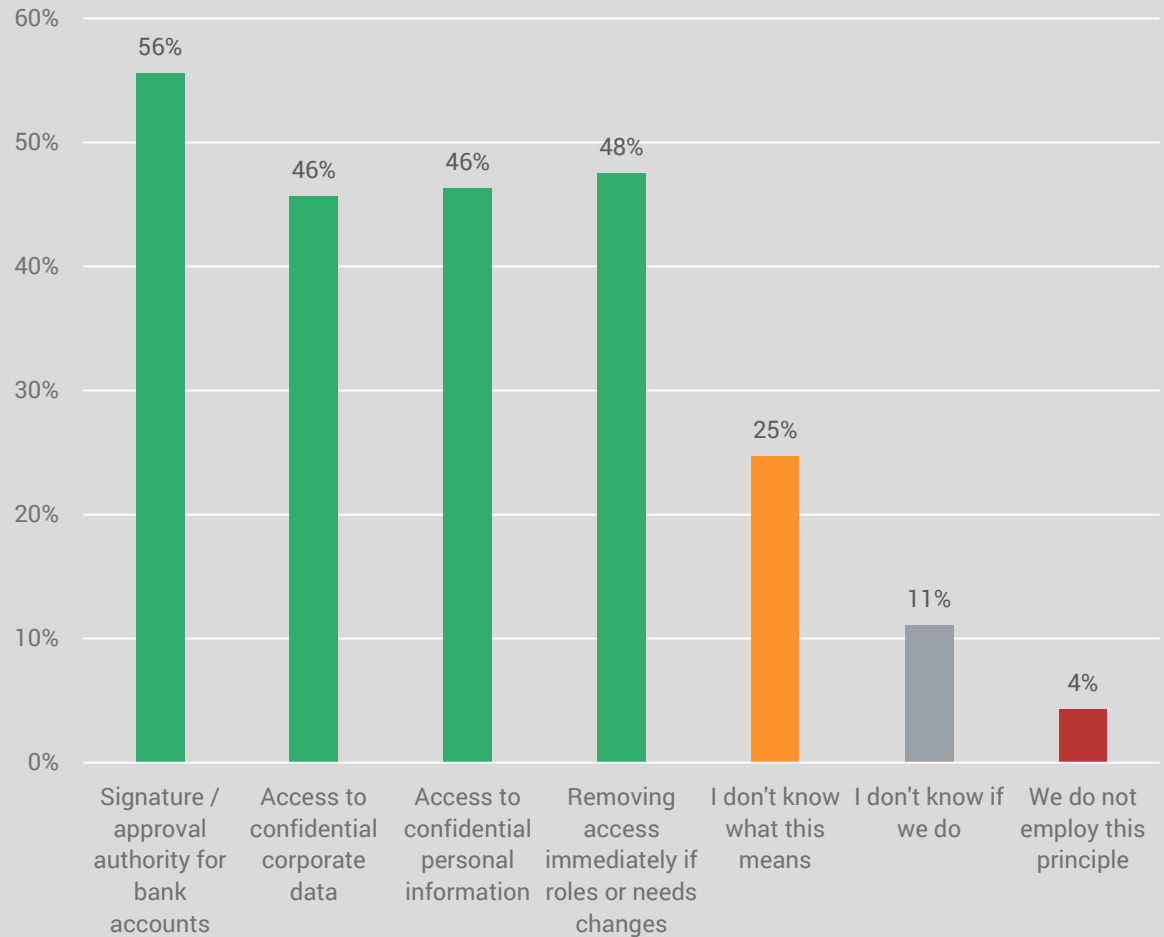


# Principle of Least Privilege

## Principle of Least Privilege

- Approximately half of organizations employ the principle of least privilege in at least one of its various forms.
- 1/4<sup>th</sup> of non-bank respondents were unsure of what the term referred to; however, this does not necessarily mean they weren't employing it.
- 11% were unsure of their company's status on this principle.
- Only 4% could say with certainty that their firm does not employ this principle.

## We intentionally employ the principle of least privilege for: (Select all that apply)



2018 Strategic Treasurer & Bottomline Technologies Treasury Fraud & Controls Survey

# Dedicated & Regular Security Training

## Awareness / Training / Testing

- This principle focuses on ensuring that treasury staff are routinely educated and updated with regards to best practices for security, and also new fraud developments.
- While many organizations emphasize the “technology” components of security, staff training and testing commonly falls to the wayside.

### Industry Use: Current State



- While practically all banks require regular training and testing of their employees on security and fraud, traction in the broader financial environment is limited.



### Awareness

- What types of fraud are corporates experiencing?
- What specific exposures should we be concerned about?



### Training

- What types of attacks should I be wary of?
- How can I keep my company credentials and data safe?
- What should I do in the event of a fraud attack?

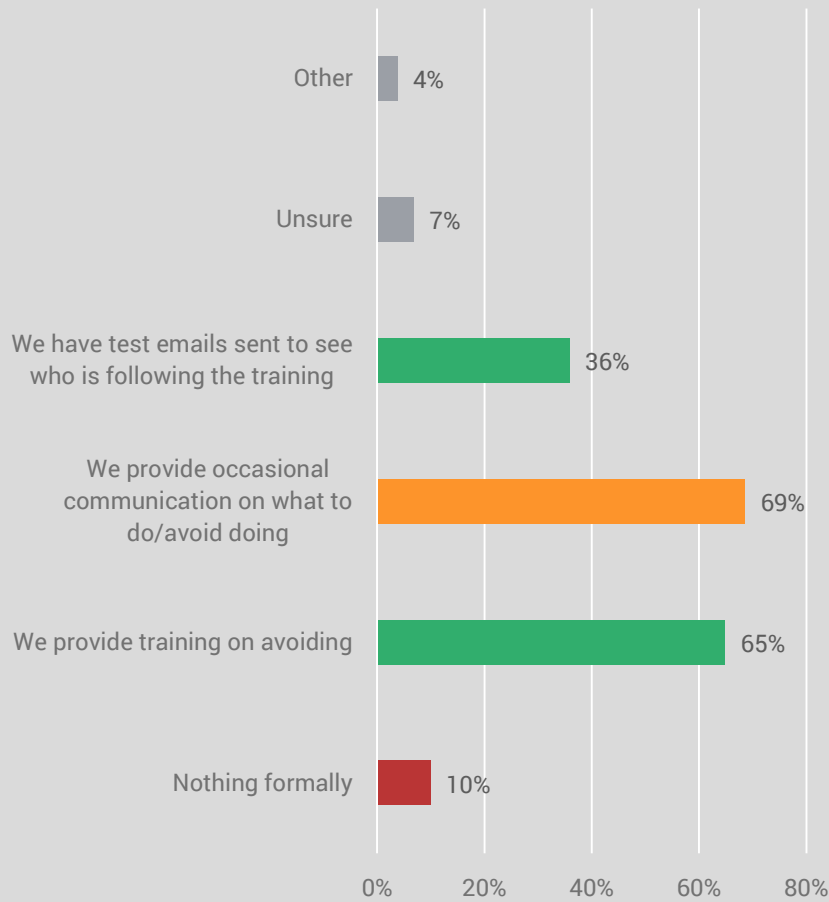


### Testing

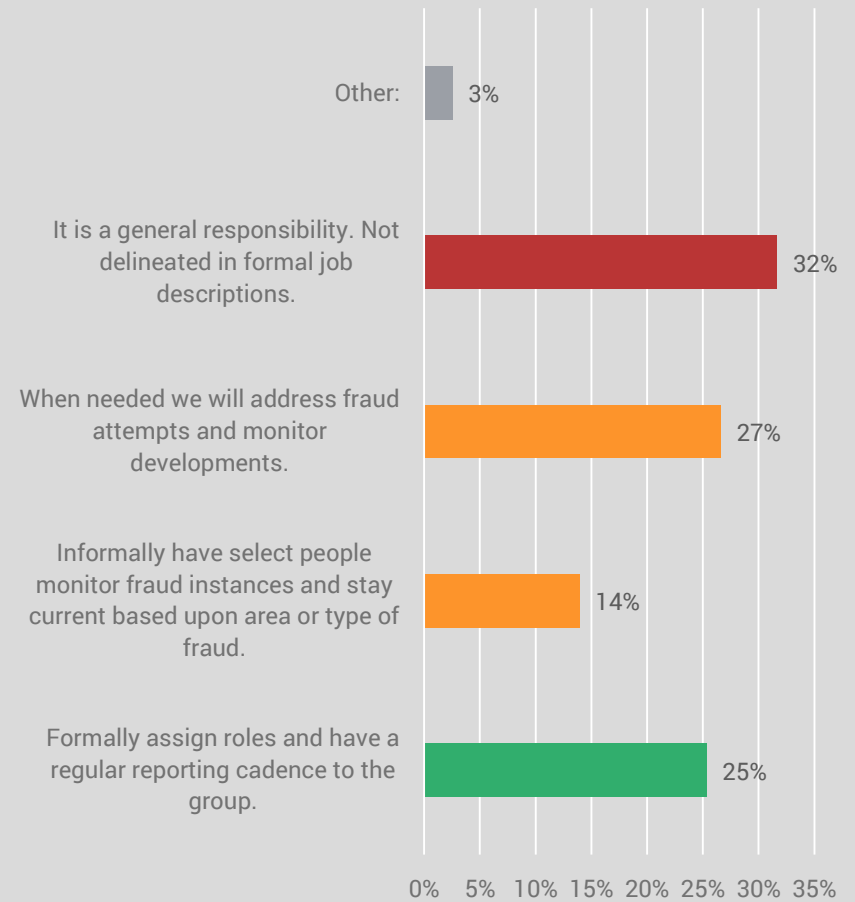
- Deliver “Fake” phishing emails to staff and evaluate their response.
- Provide written tests/quizzes on security policies/procedures to determine employee susceptibility.

# Dedicated & Regular Security Training

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



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



2018 Strategic Treasurer & Bottomline Technologies Treasury Fraud & Controls Survey

# Final Thoughts, Key Takeaways

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



**Fraud Experience Continues to Escalate.** Since 2016, the number of organizations that experience fraud has risen steadily from 40% to 57%. Today, more organizations experience fraud than those that don't.



**Today's Criminal is Sophisticated and Persistent.** It is not just simple check fraud that criminals are using to target firms. Today's fraudulent schemes have become incredibly complex and technologically advanced.



**The Security Response Must be Comprehensive: Technology & Human.** Given the current fraud environment, companies have no choice but to adopt security layers and controls that comprehensively cover all exposures and access points.



**Take Action Proactively...Do Not Wait.** Plugging a gap after a criminal has exposed it is too late. Be proactive in identifying and correcting weaknesses before a criminal identifies them.

## 2019 PDG National Bursars SFS Conference



### When?

- March 31<sup>st</sup> – April 3<sup>rd</sup> 2019



### Where?

- San Antonio, Texas
- Hilton Scottsdale Resort & Villas



Click here to learn more!

**EMPLOYEE TRAINING**  
**TREASURY SECURITY**  
ONLINE VIDEO COURSE

TRAINING · TESTING · DOCUMENTATION  
Persistent · Updated · Subscription-Based

Increased Awareness   Greater Knowledge   Fraud Prevention   Risk Mitigation   SWIFT CSP

Want to learn more? Visit our website [here](#)



### Craig Jeffery, CCM, FLMI

Founder & Managing Partner  
Strategic Treasurer

Email: [craig@strategictreasurer.com](mailto:craig@strategictreasurer.com)

Direct: +1 (678) 466-2222



### Strategic Treasurer

525 Westpark Drive, Suite 130  
Peachtree City, GA 30269

Email: [info@strategictreasurer.com](mailto:info@strategictreasurer.com)

Phone: +1 (678) 466-2220

