

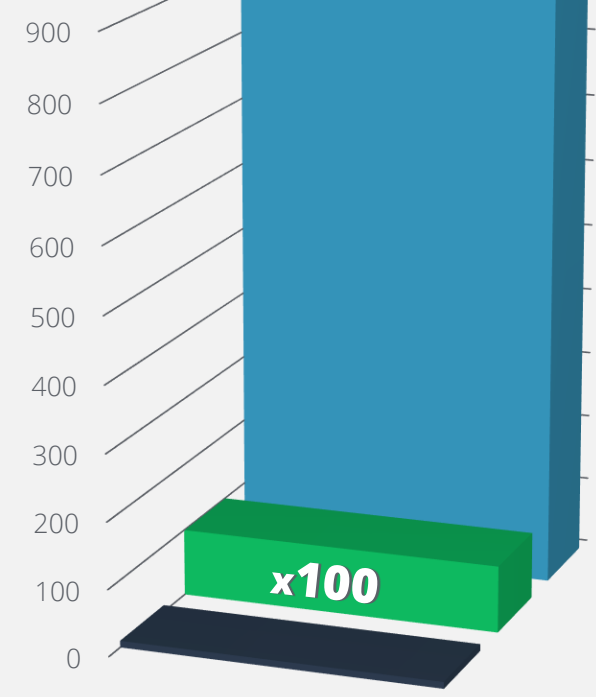
GLOBAL TREASURY FRAUD & CONTROLS 2016 SURVEY RESULTS



Security matters! Treasury professionals ranging from global multinational corporations to bank treasuries all the way to government and not-for-profit organizations **all view fraud, cyber-fraud and the necessary controls as highly important issues.** This heightened attention comes from very public incidents of data breaches as well as hard dollar losses from cyber/social engineered theft that are steadily on the rise.

The survey began in the fall of 2015 and was completed on January 2, 2016. Over 300 global respondents took part in this comprehensive study. More than 60% came from North America and over 25% were from EMEA. The remainder were from Asia-Pacific and Latin America.

CRIME DOES PAY!



SYSTEM FRAUD

Typical Payout Range:

\$1M-10M+

WIRE (BEC) FRAUD

Typical Payout Range:

\$130K+

CHECK FRAUD

Typical Payout Range:

\$1K-2K

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

The risk/reward calculus for criminals has changed as the potential payouts are larger than ever. While many corporates are on the watch for check fraud, **the larger targets remain unplanned for and vulnerable to attack.**

...& IT'S ON THE RISE

TOP FOUR TYPES OF FRAUD ATTEMPTS

1. CHECK FORGERY
2. WIRE / IMPOSTER FRAUD
3. ACH FRAUD
4. CHECK CONVERSION

While there has been a rise in wire and imposter fraud, survey data indicates that traditional check forgeries still remain on top of the list of attempts.

On the whole there has been a progressive increase in both fraud attempts and successes on multiple fronts.

REAL RATES OF LOSS

CHECK FORGERY

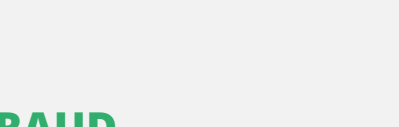
More than one in five firms that were targeted for check forgery suffered a loss in the past two years.



21%

WIRE FRAUD & IMPOSTER WITH WIRE

Nearly one in four firms targeted for this type of fraud experienced some loss over a 2-year period.



24%

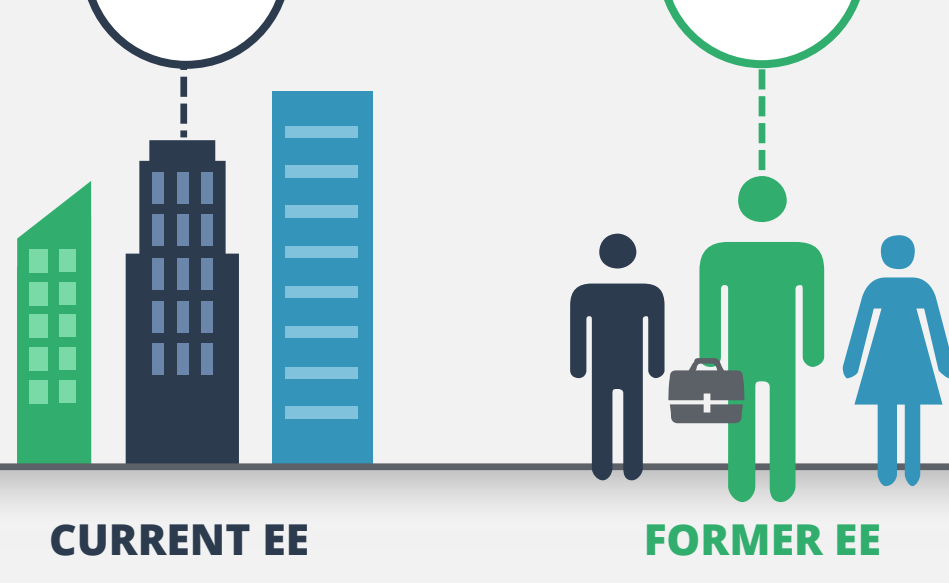
MAN IN THE EMAIL/IMPOSTER FRAUD

These large-sum fraud attempts resulted in 8% of firms overall suffering a loss (>10% who were targeted).



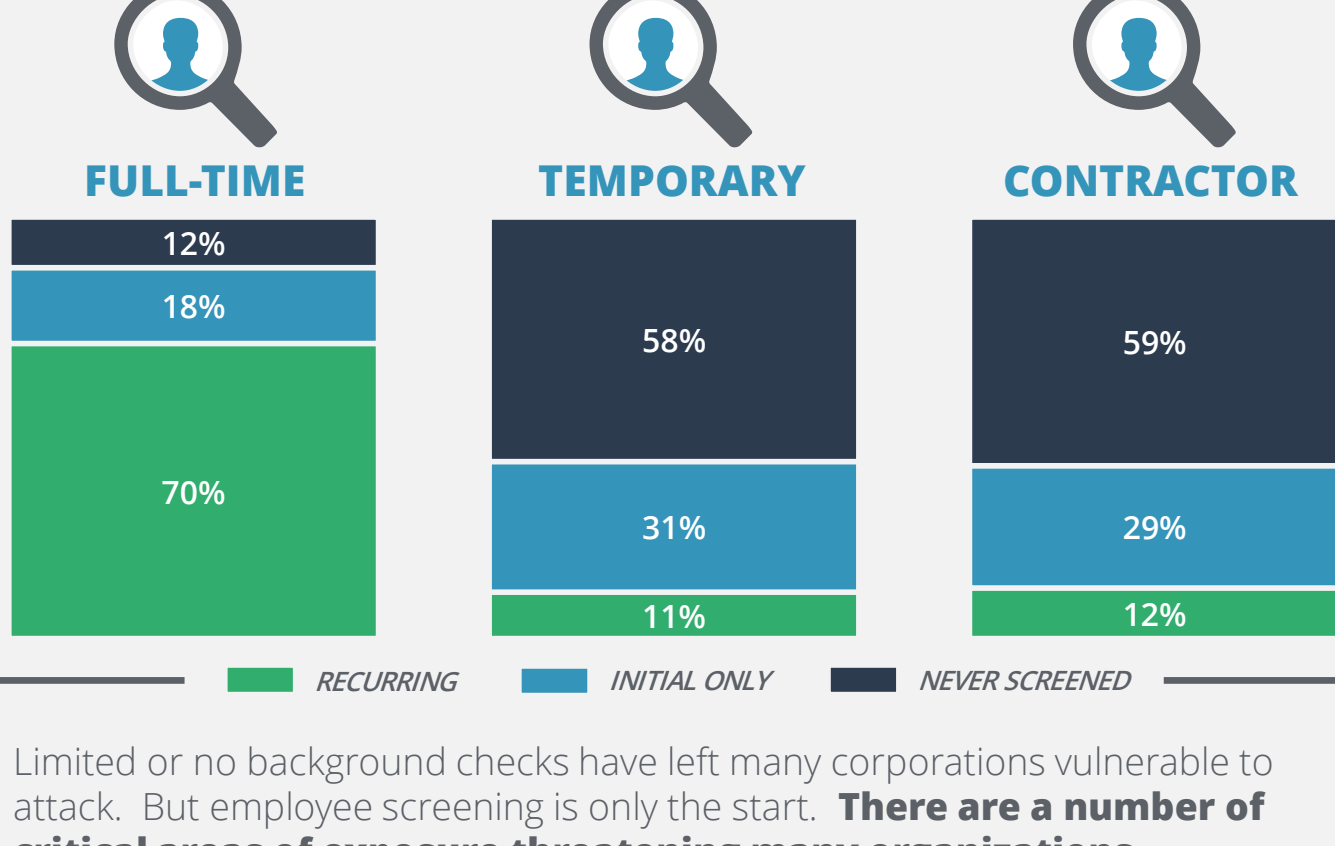
>10%

FROM INSIDE & OUT



Over 1/3 of respondents identified their corporation's employee (EE) roster (current + former) as a source of fraud for their firm. 59% of firms also claimed non-EE as a source and 11% claimed unknown and/or other sources as well.

EE SCREENING...



Limited or no background checks have left many corporations vulnerable to attack. But employee screening is only the start. **There are a number of critical areas of exposure threatening many organizations.**

AREAS OF HIGH RISK!

57%

CONTROL FRAMEWORK

57% of firms have no control framework. None. Nothing in treasury. Nothing at the company level.

42%

FRAUD MONITORING

Only 42% of firms have formally assigned fraud monitoring roles and responsibilities.

25%

CONTROL DESIGN

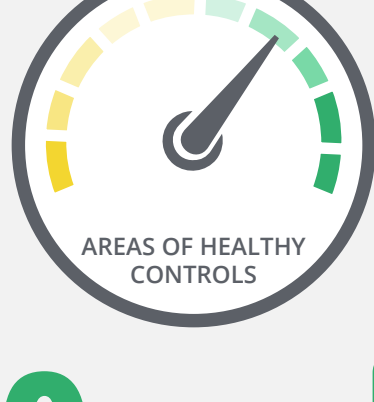
25% of firms have banking structures that do not (10%) or only partially (15%) reflect a control design.

35%

SANCTION SCREENING

35% of firms do NOT screen for sanctioned parties at any time in their processes, relying solely on banks.

POSITIVE PROGRESS...



45% → **>90%**

RECONCILIATIONS

45% of firms reconcile 90% or more of their bank accounts daily. 24% of firms reconcile 100% of their accounts daily.

70% →

A.B.A.C. POLICY

70% of respondents indicated their firm had an Anti-Bribery/Anti-Corruption policy on file. 16% were uncertain.

70% → **>90%**

VISIBILITY

70% of firms can see 90-100% of their bank account balances and activity on a daily basis.

LIMITED SYSTEM ACCESS PROVIDES ADDED PROTECTION

88%

MOBILE INITIATION

Do not allow mobile transaction initiation

90%

B.Y.O.D. POLICY

No transaction initiation from personal devices

PROTECTIVE TACTICS

TOP 2 TACTICS USED TO REDUCE EXPOSURE & INCREASE PROTECTION FROM LOSS

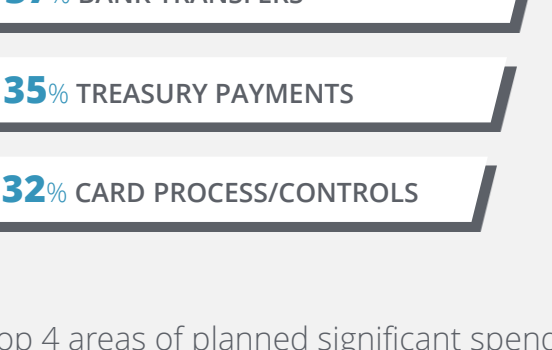
CYBERFRAUD INSURANCE

INCREASING COVERAGE VS DECREASING COVERAGE



The ratio of firms change in coverage year to year was 9:1 in favor of more protection.

TECHNOLOGY SPEND



The top 4 areas of planned significant spend to combat fraud and increase controls.

DOWNLOAD THE FULL REPORT

This infographic is intended to convey some interesting highlights of what your peers are experiencing and doing to prevent/detect fraud.

There's much more. →

Access the full report to learn from these fraud attempts and discover some of the best practices and plans for preventing future attacks.



StrategicTreasurer.com/2016-Treasury-Fraud-Controls

All of the above values are taken from the 2016 Global Treasury Fraud and Controls Survey Report, are Strategic Treasurer estimations, or are calculations from FBI and banking data. This survey is authored and published by Strategic Treasurer. It was underwritten by Bottomline Technologies.

Copyright © 2016 Strategic Treasurer, LLC