



Combating Fraud

6 Key Security Principles – Part 2

Craig Jeffery, *Managing Partner, Strategic Treasurer*

Debbi Denison, *Senior Consultant, Strategic Treasurer*

About the Presenters

Connect on 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.



Debbi Denison

Senior Consultant
Strategic Treasurer

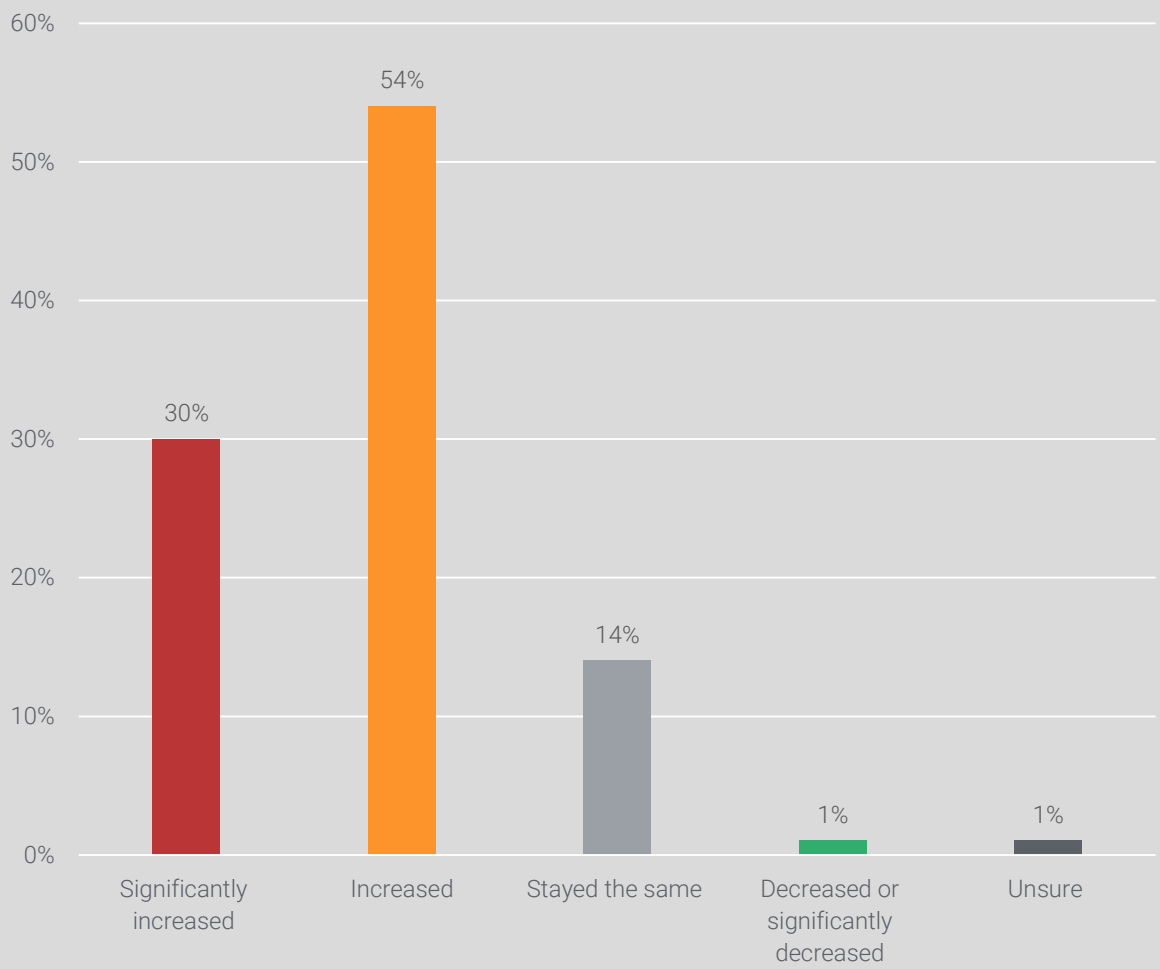
Debbi Denison is a senior consultant at Strategic Treasurer responsible for leading client projects and relationships across working capital, cash management, liquidity management, treasury technology, and risk domains. Mrs. Denison has held senior treasury positions with global, multi-national and Fortune 500 corporations in the fields of utility, airline, consumer products and pharmaceuticals. Her leadership experience comprises leveraging technology to proactively identify and implement leading practices with respect to global liquidity, pooling structures, credit card programs and accounts receivable factoring.

State of Treasury Fraud in 2018

Escalated Threat

- Comparing 2018 to 2017, the vast majority (84%) of corporate 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 corporate treasury environment.

Corporates: 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

State of Treasury Fraud in 2018

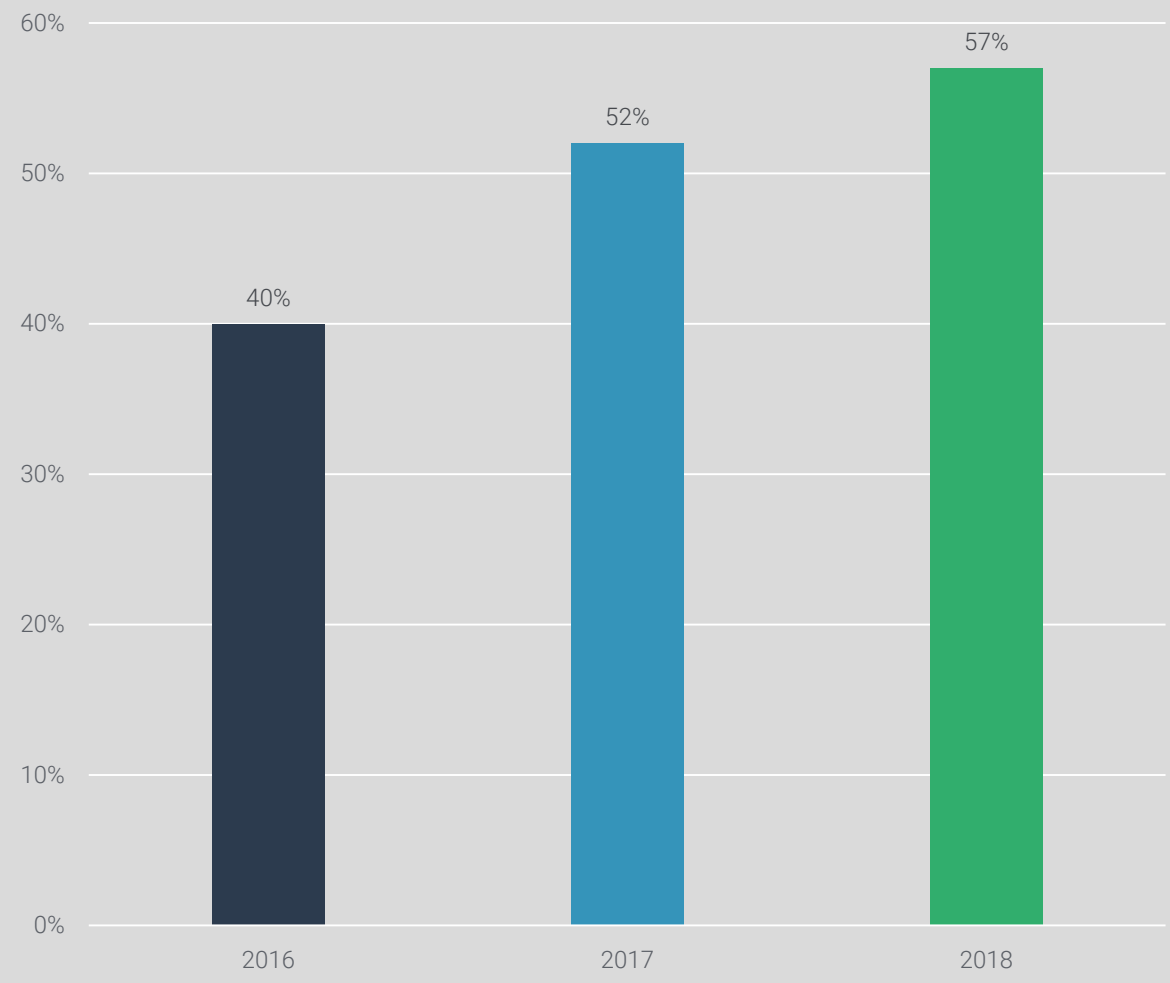
Connect on [StrategicTreasurer.com](https://www.StrategicTreasurer.com)   

Fraud Experiences Rise

- Looking at corporate fraud experiences, it appears that practitioners are correct in their perception that fraudulent threats have increased.
- These figures represent a 17% overall increase (40%+ year-over-year) in corporate 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



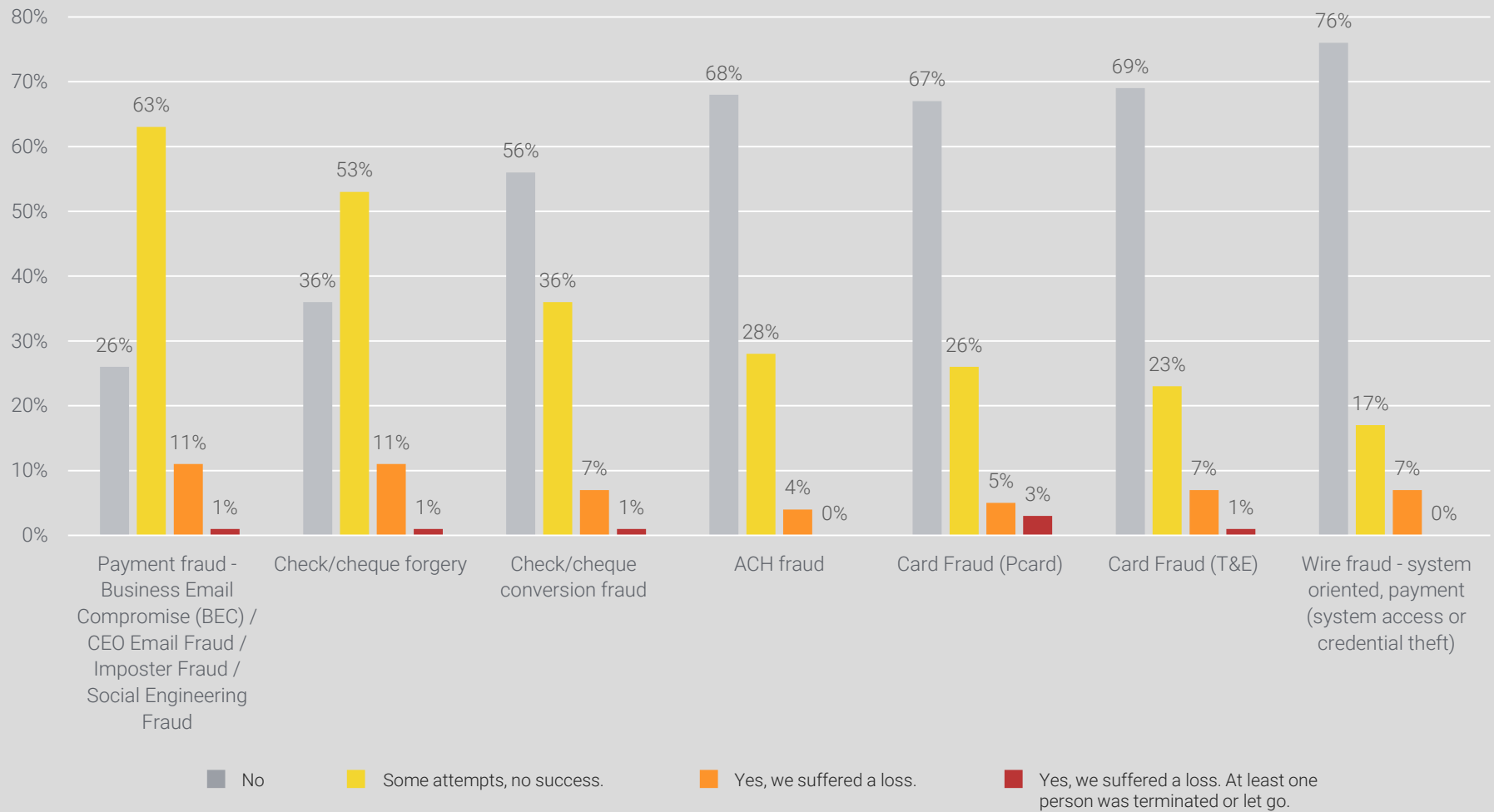
2018 Strategic Treasurer & Bottomline Technologies Treasury Fraud & Controls Survey

State of Treasury Fraud in 2018

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

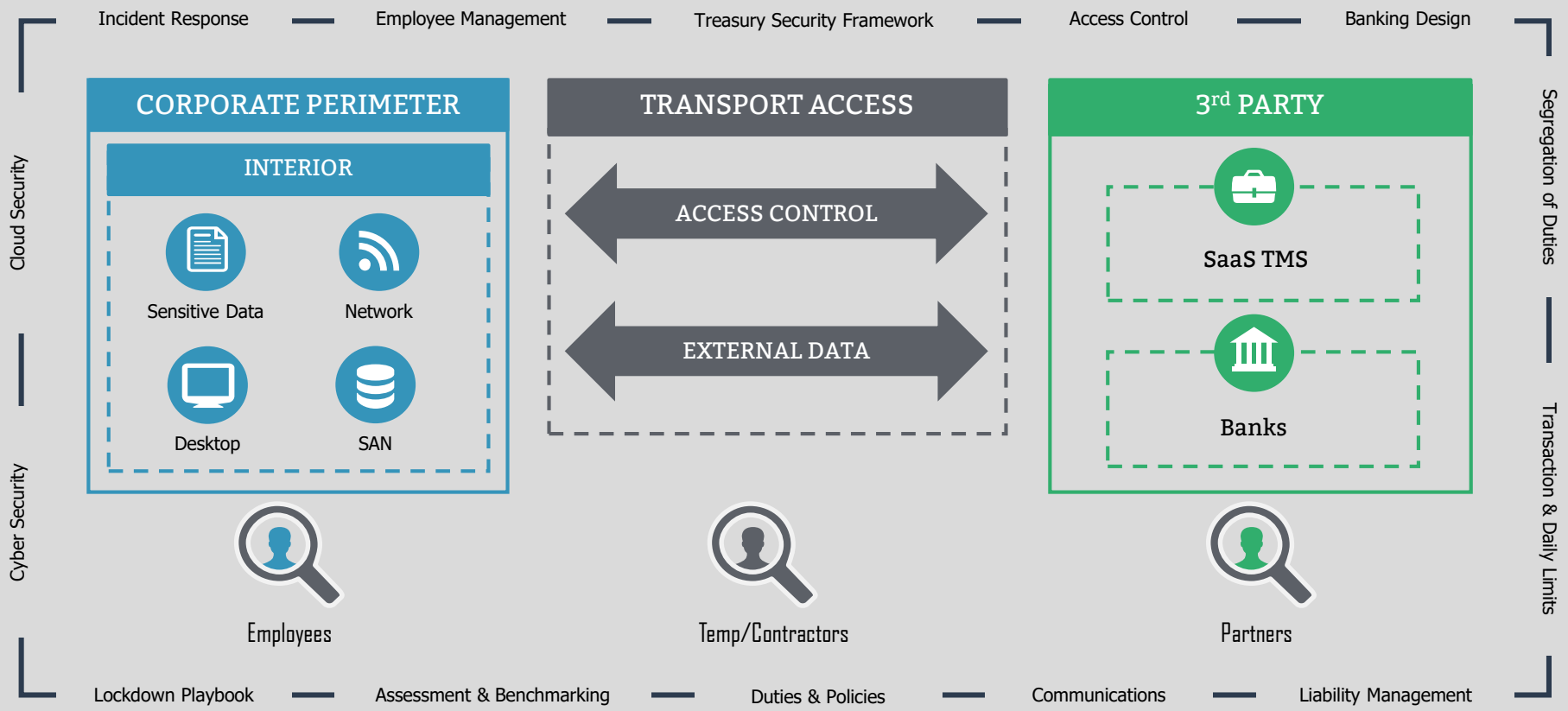
Corporates: Have you experienced any of the following in the past two years?

Data excludes "unsure" responses

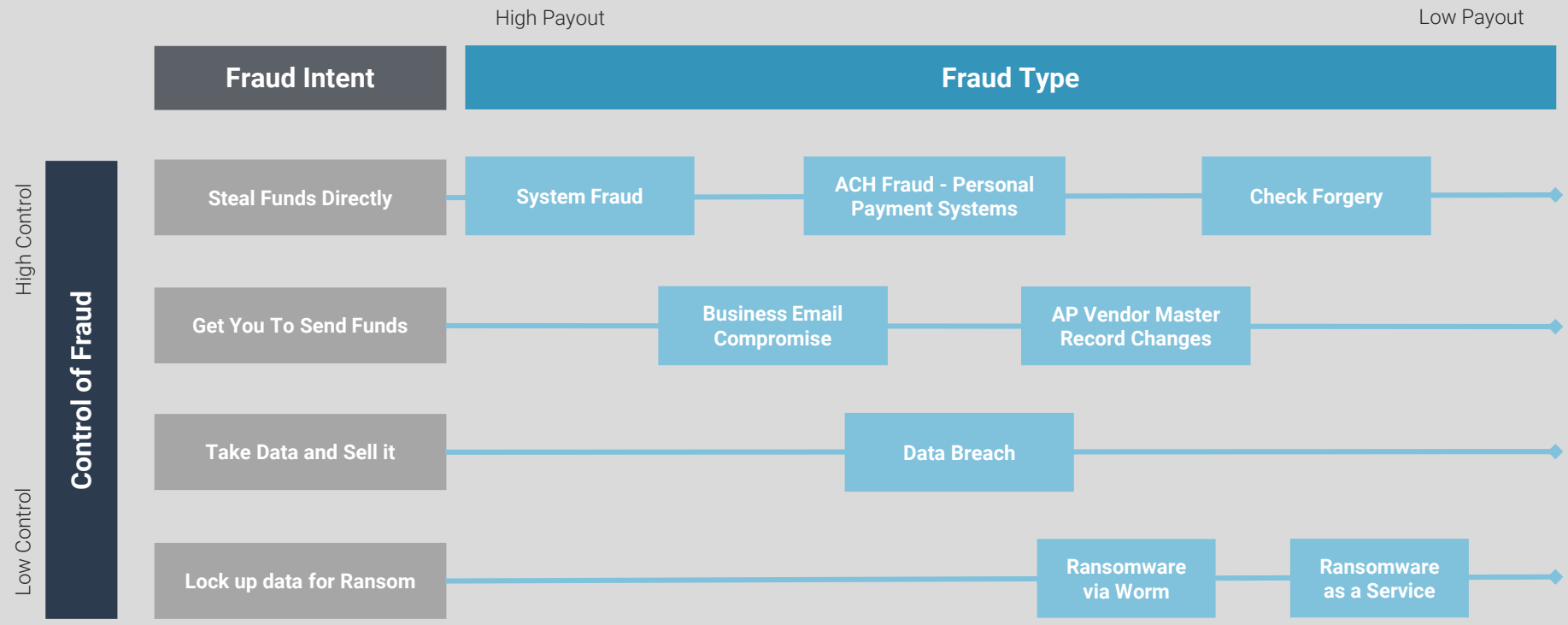


2018 Strategic Treasurer & Bottomline Technologies Treasury Fraud & Controls Survey

The Fraud Battlefield: Access Control



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.








Items to Consider

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

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**

12 Security Principles

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

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 first six principles were covered at length in a previous webinar; this presentation will focus on principles 7-12.

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

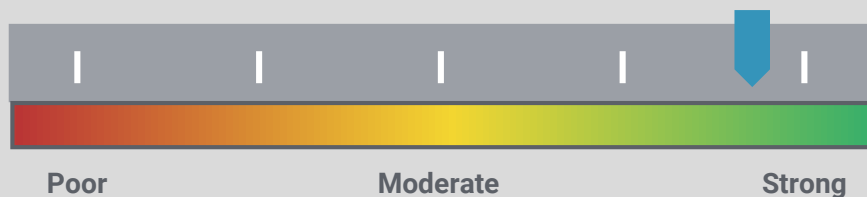
Principle 7: Dual Controls

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

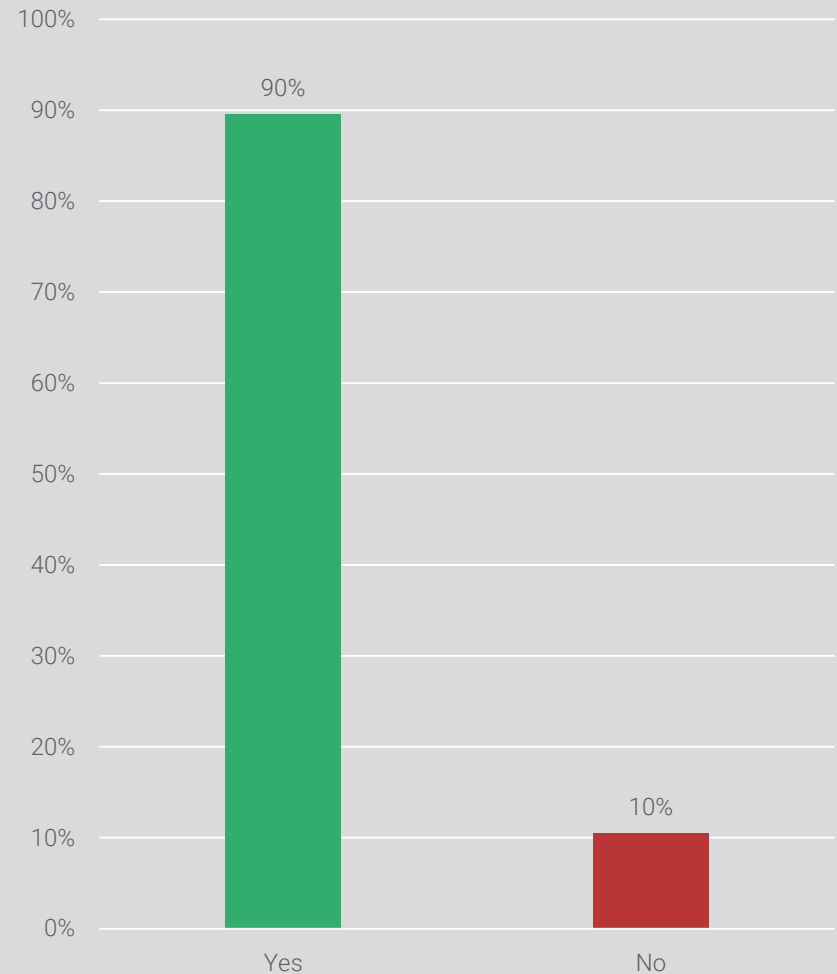
Dual Controls

- 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 corporates are actively using this security practice (see graph on right)

Industry Use: Current State



Corporates: Does your organization require dual controls for all transactions?



2018 Strategic Treasurer & Bottomline Technologies Treasury Fraud & Controls Survey

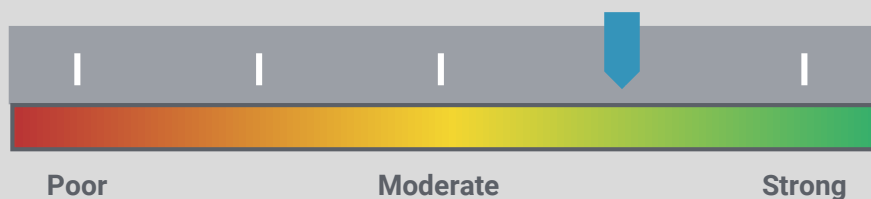
Principle 8: Layers

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

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 corporate 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.

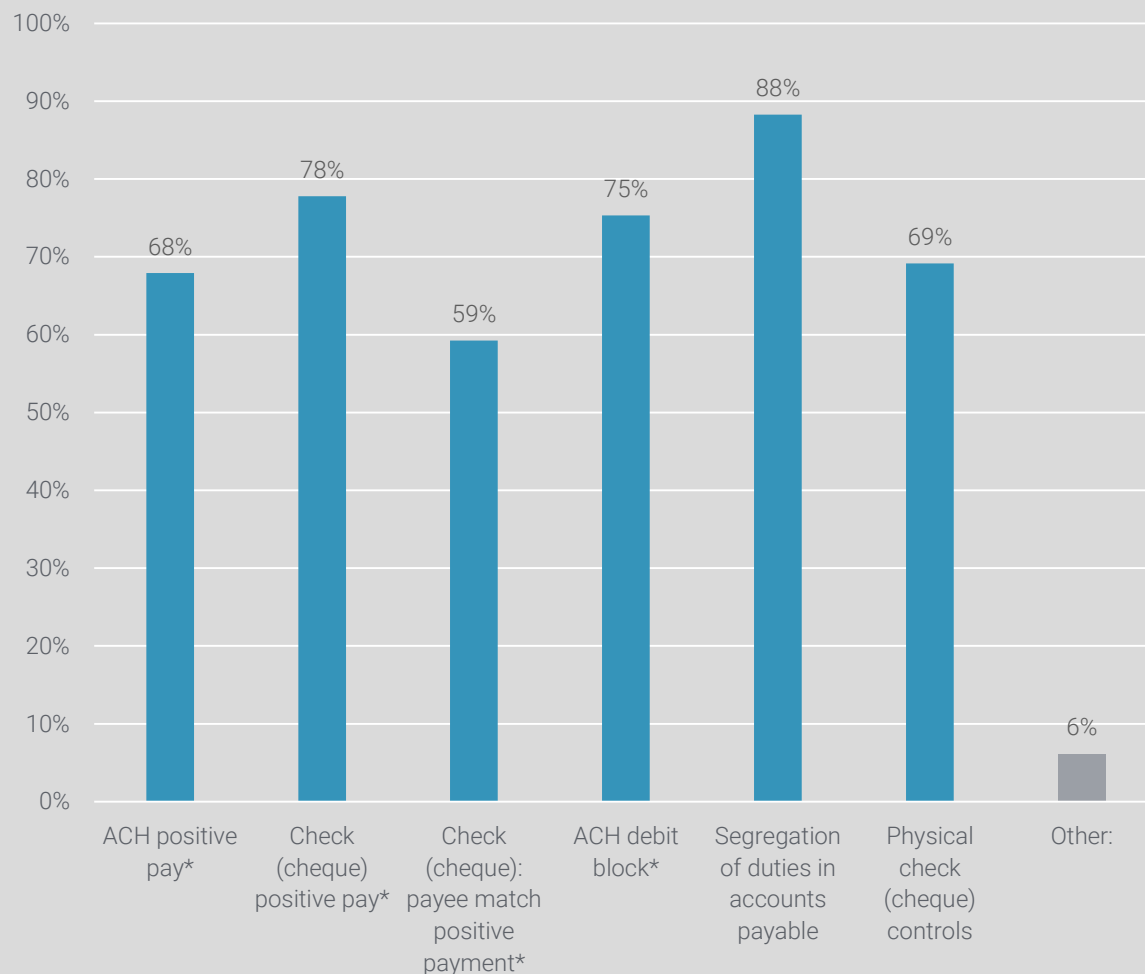
Principle 8: Layers

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

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 “juncture” in the payments process.
- This practice results in multiple points where fraud can be identified and thwarted.

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



2018 Strategic Treasurer & Bottomline Technologies Treasury Fraud & Controls Survey

Principle 9: Awareness / Understanding / Testing

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

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, less than half of corporates do the same.



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?



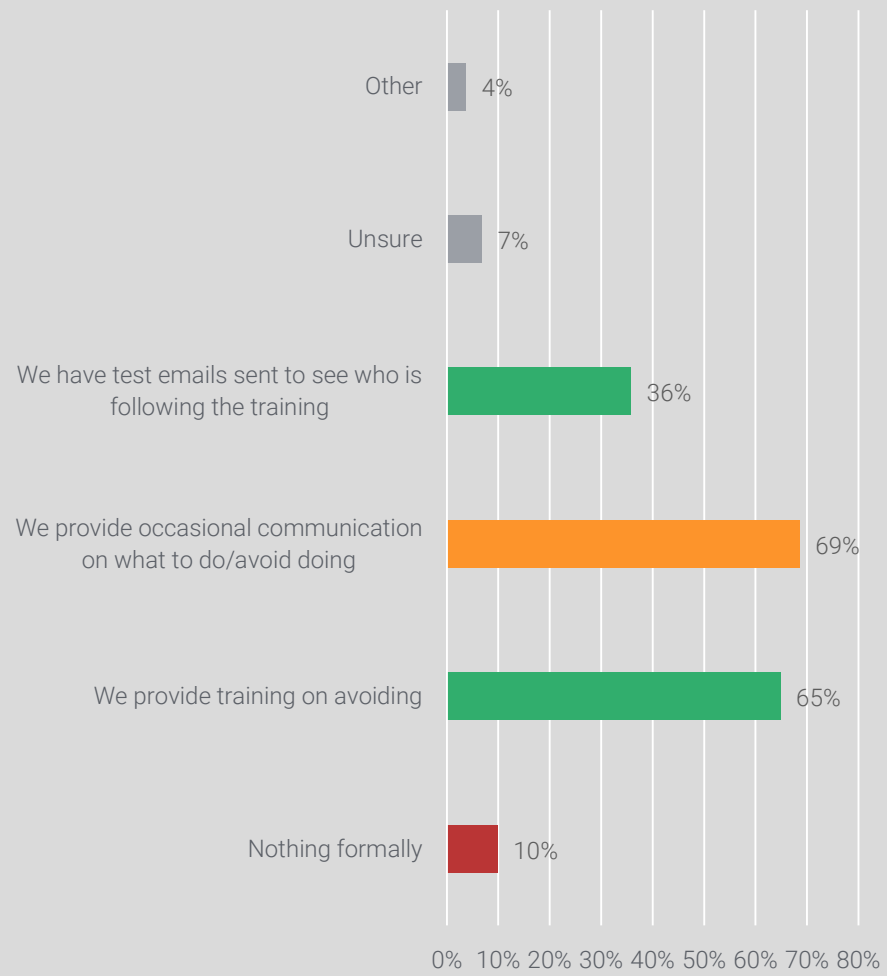
Testing

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

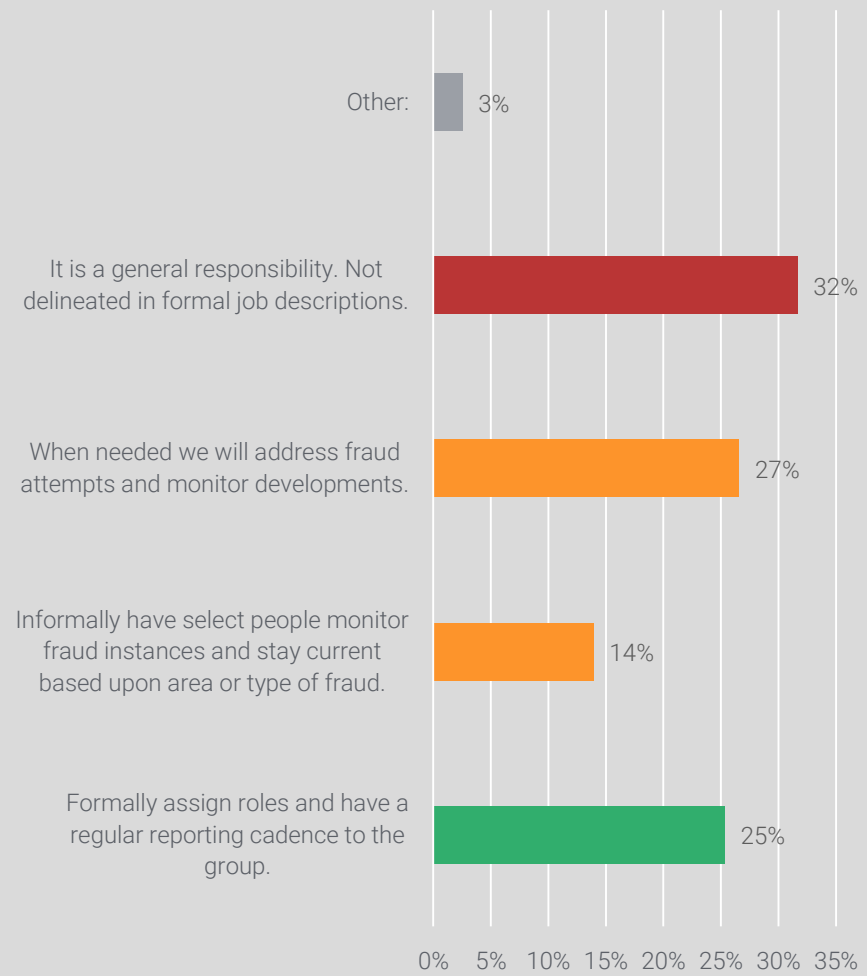
Principle 9: Awareness / Understanding / Testing

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

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



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



2018 Strategic Treasurer & Bottomline Technologies Treasury Fraud & Controls Survey

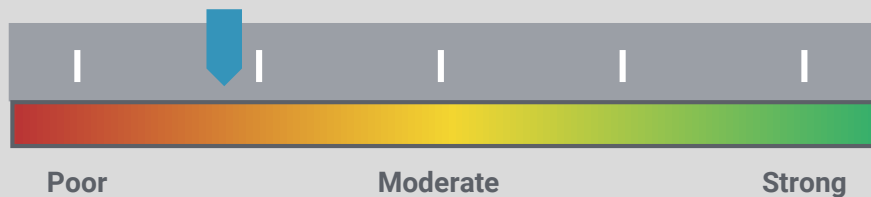
Principle 10: Monitoring

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

User / Employee Monitoring

- Many technology solutions available today have built-in functionality that allows an administrator to monitor employee / user activity that occurs through the system.
- This can help detect erroneous behavior and also trace criminal activity back to specific individuals or accounts.

Industry Use: Current State



- While the banking sector has done well to adopt user monitoring software, implementation of such solutions on the corporate side has not followed suit.



Banks

- Bank policies around security and fraud tend to be more stringent than their corporate counterparts.
- Banks are also more advanced with their security techniques and fraud prevention strategies.
- Currently, over 3/4ths of banks have the ability to monitor user behavior on their system, either in real-time or after the fact.



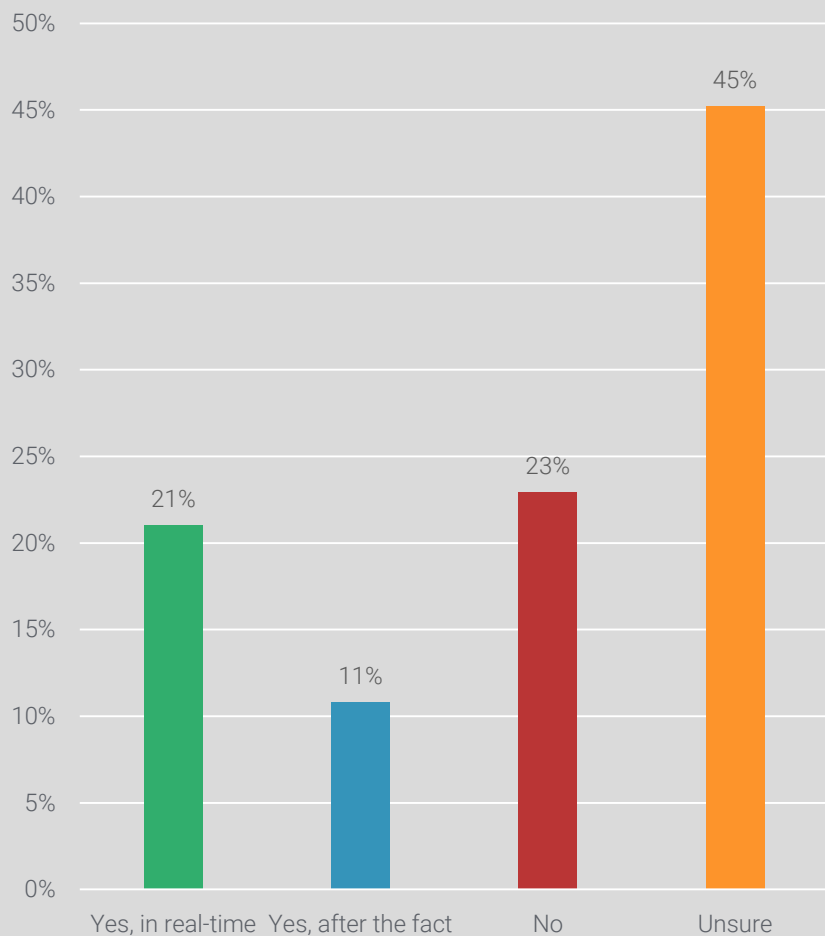
Corporates

- While corporates have been investing heavily in security controls, they have not kept pace with banks.
- Currently, less than 1/3rd of corporates can monitor user behavior in their system.

Principle 10: Monitoring

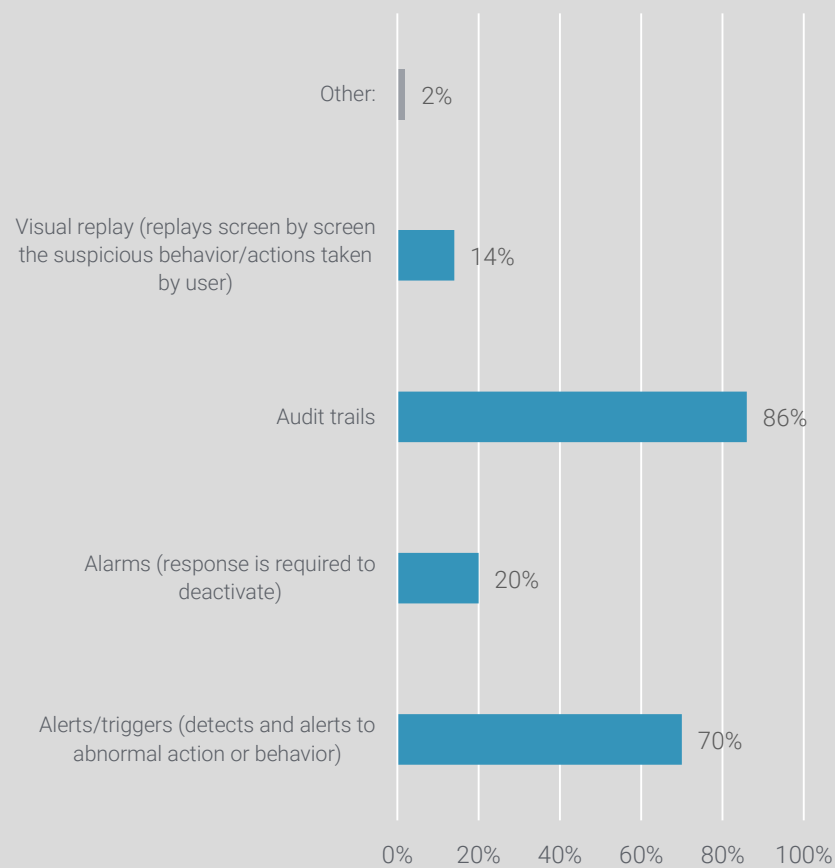
Connect on [StrategicTreasurer.com](https://www.StrategicTreasurer.com)   

Corporates: Do you have technology implemented to proactively monitor anomalous or suspicious behavior within your system(s)?



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

Of those that selected "yes" to previous question



2018 Strategic Treasurer & Bottomline Technologies Treasury Fraud & Controls Survey

Principle 11: Privilege

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

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, even if such practices are undefined or informal.

Sensitive Information to Withhold



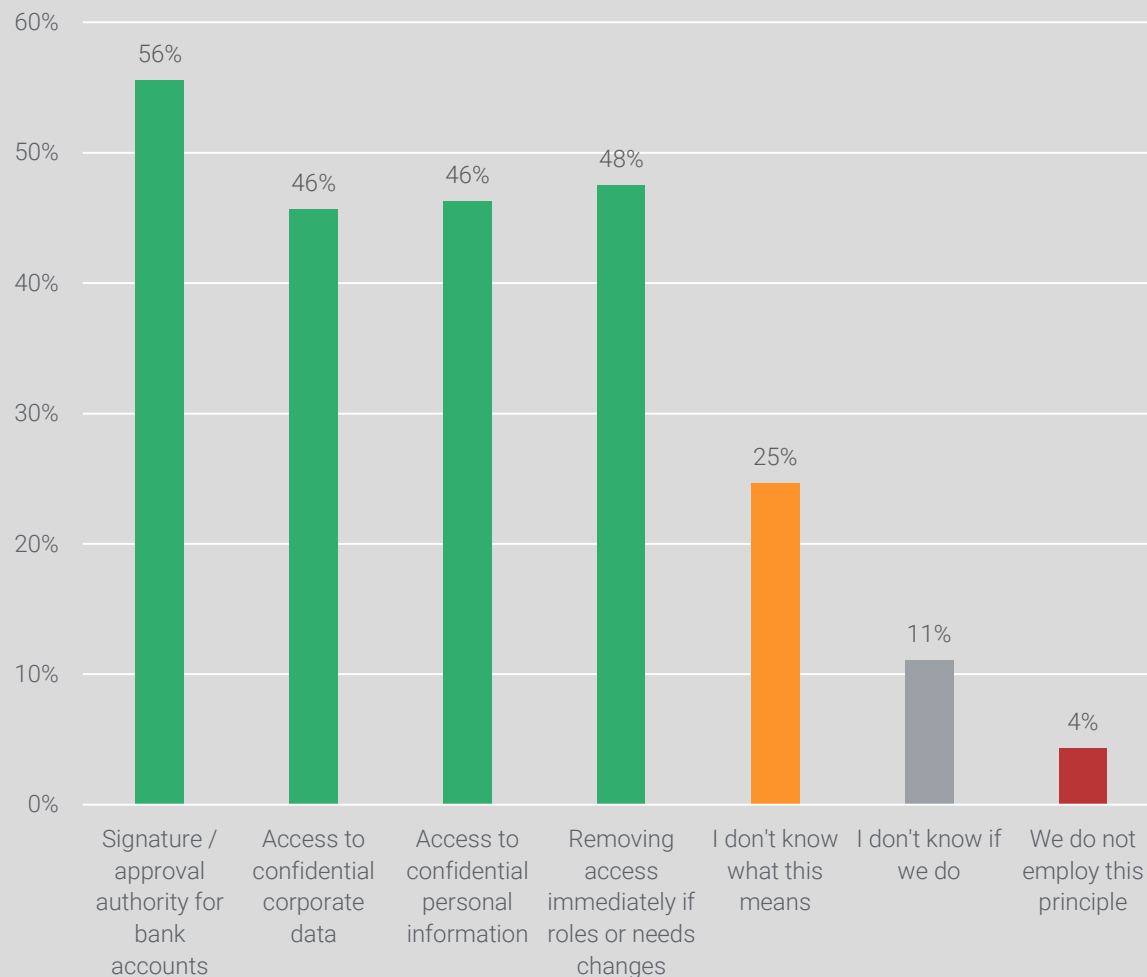
Principle 11: Privilege

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

Principle of Least Privilege

- Approximately half of organizations employ the principle of least privilege in at least one of its various forms.
- 1/4th of corporate respondents were unsure of what the term referred to; however, this does not necessarily mean they were not 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

Principle 12: Secure Removal & Deletion of Data

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

Removing / Deleting Data

- While sensitive data must always be kept secure, there comes a time when such information must be cleared.
- Improper management of this step could be devastating if files are not completely destroyed or if they are misplaced.
- Remember to clearly document when records are deleted to establish audit trails, and assign a witness to view and “sign off” on the deletion/removal process.

Industry Use: Current State



- Data removal processes across the corporate landscape vary; some have clearly defined practices in this arena, while others perform it on an “ad-hoc” basis

Areas to Consider: Sensitive Information



Vendor Master Records



Bank Account Records



Check Stock



Financial Statements



Account Signatories

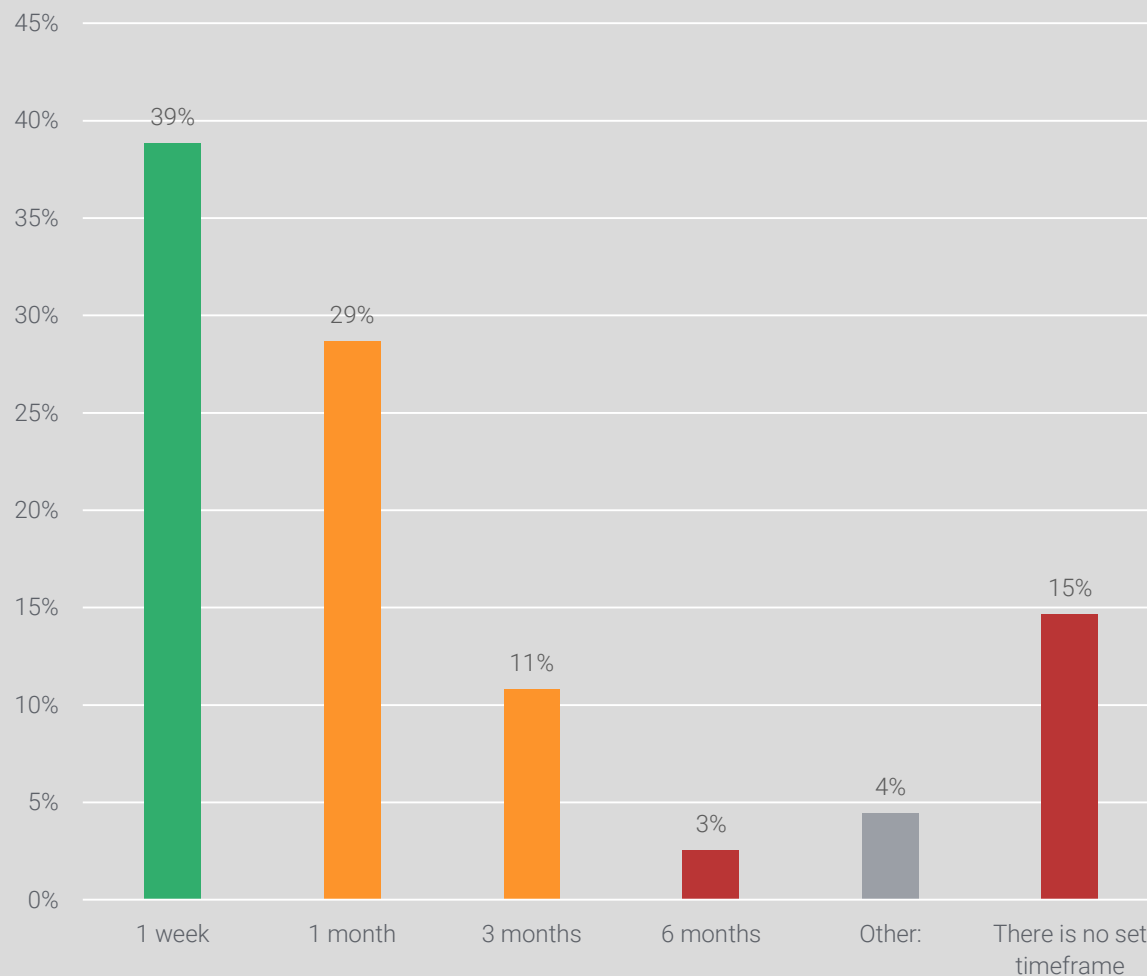
Principle 12: Secure Removal & Deletion of Data

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

Removal & Deletion of Data

- An area of data removal that is particularly important for treasury lies around account signers.
- Account signers are typically treasury staff with privileged access to payment systems and bank account data.
- When employee turnover for one of these positions occurs, it is vital that the company quickly update their records to reflect the changes.
- The longer it takes to reflect such changes, the more exposed a company is through falsified signatures.

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



2018 Strategic Treasurer & Bottomline Technologies Treasury Fraud & Controls Survey

Key Takeaways for Treasury:



Fraud Experience Continues to Escalate. Since 2016, corporate fraud experience has risen steadily from 40% to 57% of organizations.



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. 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 still too late. Be proactive in identifying and correcting weaknesses before a criminal identifies them.



Craig Jeffery, CCM, FLMI

Founder & Managing Partner

Email: craig@strategictreasurer.com

Direct: +1 (678) 466-2214



Debbi Denison

Senior Consultant

Email: debbi.denison@strategictreasurer.com

Direct: +1 (678) 466-2237

**Sign-Up for Strategic
Treasurer's Exclusive
Webinar List**

Review this Webinar

Thank you for participating in this event!