

Austin Area Chapter Association of Certified Fraud Examiners

Update of Chapter Activities

Fall Seminar – The Fall Seminar was another outstanding success, and we would like to thank the speakers who took so much time to research and present the information: Bill Atwood, Joe Collins, Michelle Yankovich, Alyssa Martin, John Knox, and Mike Garner. Don't forget to register early this year for the Spring Seminar, which will be held on Thursday, April 19th. We should have an impressive lineup of speakers and topics prepared for you.

Spring Scholarships – Please note that we are accepting scholarship applications through March 31st, and plan to award scholarship winners at the April seminar meeting. Please advise any accounting/criminal justice/business majors you are in contact with to visit our website at austinacfe.com for a scholarship application form.

Community Services Project – The chapter has raised and approved a donation of \$300 to the Bastrop Wildfire victims. You can still go to our website's homepage and click on the link to the right to donate additional funds.

January lunch meeting – please note that the January lunch meeting will be on the 2nd Monday of the month – January 9th, in order to schedule around holiday activities. Merry Christmas everyone!

Chapter Meeting Schedule

Time: 12:00 p.m. to 1:00 p.m.

Location: Catfish Parlour
4705 E Ben White Blvd

Cost: Luncheon Only:
Members and Non-members \$12.00

Date: January 9, 2011

Speaker: Jared Jordan and Todd Lester
Navigant

Topic: Managing Risk and the Role of
Forensic Investigations in Data
Breaches

register on line: www.austinacfe.com
or

call 512-923-8656



INSIDE THIS ISSUE

- 2 What You Missed and Board & Committee Members
- 6 Speaker Biography
- 7 The Spotlight's on You!

What You Missed

By Mike Garner, CFE, CIA

If you were not able to attend the December 7, 2011 fall chapter seminar, you missed presentations on "Fraud Control Decomposed" by Mr. Bill Atwood, consultant in the areas of fraud examination, forensic accounting, auditing, tax, information systems, and enterprise reporting and planning systems; "Inside Job-Deceit on Wall Street" by Mr. Joe Collins, financial advisor and licensed broker; "Prevalence of Fraud and the Importance of Prevention" by Ms. Michelle Yankovich, Advisory Services Partner with Weaver and Ms. Alyssa Martin, Advisory Services Executive Partner with Weaver; and "Identity Theft" by Mr. Mike Garner, Compliance Director at the Texas Adjutant General's Department and Mr. John Knox, Principle Partner in a CPA firm specializing in litigation consulting and taxation.

Fraud Control Decomposed – The objectives of this session were to reexamine the fraud triangle; understand the role of controls; understand the underlying control issues applicable to any business environment; and to articulate some common elements of control. Mr. Atwood emphasized that fraud control is about internal controls that minimize fraud opportunities including pervasive constraint; identifying the stakeholders; addressing the tone at the top; and ensuring segregation of duties. The role of controls includes effective accomplishment driven by compliance. Internal control failures can be intentionally created or through error but the impact will be negative.

To assist in accomplishing control objectives, organizational alignment and process articulation must be understood across the organization. Mr. Atwood also discussed the budget as a control element; process controls; and the importance of organizational design in any system of control.

Inside Job-Deceit on Wall Street – Mr. Collin's presentation included discussions of the financial meltdown and the 2008 stock market crash related to unethical activities, fraudulent collateralized loans, and greed. He discussed what happened, how it happened, and why it happened. The resulting financial crisis will take at least a generation to resolve. Derivatives of what happened included low interest rates; predatory lending; easy credit; "asleep at the wheel" regulators; toxic mortgages; speculation; and option Adjustable Rate Mortgages (ARM).

Mr. Collins discussed Bank Transfer Day and its effect on big banking institutions. Bank Transfer Day encouraged bank customers to transfer their cash out of big banks to credit unions.

continued on page 3

AUSTIN AREA CHAPTER OF
THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS
PO Box 13462, AUSTIN, TEXAS 78711

BOARD & COMMITTEE MEMBERS

FISCAL YEAR 2012

Glyn Rogers, President
glynrogers@letu.edu
512-748-4953

Andrew Prough, Vice-President
andyprough@texasfraudexaminers.com
512 262-8760

David Heater, Treasurer
David.Heater@att.net
512-923-8656

Mike Garner, Secretary
Adjutant General's Department
Mike.D.Garner@tx.ngb.army.mil
512 782-5640

Shari Daffern, Director
Texas Water Development Board
shari.daffern@twdb.state.tx.us

Marci Sundbeck, Director
Employees Retirement System
marci.sundbeck@ers.state.tx.us
512 867-7302

Tracy Bohmer, Director
tracy@tracybohmercpa.com
512 303-3880

Gilbert Mokry, Director
Texas Water Development Board
gilbert.mokry@twdb.state.tx.us

John Knox, Director
jbkcpapc@sbccglobal.net

The event is in response to Bank of America's decision to charge its debit card users with a \$5 monthly fee and Wells Fargo's \$3 monthly charge of the same. Both Bank of America and Wells Fargo cancelled these fees due to customer feedback. The purported reason for charging these fees was the Durbin Amendment which went into effect 1 October 2011 and limits the fees that banks can charge merchants when a consumer swipes their debit card from 44 cents to 24 cents. According to experts, a customer making 25 debit card transactions a month would lead the bank to lose \$5 it would have made before the Durbin Amendment. As a result, many of the larger banks planned to making up for lost revenue by charging for debit card use, the cost ranging anywhere from \$3 to \$5 per month.

The Gramm–Leach–Bliley Act (GLB), also known as the Financial Services Modernization Act of 1999, (Pub.L. 106-102, 113 Stat. 1338, enacted November 12, 1999) is an act of the 106th United States Congress (1999–2001). It was signed into law by President Bill Clinton and it repealed part of the Glass–Steagall Act of 1933, opening up the market among banking companies, securities companies and insurance companies. The Glass–Steagall Act prohibited any one institution from acting as any combination of an investment bank, a commercial bank, and an insurance company.

The meltdown - The Gramm–Leach–Bliley Act allowed commercial banks, investment banks, securities firms, and insurance companies to consolidate. For example, a commercial bank holding company merged with an insurance company in 1998 to form the conglomerate Citigroup, a corporation combining banking, securities and insurance services under a house of brands that included Citibank, Smith Barney, Primerica, and Travelers. This combination, announced in 1998, would have violated the Glass–Steagall Act and the Bank Holding Company Act of 1956 by combining securities, insurance, and banking, if not for a temporary waiver process. The law was passed to legalize these mergers on a permanent basis. GLB also repealed Glass–Steagall's conflict of interest prohibitions "against simultaneous service by any officer, director, or employee of a securities firm as an officer, director, or employee of any member bank."

Mr. Collins then provided a history lesson on some of the causes of the financial crisis. The Financial Crisis Inquiry Commission (commission) reported in January 2011 that from 1978 to 2007, the amount of debt held by the financial sector soared from \$3 trillion to \$36 trillion, more than doubling as a share of gross domestic product

continued in next column

The very nature of many Wall Street firms changed—from relatively staid private partnerships to publicly traded corporations taking greater and more diverse kinds of risks. By 2005, the 10 largest U.S. commercial banks held 55% of the industry's assets, more than double the level held in 1990. On the eve of the crisis in 2006, financial sector profits constituted 27% of all corporate profits in the United States, up from 15% in 1980. The commission concluded that the crisis was avoidable and was caused by: widespread failures in financial regulation, including the Federal Reserve's failure to stem the tide of toxic mortgages; dramatic breakdowns in corporate governance including too many financial firms acting recklessly and taking on too much risk; an explosive mix of excessive borrowing and risk by households and Wall Street that put the financial system in crisis; key policy makers ill prepared for the crisis, lacking a full understanding of the financial system they oversaw; and systemic breaches in accountability and ethics at all levels.

Mr. Collins discussed a credit default swap (CDS) as a form of insurance. If a borrower of money does not repay a loan, it defaults. If a lender has purchased a CDS on that loan from an insurance company, the lender can then use the default as a credit to swap it in exchange for a repayment from an insurance company. However, one does not need to be the lender to profit from this situation. Anyone (usually called a speculator) can purchase a CDS. If a borrower does not repay his loan on time and defaults not only does the lender get paid by the insurance company, but the speculator gets paid as well. It is in the lender's best interest that he gets his money back, either from the borrower, or from the insurance company if the borrower is unable to pay back his loan. However, it is in the speculator's best interest that the borrower never repays his loan and defaults because that is the only way that the speculator can then take that default, turn it into a credit, and swap it for a cash payment from an insurance company.

Mr. Collins discussed whether a financial meltdown could happen again and then went into MF Global's filing for bankruptcy on October 31, 2011. MF Global Holdings, once run by former Goldman Sachs Group Inc. co-chairman Jon Corzine, filed the eighth-largest U.S. bankruptcy after a wrong-way \$6.3 billion trade on its own behalf on bonds of some of Europe's most indebted nations (specifically Greece – see voluntary debt write-downs in the information included below). In disclosing information during the bankruptcy there was \$1.2 Billion of client assets identified as missing.

He then moved to what is happening in Europe and specifically Greece. When Greece joined the European Union they went on a borrowing and spending spree.

This was due in part to the low interest rates that poorer European Union countries like Greece, Spain, Portugal, Italy, and Ireland were able to use to borrow as part of this union (the same rate as financially prudent and stable countries such as Germany and France). Since these poorer countries had higher inflation rates than the rates at which they could borrow, there was incentive for them to borrow and spend. In order to get into the European Union, Greece needed to reduce its debt and to do so they received what amounted to off the books loans from Goldman Sachs (through a derivative identified as a currency trade rather than a loan) amounting to over \$3 Billion in 2000-2001. This derivative has already cost Greece much more than the original off-balance sheet accounting loan and still is paying Goldman Sachs debt type payments, transaction fees, and indirect costs.

Mr. Collins explained the interrelationship of the European Union debtor nations (Greece, Spain, Portugal, Italy, and Ireland) to not only the other European Union nations but to all nations through the banking industry. Some of the causes of the Euro crisis included that 27 countries adopted the Euro, borrowing was used to fund public sector wages, borrowing was used to fund public sector pensions, borrowing was used to live beyond their means, allowing government debt to increase higher than the country's Gross Domestic Product (GDP), lack of accounting and reporting controls, and lax controls by regulators.

European financial institutions are already bailing out Greece, Portugal, and Ireland and it appears that additional bailouts will continue to be needed for these countries and Italy and Spain are next. In the case of Greece investors have already been required through agreements to voluntary debt write-downs sometimes known as "haircuts." This led in part to MF Global's bankruptcy (see above).

To forestall the US financial crisis the federal government loaned more than \$7.7 Trillion in connection with the financial crisis. The banks receiving these loans reaped an estimated \$13 billion of income by taking advantage of these below-market interest rates. Mr. Collins also mentioned the following: Judge tosses out \$285 Million plea deal reached between the SEC and Citigroup for Citigroup's misleading investors (investors lost over \$700 Million while Citigroup profited \$130 Million); SEC charges related to the financial crisis included 81 companies and individuals, 39 senior management officers, 24 director level positions, and totaling \$1.97 Billion in financial penalties and recoveries; underwater mortgages; and federal loans to big banks.

continued in next column

The Prevalence of Fraud and the Importance of Prevention – Ms. Yankovich and Ms. Martin started their presentation with the definition of Fraud then covered identifying fraud schemes, the prevalence of fraud, the fraud risk assessment, methods to mitigate fraud risk, and then closed with real world examples. Fraud was defined as any illegal act characterized by deceit, concealment, or a violation of trust. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.

In helping those in attendance better understand the prevalence of fraud they discussed the overwhelming fraud statistics in the workplace from the mailroom to the boardroom. Then quickly went into the focus of their presentation which was fraud prevention.

Prevalence of Fraud - Ms. Yankovich and Ms. Martin discussed the red flags of fraud including inventory adjustments and shrinkage; compensation tied to operating results; consistently meet or exceed expectations; operations in countries with history of bribery; related party transactions; lackadaisical oversight; etc. Primary fraud risk factors include: lack of internal controls; lack of management review; override of existing controls; poor tone at the top; and the lack of independent checks (audits). Provided information and related case studies on fraud schemes involving kickbacks, competitive bid rigging, bribery, conflicts of interest, and falsification of documents.

The Prevalence of Fraud and the Importance of Prevention – Ms. Yankovich and Ms. Martin started their presentation with the definition of Fraud then covered identifying fraud schemes, the prevalence of fraud, the fraud risk assessment, methods to mitigate fraud risk, and then closed with real world examples. Fraud was defined as any illegal act characterized by deceit, concealment, or a violation of trust. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.

In helping those in attendance better understand the prevalence of fraud they discussed the overwhelming fraud statistics in the workplace from the mailroom to the boardroom. Then quickly went into the focus of their presentation which was fraud prevention.

Prevalence of Fraud - Ms. Yankovich and Ms. Martin discussed the red flags of fraud including inventory adjustments and shrinkage; compensation tied to operating results; consistently meet or exceed expectations; operations in countries with history of bribery; related party transactions; lackadaisical oversight; etc.

Primary fraud risk factors include: lack of internal controls; lack of management review; override of existing controls; poor tone at the top; and the lack of independent checks (audits). Provided information and related case studies on fraud schemes involving kickbacks, competitive bid rigging, bribery, conflicts of interest, and falsification of documents.

A typical organization loses 5% of its annual revenue to fraud. The median occupational fraud loss is \$160,000 and lasts about 18 months before being detected. Nearly one-quarter of all frauds involve losses over \$1 Million. Fraud occurs most often at private companies (over 40%); then public companies (over 30%); then Government agencies (over 15%) and non-profits (less than 15%) - 2010 Association of Certified Fraud Examiners "Report to the Nations."

Fraud schemes ranked by number of cases include billing schemes, check tampering, corruption, skimming, expense reimbursement, non-cash, cash on hand, payroll, larceny, financial statement, and disbursements. The perpetrators of fraud are more likely to be an employee (employee 46%, manager 37%, and owner/executive 17%) but the median loss amount of each fraud is much higher with the owner/executive (employee \$50,000, manager \$150,000, and owner/executive \$485,000) - 2010 Association of Certified Fraud Examiners "Report to the Nations."

The fraud impact on companies is extensive because not only do you have potentially large financial costs associated with the fraud but you also have business disruption, loss of staff productivity, loss of confidence and trust in the company and the company's management, loss of employees, and loss of current and future investment and/or grant funding. The best practices used to prevent fraud includes creating a organization-wide culture of integrity from the top throughout operations; conduct a fraud risk assessment on a regular basis; and develop a deterrence plan in response to the risks identified in the fraud risk assessment.

Fraud Risk Assessment – Ms. Yankovich and Ms. Martin (Weaver) walked us through a fraud risk assessment and the differences from an internal audit risk assessment. Risk is defined as the degree of probability than an unfavorable event will significantly impact a functional area's ability to meet their objectives and the related internal control objectives. A fraud risk assessment will identify and recognize fraud risks in the organization, determine their likelihood, and determine methods to manage and mitigate the fraud risk. The fraud risk assessment allows you to determine critical information; identify systems that process, store, or transmit critical information; discover vulnerabilities; and create new processes, controls, and procedures for mitigating fraud risk.

The assessment and monitoring plan is a key element in identification, prevention, and detection of fraud. The risk assessment methods include brainstorming possible fraud schemes and scenarios; identify gaps in accounting that could be exploited; evaluate controls design and operation; and improve prevention safeguards.

Weaver then went through the risk assessment process including identifying and assigning a risk rating to possible fraud schemes. The risk rating will help determine the significant fraud risk exposures areas that should be assessed.

continued in next column

The risk rating system used by Weaver includes a rating of likelihood and associated impact. The results are then ranked for each evaluated organizational area and then Weaver develops a risk map with legend and an illustrated heat map that identifies the top fraud risks.

Mitigating Fraud Risks – Weaver links risk responses to the fraud triangle. Anti-fraud controls are built to deter or prevent the ability, incentive, and opportunity to commit fraud. This can be done through strengthening existing systems, processes, and procedures and implementing new procedures and controls. Weaver prepares a list of processes; potential fraud schemes associated with each process; and a control response associated with each potential fraud scheme. It was emphasized that fraud schemes are not static and considerations should be given to the economic environment; the organization structure and culture; and the industry. The organizational structure, systems of risk management, and systems of controls should be robust enough to identify and address new vulnerabilities as they emerge.

An important fraud prevention step is to identify what you are already doing that helps prevent and combat fraud including which departments perform risk assessments; the control activities already being performed that address fraud risks; and the automated controls that have already been implemented to help prevent and detect fraud in the organization. Fraud prevention measures include a commitment of company resources; prosecuting offenders; ensuring appropriate segregation of duties; performing regular internal audits; implementing aggressive and preventive Information Technology controls; implementing a fraud hotline and investigating fraud tips; and establishing checks and balances for ongoing monitoring.

Fraud Detection – When identifying and investigating fraud Weaver recommended that we focus on the five core elements of intent, motive, opportunity, repetitive acts, and concealment. Analytical techniques for fraud detection include data mining or IT forensics techniques; statistical analysis techniques; and classification, verification, and validation techniques. Weaver discussed each of these techniques.

In order of occurrence the methods used for initial fraud detection include: tips (40%); management review (15%); Internal Audit (14%); by accident (8%); account reconciliation (6%); document examination (5%); External Audit (4%); and other (8%) - 2010 Association of Certified Fraud Examiners "Report to the Nations."

Closing – Weaver closed their presentation with a number of real world examples of fraud where they had some involvement in the investigation and identification of recommended corrective actions. There was a great deal of interaction during this part of the presentation.

Key takeaways were provided for each of the scenarios discussed. These takeaways included; exit interviews can be a valuable learning tool; Human Resources is often the last point of contact before an employee leaves the organization so find out if HR personnel are attuned to the issues being raised if they have the proper escalation path when critical issues are identified; trust but verify; implement controls around segregation of duties to safeguard assets; employees that interact directly with vendors should be made aware of the ethical requirements of their position; internal auditors should be sensitive to red flags during their audits (signs of discomfort, obvious defensiveness, lack of review, lack of segregation of duties); the Foreign Corrupt Practices Act is an important concern for organizations with international operations; automated controls that lock down data modification would have been effective as preventive controls (invoice dates could not have been modified); audit procedures that may seem routine actually do catch frauds (accounts receivable confirmations red flags); and maintain professional skepticism. It is important to know from where complaints tend to come; ensure that the communication channels are clear; that routing and escalation procedures are well-defined so that issues can be dealt with at the lowest level required to effectively and thoroughly resolve the complaint.

Identity Theft – The team of Mr. John Knox and Mr. Mike Garner (team) provided a presentation on identity theft. Estimates indicated that as many as 9 million Americans have their identities stolen each year. Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes. The presentation focused on the criminal aspects of identity theft; the types of identity theft; who commits identity theft; who maintains the statistics related to identity theft; how to prevent identity theft; and what to do if it happens to you.

Identity theft is a violation of both federal and state law. In Texas it is a felony with increased felony degrees depending on the number of identity items stolen. Also if the identity theft is against the elderly (65 or older) the felony is automatically increased by one degree (example from 1st degree felony to 2nd degree).

The types of identity theft include criminal (false identification to law enforcement); financial (credit cards, telephone service, bank accounts, obtaining credit, etc); cloning (impersonation of someone else in order to conceal their own identity); medical (using another person's insurance for medical service or false claims); and child (using a minor's social security number).

The types of identity theft includes physical (dumpster diving; theft; mail theft; shoulder surfing; forgery; counterfeit checks; etc.) and electronic (IT equipment and storage media; public records; skimming data; malware; hacking; data breaches; phishing; etc.).

The identity thief is usually a friend or family member (23%) or could be through a data breach (17%); through the internet (13%); through access to a wallet/PDA/planner (11%); mail, break-in, or workplace (5% each); etc.

The Federal Trade Commission (FTC) is charged with coordinating efforts to combat identity theft. Identity theft was 21 % of the complaints received in 2009. Texas was 30th per capita in complaints and 3rd in complaints of identity theft. ID theft complaints were most common to 20-29 year olds followed closely by 30-39 year olds.

To help prevent identity theft use passwords; secure information in your home; use a shredder; control bills, invoices, and other records; don't give out personal information on the phone, in the mail, or on the internet; collect mail promptly and place a vacation hold when you are leaving for more than a few days; shred credit card applications, invoices, mail and call 1-800-OPTOUT to stop credit card offers. Do not carry in your wallet your SSN card, health insurance cards except when needed; and only needed credit/debit cards. Pick up new ordered checks at bank and do not include your driver's license number or SSN on your checks. Don't open unknown e-mail. Do not store personal data or financial data on your laptop unless necessary and do not use automatic logins. Use virus protection and firewalls. Dispose of hard drives properly (destroy).

continued in next column

If identity theft happens to you:

1. Place a fraud alert with one of the credit reporting companies TransUnion 800-680-729; Equifax 800-525-6285; or Experian 888-397-3742.
2. Review your credit report and look for companies you didn't contact; accounts you didn't open; debts on your account you can't explain; your SSN; your address; and your name and initials. If you find an error get it removed.
3. Close all affected accounts. After you have called notify banks and credit card companies in writing; send certified mail return receipt; request dispute forms; keep a copy of all correspondence; and keep all original documents.
4. File a police report. Police departments are required to take a report of identity theft. File a report with your local police; get a copy of the report; and make several copies.
5. File a complaint with the FTC online at www.ftc.gov/idtheft or by telephone at 877-438-7338.

The team closed their identity theft presentation by providing examples of addressing and correcting specific and more serious legal identity theft concerns.

Speaker Bio's

Jared Jordan is an Associate Director in Navigant's Disputes & Investigations practice. He is a Certified Fraud Examiner with over 12 years of experience providing financial, dispute resolution and investigative consulting services to attorneys, government agencies and corporate clients. Jared's experience includes conducting fraud and forensic accounting investigations, preparing and analyzing damage claims, examining and assessing corporate governance practices and internal controls, and evaluating complex data sets resulting from allegations of financial misrepresentation, fraud, breach of contract, director and officer misconduct, misuse of corporate funds and breach of fiduciary duty. His work has spanned multiple areas including the financial services, high-tech, energy, telecommunications, healthcare, manufacturing and homebuilding industries.

Todd Lester is a Managing Director in Navigant's Disputes & Investigations practice. He has over 23 years experience providing business, special investigative and forensic accounting consulting services including conducting assessments of operational performance, internal controls and other critical business processes in a wide variety of domestic and international forums. He has extensive experience advising clients in complex evaluations, investigations and disputes involving cost reconciliation and justification analyses, as well as complex databases and business systems. Prior to joining Navigant, Mr. Lester was in the Financial Advisory Services practice of PricewaterhouseCoopers.

The Spotlight's On You!

A special feature focusing on members of the Austin Area Chapter of ACFEs

Murray Harvel is a member of the Chapter

But maybe you didn't know...



Job Description:

I just started at the Texas Lottery Commission in October 2011 as a Senior Auditor specializing in information technology security and control as well as computer-related fraud.

What I'm working on now:

I'm learning how the Texas Lottery Commission operations and processes work, especially new computer systems just implemented (so as to be able to audit them in the new calendar year).

Best part of my job:

The Lottery's Internal Audit Division is a team that works together and supports each other, which makes for the best part of my job.

Ambition and/or Goals:

To retire from the State of Texas in five years or so and then go back into the private sector for a few years to earn enough money to *really* retire.

Years in audit field:

25 years, if you count audit consulting.

My first job:

Newspaper delivery (with over 200 papers it was the biggest bicycle route in Bay City, Texas).

Hobbies:

Improvisational comic acting (I'm a member of ComedySportz-Austin, was a performer in the ComedySportz-Houston troupe, and once even owned and managed the ComedySportz-San Antonio team).

Favorite Movie:

The King's Speech was my favorite this year.

Last books I read:

I re-read *Pale Blue Dot* by Carl Sagan (it's an excellent book); *The Wave* by Susan Casey

Favorite foods:

BBQ (ribs especially), Italian, and Mexican

Favorite Restaurants:

Iron Works, Art's Rib House, Romeos, Polvos

My pet(s):

Four cats – Zeus, Jupiter, Smokey, and Bandit

It's a good day when:

I can look back and see something accomplished

Pet Peeves:

Traffic at rush hour; people texting while driving

What I would do with a surprise afternoon off:

Sunny day – a walk around Lady Bird Lake;
Rainy day – watch a movie and/or take a nap.

I'm most proud of:

My eleven nieces and nephews that range in age from a 33 year old teacher to a newborn baby.

Most people probably don't realize:

While I have no problem performing in front of hundreds of people, I always place as an introvert on the Meyers-Briggs personality tests.