




Fraud Triangle Analytics

Applying Cressey's Theory to E-mail Communications

Part 2 of 2



Research indicates that e-mail communications can be a strong indicator of an employee's incentive/pressure, opportunity and rationalization – the three points of the Fraud Triangle.

A well-known statistic from the 2008 ACFE Report to the Nation on Occupational Fraud & Abuse says that 66 percent of occupational fraud is detected by anonymous tips or by accident rather than by internal audit, internal controls, or other measures. Internal audits discover only 19.4 percent of occupational fraud, according to the report. (See Figure 1 from the report on page 30.)

These statistics challenge the profession. Why isn't internal audit – often the focus of a large amount of time and money in organizations – at the top of the list for detecting incidences of fraud? Part of the answer could be right in front of many CFEs.

The Gartner Research Group, in its May 2005 study, "Introducing the High-Performance Workplace: Improving Competitive Advantage and Employee Impact," states that 80 percent of enterprise content – such as e-mails, user documents, presentations, and Web material – is unstructured in nature. Yet, most internal audit and anti-fraud testing only focuses on the remaining 20 percent of data that's structured, like financial accounting systems or transactional databases.

Reviewing someone's e-mails for potential fraud can be like searching for the proverbial needle in a haystack. Companies might also be a little squeamish about invading the personal privacy of their employees, even though they're typically scanning all employee e-mail activity daily for various threats.

This second part of a two-part article explores the methodology and research results of Fraud Triangle Analytics as it relates to e-mail communications and provides practical guidance on integrating this innovative monitoring approach into your internal audit and anti-fraud work plans.

By Dan Torpey, CPA; Vince Walden, CFE, CPA; and Mike Sherrod CFE, CPA

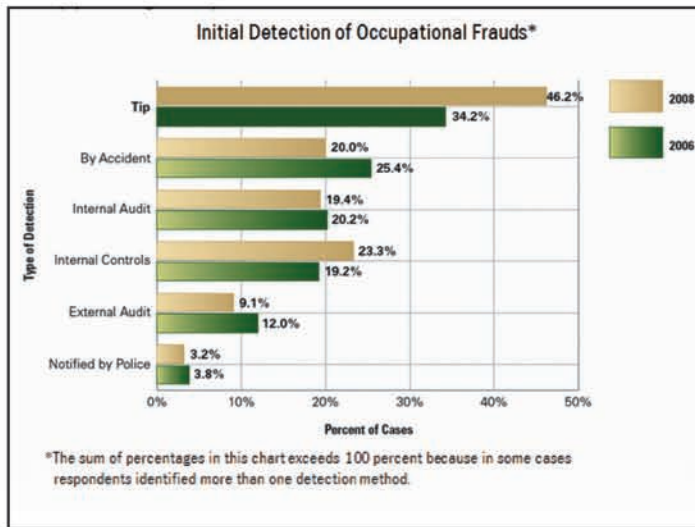


Figure 1

Yet, while organizations have access to the many volumes of e-mail data that flow to and from their offices, there hasn't been a systematic way to cull the data into an organized and effective anti-fraud solution. That is, until now. Welcome to Fraud Triangle Analytics.

ALIGNING KEYWORDS, TERMS AND PHRASES TO DETECT RISKS

In the May/June article, "Exposing the Iceberg," we introduced a method to detect fraud by analyzing employees' e-mails for keywords, terms and phrases (referred to hereafter as "keywords" for simplicity) that are directly related to the three legs of the well-known Fraud Triangle.

The Fraud Triangle illustrates some of the fundamental concepts of fraud deterrence and detection. In the 1950s, criminologist Dr. Donald R. Cressey (one of the co-founders of The

Institute for Financial Crime Prevention, the precursor to the ACFE) developed the Fraud Triangle to explain why people commit fraud. His premise was that all three components – incentive/pressure, opportunity, and rationalization – are present where fraud exists.

For the past year, Ernst & Young's fraud investigators (led by the authors of this article) and an ACFE research team (led by John Gill, J.D., CFE, ACFE's director of research) developed an objective list of keywords that are specific to each Fraud Triangle component. (See Figure 2.)

The team has accumulated, organized, and tested a library of more than 3,000 keywords distinctive to the major fraud categories: financial statement fraud, asset misappropriation fraud, and corruption fraud. We've also collaborated with the FBI and several Fortune 500 companies to refine the methodology.

STRONG INDICATORS OF TRIANGLE COMPONENTS

To discover whether e-mail communications are an effective indicator of employees' incentives/pressures, opportunities, and rationalizations, we selected two Ernst & Young cases: one that involved financial statement fraud where the company was recognizing revenue after the cut-off period, in which there was an eventual restatement, and another case that investigated foreign corruption using the U.S. Foreign Corrupt Practices Act (FCPA), which resulted in a conviction.

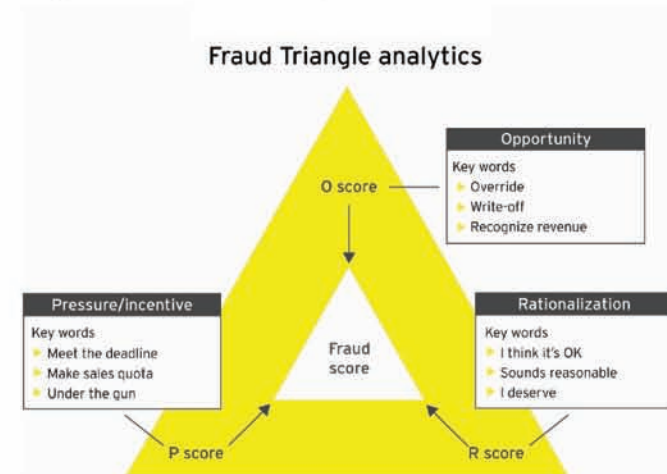


Figure 2

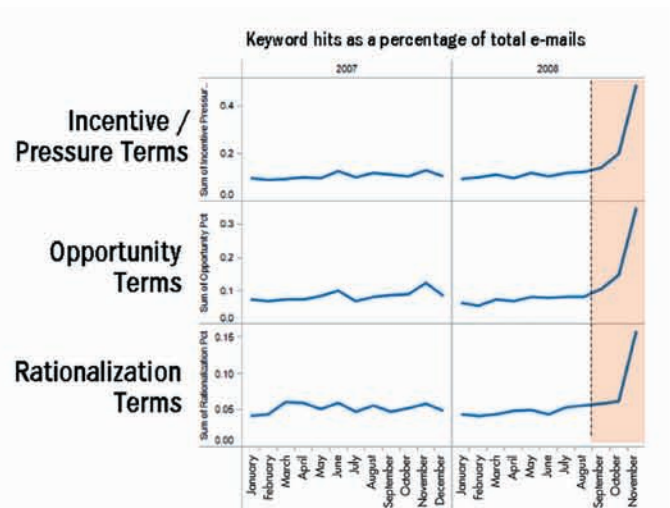


Figure 3

In the two cases, 21 individuals and more than 2 million e-mails were investigated. Both cases had been resolved when we began our analysis. Our hypothesis: to find an increase in the frequency of keywords from each Fraud Triangle component during the period of alleged fraudulent activity.

The first case, financial statement fraud with revenue recognition, involved a multinational company. Using commercially available text search and retrieval software, investigators searched

Reviewing someone’s e-mails for potential fraud can be like searching for the proverbial needle in a haystack. Companies might also be a little squeamish about invading the personal privacy of their employees, even though they’re typically scanning all employee e-mail activity daily for various threats.

INCENTIVE/PRESSURE TERMS
<i>problem, committing, creative, concern, not sure, clarify, split, spread, revise, sorry</i>
OPPORTUNITY TERMS
<i>correct, appropriate, reserve, misconduct, conditional, departing, discount, difficult, fail, critical</i>
RATIONALIZATION TERMS
<i>therefore, find out, it's OK, get back, challenge, find it, figure out, catch, does not make sense, doesn't make sense</i>

Figure 4

more than 1.9 million e-mails from 18 suspected executives and related attachments for the keywords in the “financial statement fraud library” we had compiled. The investigation period covered the three months of September, October, and November 2008.

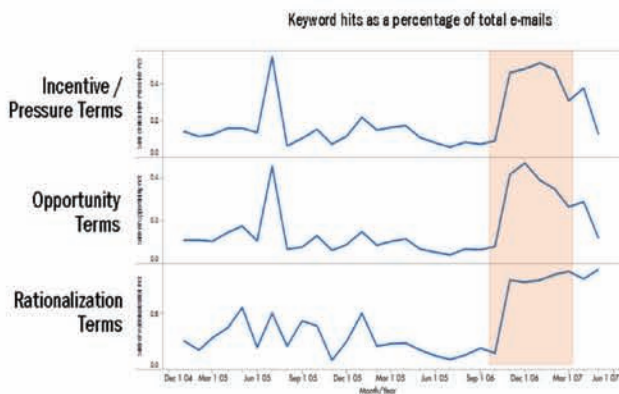


Figure 5

As demonstrated in Figure 3 on page 30, we observed a sharp increase in all three lists of keywords that we linked to the three components of the Fraud Triangle during the alleged

revenue recognition period of these 18 individuals. (Note that keyword hits are expressed as a percentage of total available e-mails in the database on a month-by-month basis for comparative purposes.)

Each list has its own set of distinct terms related to incentive/pressure, opportunity, and rationalization. This “co-occurrence” supports the Fraud Triangle theory that, at least in this example, all three components were present when revenue recognition issues existed.

The top 10 keywords from our financial statement fraud library that drove the hits during the period under review included those in Figure 4.

The corruption/FCPA case also involved a multinational company. Investigators searched more than 105,000 e-mails belonging to the three suspected executives for the keywords in our compiled “corruption fraud library.” The investigation went as far back as 2000; however, the key area of focus was the period from September 2006 through March 2007.

As shown in Figure 5, we observed sharp increases from these three individuals in all three lists during the alleged bribery period. (As in Figure 3, keyword hits are expressed as a percentage of total available e-mails in the database on a month-by-month basis for comparative purposes.) Once again, this co-occurrence supports Cressey’s theory that all three Fraud Triangle components are present when fraud, in this case bribery, was present.

The top 10 keywords from our corruption fraud library that drove the hits during the period under review included those in Figure 6. We also analyzed two additional corruption cases, which yielded similar results (not shown here). We don’t suggest that we can draw hard conclusions between e-mail communications and the three components of the Fraud Triangle at this time. However, the results from our investigations so far seem to demonstrate that there’s a correlation between the words used by

INCENTIVE/PRESSURE TERMS
<i>manage, risk, ethical, problem, commit, concern, clear, fake, cover, protect</i>
OPPORTUNITY TERMS
<i>policy, fund, complain, investigate, process fee, consult, audit, offshore, renewal, commission</i>
RATIONALIZATION TERMS
<i>therefore, challenge, complex, entitled, get back, catch, mistake, justified, find out</i>

Figure 6

individuals in e-mail communications and behaviors that show a manifestation of incentive/pressure, opportunity, and rationalization.

Perhaps even more important is that each Fraud Triangle component seems to co-occur at the same time during the fraudulent time period. We encourage the investigative community, including law enforcement, to conduct their own investigations using these methods.

APPLYING FRAUD TRIANGLE ANALYTICS

In the first part of this article, “Exposing the Iceberg,” in the May/June issue, the fictitious internal audit director, Bonnie Parker, and her team completed its fraud risk assessment. The team now has determined it needs to conduct additional testing of its 21-member sales department in Africa because they suspect some irregularities in the interactions among salespeople and government officials – a definitive fraud risk. Parker wants to run the corruption fraud library of keywords on e-mails to identify possible bribery evidence.

The internal audit team also customizes its keyword library to include company-specific jargon and industry or geographic-specific keyword terms or phrases. The team begins working with the IT department, in coordination with the company’s office of general counsel and related e-mail records policies adopted by the corporation, to collect the live server e-mail communications of the 21-person sales force team from the previous 90 days.

In this example, the members of the sales force team don’t need to know about the analysis because the internal audit team won’t be inspecting the hard drives of their work computers – just the company server that stores e-mails. This probe isn’t yet an investigation; it’s part of the company’s proactive fraud-monitoring efforts; however, if data is collected outside of the United States, international data privacy laws might be applicable especially in European countries. It’s important to consult with legal counsel prior to removing any data outside of the respective country.

NOW FOR A LITTLE MATH

After running the library of corruption fraud keywords contain-

ing the (1) incentive/pressure terms (P-Score), the (2) rationalization terms (R-Score) and the (3) opportunity terms (O-Score) against the e-mail communications, the internal audit team scored each of the lists independently and came up with an overall “fraud score” ranking for the 21 employees. The fraud score is the sum of squares $\sqrt{O^2 + P^2 + R^2}$ of each component, which allows Parker to sort from highest to lowest risk factor among the 21 employees as demonstrated in Figure 7.

Parker then plotted these scores on a graph. (See Figure 8) She identified the three individuals with the highest R-Score, P-Score, and O-Score. Those three employees, according to the Fraud Triangle theory, are most likely to have committed fraudulent activity.

Parker can follow up with additional e-mail “text” analytics procedures on the three high-risk individuals identified. Such procedures can include such questions as:

- Who’s talking to whom? (social network analysis)
- About what? (concept clustering and natural language processing)
- Over what time period? (time series analysis)

Focusing on the three individuals, rather than the 21, and combining the who, what, and when text analytics procedures mentioned previously, Parker can quickly identify key risks, errors or potential fraudulent acts in the data with minimal document-by-document review.

FRAUD TRIANGLE ANALYTICS AND YOUR ANTI-FRAUD EFFORTS

You can integrate Fraud Triangle Analytics into your anti-fraud program, especially if your organization has already conducted an

Person	P-Score	R-Score	O-Score	Fraud Score
1	0.90	0.93	0.82	1.53
2	0.98	0.89	0.92	1.62
3	0.86	0.89	0.87	1.52
4	0.38	0.49	0.30	0.69
5	0.88	0.76	0.07	1.16
6	0.40	0.67	0.02	0.78
7	0.91	0.03	0.78	1.20
8	0.38	0.51	0.50	0.81
9	0.93	0.57	0.29	1.13
10	0.92	0.26	0.22	0.98
11	0.62	0.03	0.56	0.84
12	0.42	0.60	0.29	0.79
13	0.71	0.93	0.71	1.36
14	0.37	0.94	0.26	1.04
15	0.60	0.75	0.68	1.17
16	0.99	0.41	0.07	1.07
17	0.07	0.22	0.50	0.55
18	0.78	0.76	0.60	1.25
19	0.73	0.12	0.46	0.87
20	0.36	0.56	0.09	0.67
21	0.45	0.00	0.23	0.50

Figure 7

The “perfect storm” of fraud is brewing as global economic conditions create increased pressure on earnings while internal controls weaken and staffs are reduced.

internal investigation in which e-mails were a source. The key to the process is developing three lists of words – corresponding to the three components of the Fraud Triangle – rather than a single random list of words.

The Fraud Triangle Analytics chart on page 54 shows steps you can take in conducting a fraud investigation.

FUTURE POTENTIAL FOR FRAUD TRIANGLE ANALYTICS

The “perfect storm” of fraud is brewing as global economic conditions create increased pressure on earnings while internal controls weaken and staffs are reduced. As bonuses are cut and workloads

established fraud theory. When combined with traditional rules-based analytics, Fraud Triangle Analytics can be a powerful tool for identifying large and unusual anomalies derived from the multidimensional attributes in e-mail communications surrounding high-risk business events. The results can then be linked back to journal entries as valuable, corroborative evidence.

Fraud Triangle Analytics focuses on high-risk areas in which controls might not necessarily exist or are perhaps even bypassed and, therefore, it fits naturally into creating a more robust fraud risk assessment.

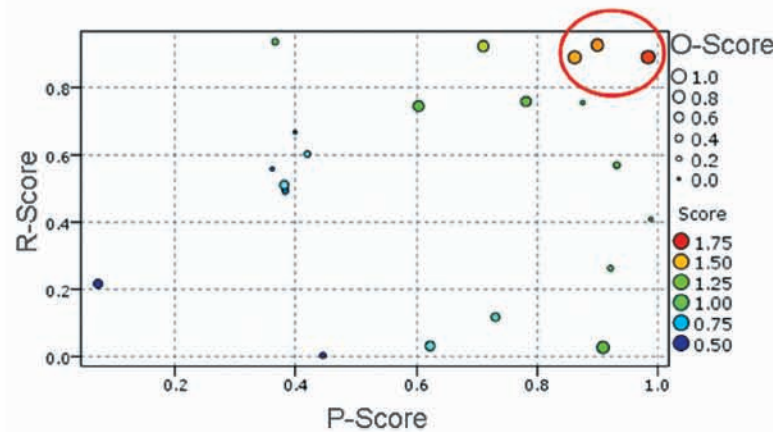


Figure 8

increase, there also might be an enhanced rationalization to commit fraud. Companies worldwide are identifying processes and methodologies to proactively fight fraud.

The concepts in this article might appear to be nontraditional or outside the “comfort zone” for some because we are analyzing employees’ e-mails. These methods surely are different from traditionally analyzing journal entries with ACL, Microsoft’s Access, or Excel. Those tools typically rely on “rules-based queries” that require an auditor to “ask questions of the data” based on what is currently known. This approach often requires both time and luck to uncover potential anomalies in data that could include indicators of fraudulent activity.

However, we want to help companies bolster their fraud-detection efforts by incorporating new techniques based on

Over time, we expect our library of words, terms and phrases – co-developed by the ACFE – to grow as we conduct more reactive fraud examinations and proactive risk assessments for our clients across multiple industries.

The Ernst & Young/ACFE keyword list is proprietary and only available to our clients as we continue to invest resources in updating the library with current events and new fraud risks. However, we encourage companies to develop their own keyword libraries based on their previous fraud risks and unique experiences. Similar to Ernst & Young, companies adopting Fraud Triangle Analytics should also strive to update their lists because fraud risks are in constant flux. As companies expand globally, bribery, and corruption issues and

FCPA stipulations are rising to the top of managements’ list of concerns, and as such, we need to increase our global libraries of words, terms, phrases, and local idioms. For example, in Brazil, to “buy one a cup of coffee” can be used as an expression to offer a bribe.

With help from our global offices, we have translated our keyword library into six languages, including Chinese, Spanish and Russian, and have also added regional idioms. Our long-term goal is to have a library with added local idioms for each of the 140 countries in which we conduct business.

CUTTING COSTS, DETERRING FRAUD

We’re still amazed to discover strong evidence in suspects’ e-mails during a reactive fraud examination. But fraud examiners are often bewildered when they are assigned to proactively

FRAUD TRIANGLE ANALYTICS	
Conduct a fraud-risk assessment to identify areas of focus.	<ul style="list-style-type: none"> • Assess tone at the top, anti-fraud training, and code of ethics.
	<ul style="list-style-type: none"> • Evaluate internal and external fraud risks. • Conduct facilitated sessions outside of the internal audit department. • Conduct employee surveys (via intranet, e-mail or the Web).
	<ul style="list-style-type: none"> • Prioritize risks by “likelihood of occurrence” (x-axis) and “business impact” (y-axis).
	<ul style="list-style-type: none"> • Conduct a brainstorming session to develop a company-specific library of keywords corresponding with incentive/pressure, opportunity, and rationalization. Maintain this list and modify over time as risks change. Consider global translation with local idioms.
Map top risks to business units and business units to key employees.	<ul style="list-style-type: none"> • Identify top risks and map to key employees.
	<ul style="list-style-type: none"> • Discuss data sources for selected employees. (A minimum of 10 employees is a good rule of thumb to provide enough data for a peer comparison analysis.)
	<ul style="list-style-type: none"> • Consult with in-house legal or executive management to confirm corporate e-mail policy. (Note: If data collection is outside the United States, be sure to comply with international data privacy laws, especially in European countries. Consult with legal counsel prior to removing any data outside of other countries.)
	<ul style="list-style-type: none"> • Coordinate with IT to identify available e-mails on the corporate server. Three to six months of e-mails will suffice, but one year is best. (You could review e-mails on individuals’ hard drives. But this is still a proactive assessment, not an internal investigation. So the time, expense, and interruptions might not be warranted.)
	<ul style="list-style-type: none"> • Ask IT to copy the selected individuals’ e-mail files from the server to an external storage device for off-line processing.
Process the e-mail data and conduct searches and related analytics.	<ul style="list-style-type: none"> • Load e-mail into an analysis search engine or various electronic discovery software applications. (Several outside service providers can process this data and conduct the searches for you for less than \$1,500 per gigabyte of data processed. All you provide are the e-mails and the keyword library.)
	<ul style="list-style-type: none"> • Execute the search-term library on the data set. • Employee analysis: Rank employees with keyword hit frequency scoring by who has the highest over all hits from all three libraries. (See Figures 7 and 8.)
	<ul style="list-style-type: none"> • Time series analysis: Plot the e-mail hit frequency of the data set as a percentage of the overall documents/e-mails available in the database on a month-by-month basis and look for spikes in which all three libraries are increasing together (see Figures 3 and 5) indicating that the Fraud Triangle conditions might be present.
	<ul style="list-style-type: none"> • Targeted time series analysis: Perform the same time series analysis on the individuals with the highest key-word hits.
Perform additional, more focused, analytics on those high-risk individuals with the highest “fraud score.”	<ul style="list-style-type: none"> • Conduct additional e-mail analytics to understand the “who,” “what,” and “when” of the key communications surrounding the period of interest.
	<ul style="list-style-type: none"> • If findings of the reports appear suspicious, consider reviewing some e-mails in the critical time period (typically fewer than 100 if targeted correctly) to understand the full context.
	<ul style="list-style-type: none"> • If you identify highly suspicious or suspected illegal acts, notify internal counsel and/or executive management immediately. (Follow your company’s code of conduct policy, etc.)
	<ul style="list-style-type: none"> • Consider interviewing suspected individuals’ supervisors for additional information or the individuals directly.
	<ul style="list-style-type: none"> • As always, of course, use good judgment and don’t jump to conclusions. As CFEs know, we must invoke due process.

Fraud Triangle Analytics focuses on high-risk areas in which controls might not necessarily exist or are perhaps even bypassed and, therefore, it fits naturally into creating a more robust fraud risk assessment.

search through thousands of e-mails generated by fraud suspects in high-risk areas.

Routine Fraud Triangle Analytics can simplify procedures while reducing investigation and litigation expenses by catching fraud in its earliest stages. Employee fraud awareness training and an understanding of the fraud risks in areas of increased exposure throughout an organization can lead to a more heightened awareness of fraud.

While we can't eliminate fraud, we view Fraud Triangle Analytics as one of the newest forms of fraud detection. It's a great tool if used effectively in conjunction with oversight and other measures to control fraud exposure. We recognize that there will still be fraudsters and that Fraud Triangle Analytics can't catch all of them; however, it might help to reduce or identify fraud risk earlier. 🔍

Dan Torpey, CPA; Vince Walden, CPA, CFE; and Mike Sherrod CPA, CFE, are members of Ernst & Young's Fraud Investigation & Dispute Services Practice. Their e-mail addresses are: daniel.torpey@ey.com, vincent.walden@ey.com, and mike.sherrod@ey.com.

The authors recognize these individuals for their assistance with the research supporting this article:

John Gill, J.D., CFE, research director, ACFE
 Dawn Taylor, CFE, accounting editor, ACFE
 Andi McNeal, CFE, CPA, research program manager, ACFE
 Pavan Jankiraman, CFE, Ernst & Young
 Anil Markose, CISSP, Ernst & Young
 James Phung, Ernst & Young

The views expressed in this article are those of the authors and don't necessarily reflect the views of Ernst & Young LLP.

ERNST & YOUNG
Quality In Everything We Do

Reprinted from the July/August 2009 issue of

FRAUD
 M A G A Z I N E