STRATEGIC TREASURER
Consultants in Treasury

Fraud is Rampant

SIX KEY PRINCIPLES FOR SECURITY

Craig Jeffery, *Strategic Treasurer*

Tuesday, January 16th, 2018

2:00 PM EST

Today's Presenter

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 1980's. Partners and associates of Strategic Treasurer span the US, the UK, and continental Europe.

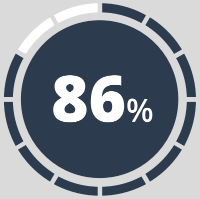
This team of experienced treasury specialists are widely recognized and respected leaders in treasury and risk management technology consulting. Known for their expertise in treasury technology, risk management, and working capital as well as other cash management and banking issues, they efficiently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

Topics of Discussion

- Treasury Fraud: Setting the Stage
- Trends in Fraud
- Security Principles (S.E.C.U.R.E.)
  - *Speed Matters*
  - *Encryption and Control of Keys*
  - *Challenge / Verify*
  - *Update Continuously*
  - *Readiness / Response*
  - *Exact and Specific Accountability Management*
- Final Thoughts
- 2018 Treasury Fraud and Controls Survey
- Questions and Answers

Treasury Fraud: Setting the Stage

2017 Treasury Fraud Overview



In 2017, **86%** of respondents were found to have experienced either payment fraud, cyber fraud, BEC/imposter fraud, or ransomware attacks within the past two years.

Many of these attempts resulted in financial losses for the organization targeted. These losses ranged anywhere from a few thousand to multiple millions of dollars.

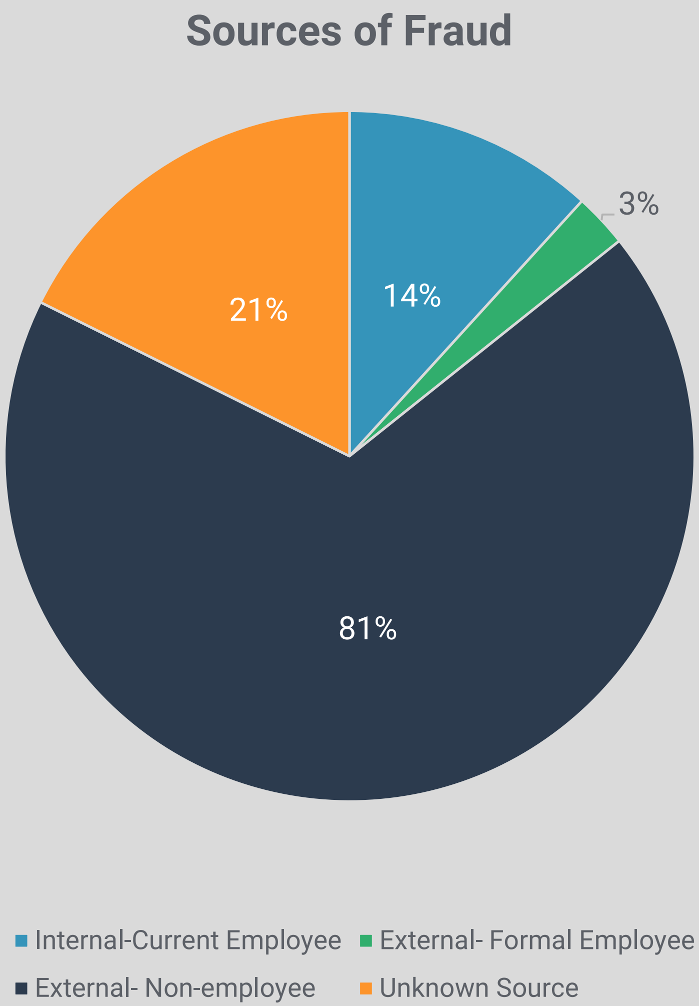
Upon further examination, it was discovered that only **13%** of organizations had a formal, current, and well-understood treasury fraud and controls framework.

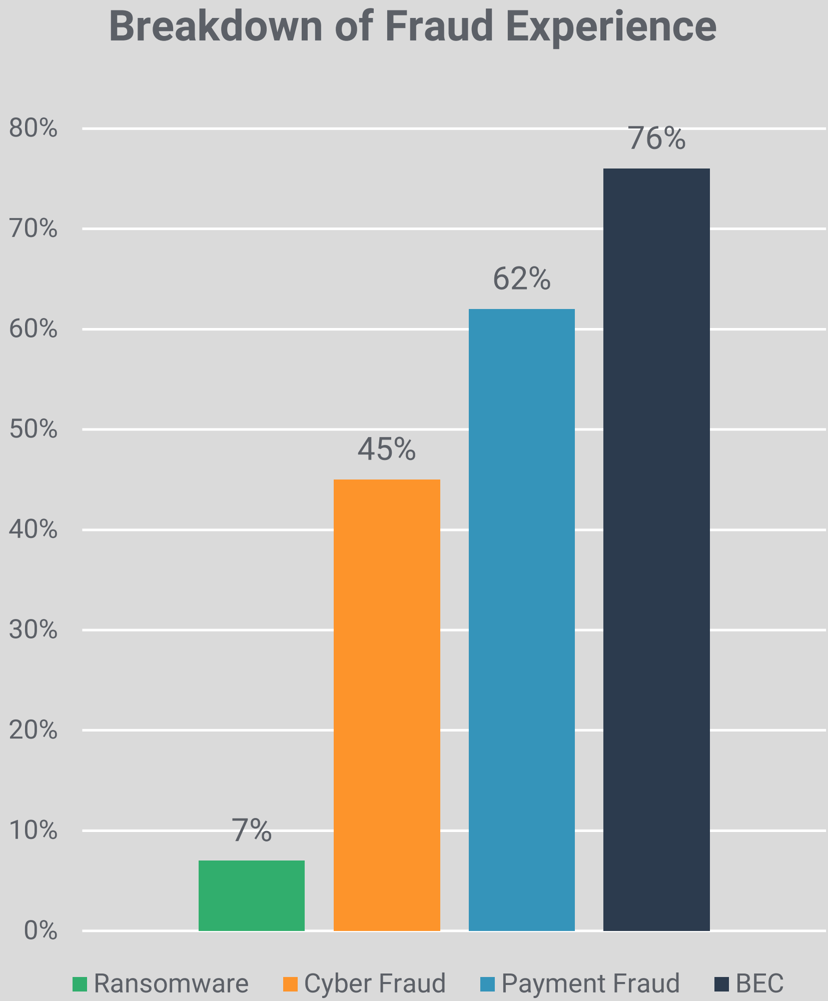
Strategic Treasurer's 12 Security Principles

(S.E.C.U.R.E. C.L.A.M.P.S.)

- ✓ **Speed Matters**
- ✓ **Encryption and Control of Keys**
- ✓ **Challenge / Verify**
- ✓ **Update Continuously**
- ✓ **Readiness / Response**
- ✓ **Exact and Specific Accountability Management**
- ✓ *Control / Dual Controls*
- ✓ *Layers*
- ✓ *Awareness / Understanding / Testing*
- ✓ *Monitoring*
- ✓ *Privilege*
- ✓ *Secure Removal / Deletion of Data*

Treasury Fraud: Sources of Attacks Vary





#1 – Speed Matters

The Criminal Playbook

- ✓ Criminal's intent: Steal money, hide evidence, delay discovery
- ✓ When a hack or cyberattack occurs, the speed with which your company responds can mean all of the difference.
- ✓ Plans are only as good as their implementation.
- ✓ The level of loss is highly impacted by how long it takes to perform tasks and respond to an attack.

Preventative Techniques

- ✓ Know what to look out for. Train your employees on how to spot suspicious activity.
- ✓ Know your direct report. What is the hierarchy of people that need to know if a transaction does not look right?
- ✓ Monitor regularly so as to seek early detection of a loss.
- ✓ Reconcile accounts regularly, either monthly or daily, either manually or through automation
- ✓ Freeze assets before they leave the banking system

#1 – Unfortunate vs Successful Approach

The Central Bank of Bangladesh

Situation | *February 2016*

- Failed to defend and update access
- Suffered a sophisticated system hack
- Criminals monitored network and processes, then sent messages that attempted to move $951mm dollars. $101mm was successfully removed. Only $20mm was recovered.
- Maximized the amount of time they had to remove the money

Result

✓ $81mm net loss

Take Away

➥ *If the hack had been recognized sooner, less money would have been lost.*

International Bank in Taiwan

Situation | *October 2017*

- $60mm sent out from their account.
- Hackers planted malware on the bank servers and through the SWIFT interbank banking system.
- Staff at the bank quickly recognized the strange transactions and were able to recover a majority of the money.

Result

✓ $1mm net loss

Take Away

➥ *Employee awareness and speed of response enabled the bank to recover a majority of the money, even after it had left the bank.*

#2 – Encryption and Control of Keys

Principle Overview

Definition

- Encrypting confidential data translates it into an indecipherable code (from plaintext to ciphertext), rendering it inaccessible to unauthorized users.

Benefits

- Unless you have access to the key, the data is secure and unreadable by outsiders.

Leading Practices

- Encrypt data and enable a remote wipe command. If a device is lost or stolen, you are in a far more protect position.
- Encrypt hard drives so that all information is secure in any situation.

Ultimate Objective

- Make data unreadable to intruders by safeguarding information.

Two Types of Encryption

Symmetric Algorithm

- Encryption and decryption keys are identical
- Key is private
- Anyone who has the key can unlock the data
- Encryption and decryption can happen quickly
- Potentially less secure

Asymmetric Algorithm

- Encryption and decryption keys are separate but linked mathematically
- One key is public, the other private
- Only you have the key to unlock the data
- Encryption and decryption are slower and require more processing power
- Potentially more secure

#2 – Encryption and Control of Keys, Cont'd

Control Access to Passwords and Keys

- Don't put passwords on the bottom of keyboards
- Change passwords and key codes/cards systematically
- Enforce compliance:
  - ✓ Check regularly to ensure that no one is out of compliance
  - ✓ Require validation of compliance via email, a monthly survey, etc.
  - ✓ Enable multi-factor authentication. This will add an extra layer of security.
  - ✓ Enforce the length and strength of passwords

Key Aspects of a Strong Password

- Consider using a phrase
- Scatter numbers and symbols throughout, not just at the beginning or end
- Do not use birthdates or characteristics easily guessed
- Never keep username, password, and account name stored together
- Store securely (in a safe or in varied places)

#3 – Challenge / Verify

Principle Overview

Definition

- From physical location access to system access, challenge and verify all points of entry.

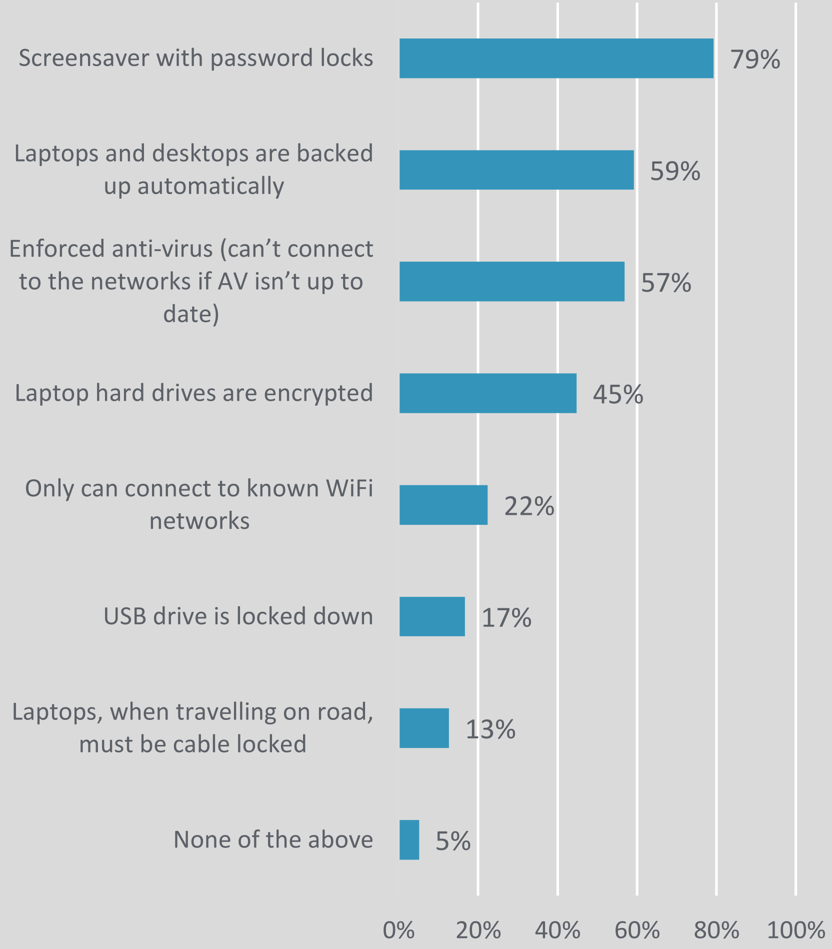
Benefits

- By barring entry, you safeguard information.
- Important while in the office and while traveling with devices that contain secure information.

Ultimate Objective

- Stop intruders at the door, denying them the opportunity to access any information or data.

For computer access security, we use or require the following: (select all that apply)



#3 – Challenge/Verify

Out of Band Authentication

- Always follow up on requests for money transfers before processing.
- Make a call or send a confirmation letter to the source.
- Use different channels to verify, as the channel upon which the request was received may be compromised.
- It is better to be overcautious and preventative than lose money.

Physical Network

- Require an ID and password for access
- Consider the use of a third level of authentication
- Secure ports of access to devices with a regularly monitored firewall

Office / Plant

- Restrict physical access in order to safeguard the information contained within your office or plant.
- Lock doors or require sign-in to visit certain areas of the office. Use locked file cabinets or safes for confidential information.
- Use video security and keycard access to track who goes where as well as track access to certain records.
- Challenge those you don’t recognize in a kind way. Do not let unknown people into the office because you are too embarrassed to ask.
- Decide on areas that need extra security. Are there records or areas that would compromise the operation if accessed?
- Consider all people who have access to office. It isn’t just staff and visitors that come through. Consider maintenance, delivery workers, and others who might have access to your office or plant.

#4 – Update Continuously

Principle Overview

Definition

- Outdated systems and people put your company and data at risk.

Ultimate Objective

- Stop intruders at the door, denying them the opportunity to access any information or data.

Areas to Update:

Networks and Software

- *Server*
- *Computer*
- *Antivirus*
- *Software*
- *Access*

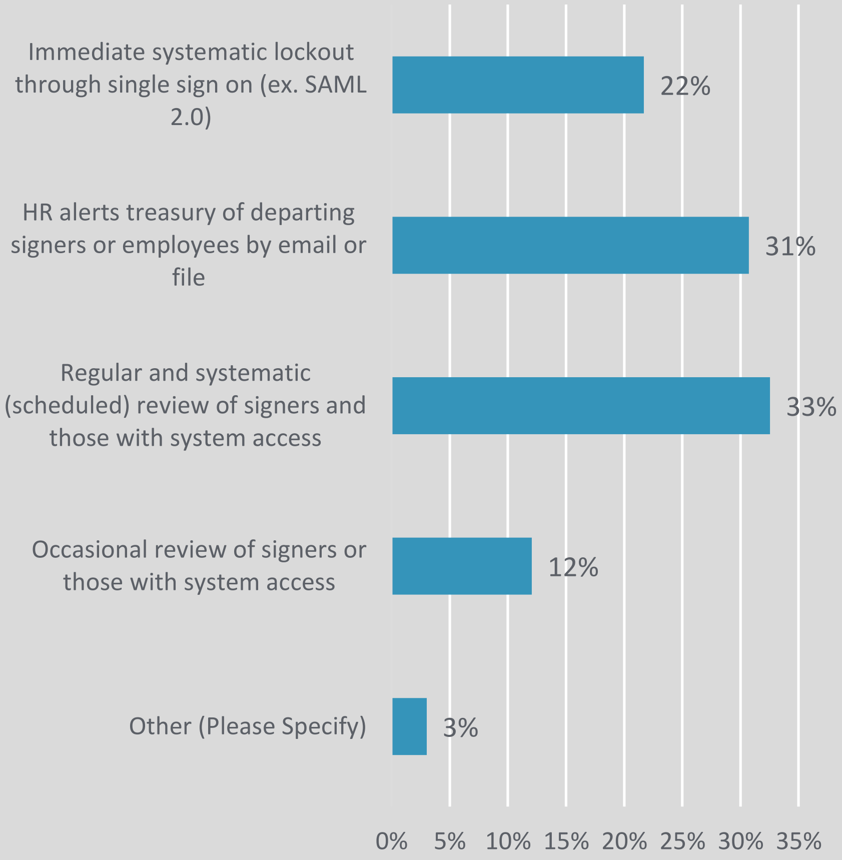
People / Employees

- *Regular training*
- *Testing on skills and response*
- *Fraud and security reviews*
- *Annual review*

Broader Community

- *SWIFT IOCs*

Access Control.
If someone leaves the organization, then system access is removed from treasury banking systems by:



Advising Clients, *Informing* the Industry.

#5 – Readiness / Response

Principle Overview

Definition

- Have a defined, well-understood plan to ensure everyone is ready and able to respond to a threat or an attack.

Questions to Ask

- Is the plan formal and defined, or informal and unwritten?
- Who should be called and alerted?
- Does your entire team know the plan?

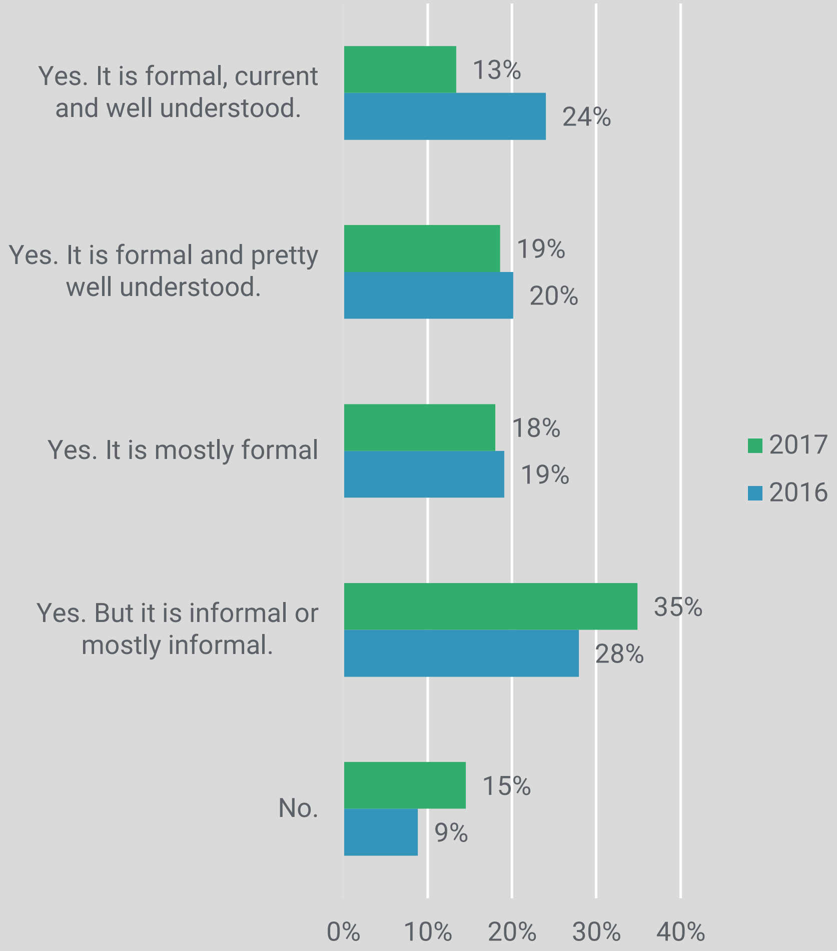
Leading Practices

- Define notification and restoration procedures
- Control access to contact information
- Communicate lockdown procedures

Ultimate Objective

- Have a well-defined plan of action for every step of a potential fraud.

Do you have a treasury fraud and controls framework?



#6 – Exact and Specific Accountability / Mgmt

Principle Overview

Definition

- Specify who holds responsibility in the organization for monitoring and responding to fraud attempts.

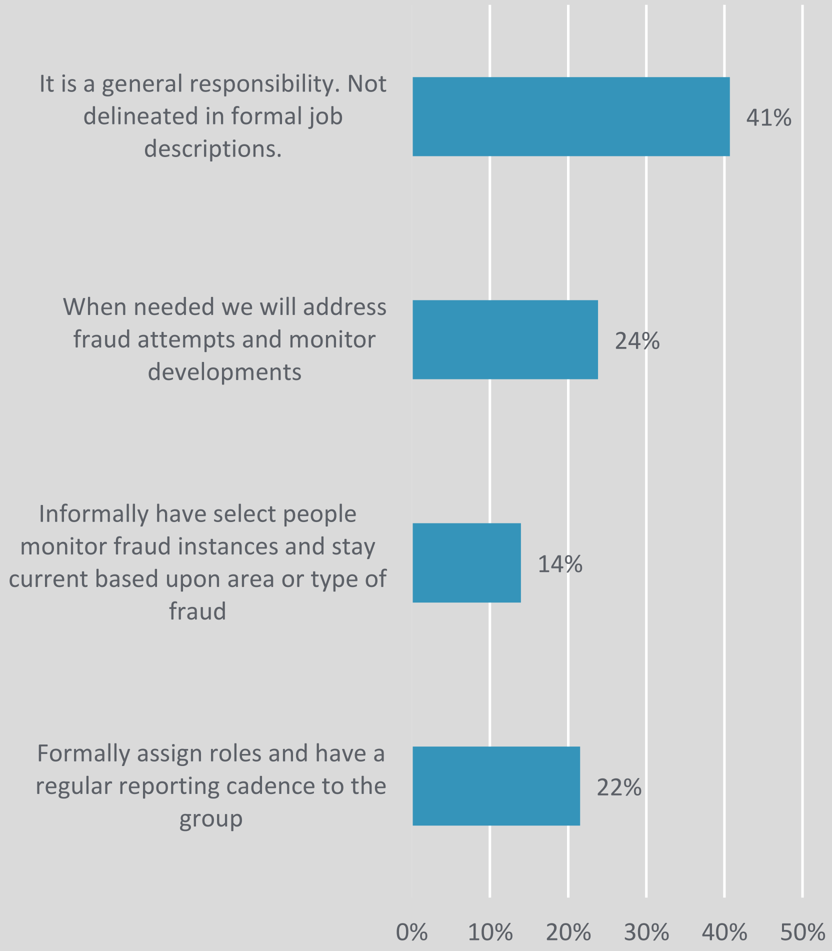
Leading Practices

- **Audit Trail**: A system will track activities by unique userID. The system logs or tracking should not be able to be altered or deleted as that could hide fraud or data breaches
- **Specific Accountability**: Control physical keys and key cards. Assign responsibility. Who is monitoring? Are their physical logs to track?

Ultimate Objective

- Have a process for assigning and tracking accountability.

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



Final Thoughts

Strategic Treasurer's 12 Security Principles

(S.E.C.U.R.E. C.L.A.M.P.S.)

- **S**peed Matters
- **E**ncryption and Control of Keys
- **C**hallenge / Verify
- **U**pdate Continuously
- **R**eadiness / Response
- **E**xact and Specific Accountability Management
- **C**ontrol / Dual Controls
- **L**ayers
- **A**wareness / Understanding / Testing
- **M**onitoring
- **P**rivilege
- **S**ecure Removal / Deletion of Data

Final Thoughts

Key Takeaways for Treasury:

Fraud is significant.

Criminals are adapting.

Criminals are using technology against you.

- Treasurers must be proactive in strengthening defenses against fraud.
- Internally educate your employees and have a defined fraud and controls framework.
- Clarify who is responsible for the proactive and reactive defenses in your organization.
- Stay aware of threats and do not underestimate fraud.

2018 Research Initiative & Training Resource

Live Survey

TREASURY FRAUD & CONTROLS

2018 Global Survey

- » *Fraud Experience*
- » *Structure & BAM*
- » *Reconciliation & Visibility*
- » *Control Framework*
- » *Cyber Risk Management & Data Protection*

Corporations & Banks

Chance to Win a pair of

Bose® Wireless Around-Ear Headphones

Available in

STRATEGIC TREASURER *Consultants in Treasury*

Underwritten by Bottomline Technologies

Learn more at **StrategicTreasurer.com**

Training Course

EMPLOYEE **TRAINING**

TREASURY SECURITY

ONLINE VIDEO **COURSE**

TRAINING · TESTING · DOCUMENTATION

Persistent · Updated · Subscription-Based

SecureTreasury™

IGNORING THE THREAT IS **NOT AN OPTION**

Learn more at **SecureTreasury.com**

Thank you for participating in this event!