THE Witness Chair

Leading-edge Ideas for CPAs Providing Litigation and Dispute Resolution Services

FALL 2012 California Society of Certified Public Accountants ISSUE 58

Transforming Cyber Security

by Shane Sims

Targeted cyber threats are committed on organizations to steal data, disrupt services and maintain access for as long as possible, thus enabling future intrusions. These threats apply to all industries, not just those that deal with payment cards or personal information. Companies that have proprietary data or are involved with international business transactions are likely targets, as well as their external law firms.

Transnational criminal enterprises often maintain remote access to the target environment for six to 18 months before they are detected. Many cyber intrusions result in lingering unfettered access for many years—and some are never detected. Discovery of advanced cyber intrusions does not typically come from in-house technology, processes or people, but rather through third parties such as domestic law enforcement, intelligence sources, customers or business partners.

When foreign governments, organized crime or hackers target an organization, their techniques used to compromise the network and enable data theft are methodical. Advanced cyber threat groups are patient, tending to invest heavily in the research and development of custom malicious code and clever means to obtain data—all designed to slip past the cyber security radar.

Cyber threats are varied, complex and evolving. Preventive and defensive measures can reduce risks; however, the perpetrators are often keenly aware of the cyber security strategies employed over the past decade. Common cyber threat groups are:

- Foreign intelligence services (for military, political or economic advantage).
- Transnational criminal enterprises (for financial gain).
- Corrupt competitors (for economic advantage).
- Lone wolf (often insider) (for financial gain or to sabotage employer).

Intelligence services of foreign governments are the most sophisticated, organized and well-funded. Data shared among senior executives is often the most targeted.

The phrase "transnational criminal enterprises" was crafted in recent years to replace the traditional tag of "organized crime." While a decade ago, organized crime groups hired individual hackers, today's hackers have formed their own global networks and work independently.

Corrupt, but authorized, users of an IT system are the most dangerous threat. The solo artist, or lone wolf, is often one who has fallen on hard times or is motivated by revenge due to an unresolved work conflict, perceived or actual potential job loss, or work disenchantment. As such, the insider is ripe to be recruited by external threat groups.

Assume a Never-ending State of Compromise

Given the cyber threat landscape, organizations have to re-engage the human element to better leverage their investments in security technology. A cybercrime investigator's mindset is needed in daily cyber security operations. The future of cyber security will have to involve human sentinels leveraging technology and custom-developed processes and procedures to constantly investigate the IT environment.

A good interrogator in a fraud investigation will initially spend time building rapport to baseline the verbal and nonverbal behaviors of the human subject to detect deception. The investigator will also gather as much intelligence as possible about the subject. These same concepts can be applied to cyber security.

Creating a baseline of network traffic and system programs, processes and connections can assist the ongoing scrutiny of the IT environment for breach indicators or deviations from the norm. By using a baseline, it is possible to identify a large file being transmitted over an authorized networking protocol that is normally not used to transmit data. Or, a connection from a user system to an email server in which the user had no email account may also be identified.

Cyber Threat Intelligence

Many organizations are developing a cyber threat intelligence program and are looking to government agencies, for-profit vendors and free sources for intelligence feeds. Some industries have formed working groups in which cyber threat intelligence is openly shared, but not available to the public.

Government agencies have established vehicles for sharing cyber threat intelligence:

- Infragard was started in the late 1990s as a partnership between the FBI and private sector. It aims to share information by combining the knowledge base of the FBI, businesses, academic

continued on page 6

In this issue

Section Action

Business Valuation

by Denise M. Frey, CPA

Development of the cost of capital in the Capital Asset Pricing Model and Buildup Method requires estimates of the risk-free rate and equity risk premium (ERP). In the past many practioners have relied upon the published 20-year Treasury spot rate for the risk-free rate and the year-end ERP reported by Ibbotson. The instability of the risk-free rate during the past few years has us re-evaluating how we develop the cost of capital. We now normalize the risk-free rate when relying on the historical equity risk premium. We only use the spot risk-free rate if we have a contemporaneous estimate of the ERP.

For many years leading up to 2008, the 20-year Treasury bond rate, a proxy for the risk-free rate, was fairly stable. This changed in late 2008. For a number of months during each of the past four years the rate fell, at times by as much as 50 percent. Between 2004 and June 2012 the monthly rate averaged 4.4 percent. The monthly rate fell below 3 percent in late 2011 and has remained there through June 2012.

Many would argue that you couldn't invest at the normalized risk free rate. However, the objective is to estimate the overall cost of capital. The historic ERP, the return of large stocks in excess of the risk free rate, was calculated using historically higher risk-free rates.

To illustrate the problem, picture the Buildup Method as a single column of building blocks, the risk-free rate as the foundation, then the ERP, size premium and the company specific risk at the top of the column. Relying on the data reported in the Ibbotson Yearbooks as of Dec. 31, 2007 and 2011, the sum of the risk-free rate and supply side ERP results in 10.7 for 2007 and 8.62 for 2011. Does it make sense that the pre-crisis cost of capital would exceed the current? It doesn't to some valuation analysts.

Relying on a historical ERP and a spot risk-free rate may understate your estimated cost of capital in the current environment. Development of defensible cost of capital can be achieved in a number of ways. We feel normalization of the risk free rate is not only practical, but also transparent.

Denise M. Frey, CPA, ABV, CFF, CVA *is Business Valuation Section chair and is at Eckhoff Accountancy Corporation in San Rafael.*

Economic Damages

by Craig M. Enos, CPA

Discount rates and risk in economic damages calculations continue to be a hot topic for forensic accountants, especially how risk should be accounted for in the discount rate (capital markets approach) or in the cash flows (expected cash flows approach).

Two recent publications are a must read for forensic accountants involved in economic damages analysis: *Dunn on Damages*, Issue 7, Summer 2012 has three articles on the topic and the recent 2012 AICPA Practice Aid *Discount Rates, Risk, and Uncertainty in Economic Damages Calculations*.

Risk needs to be accounted for in your analysis. A cash flow analysis by a forensic accountant usually results in a cash flow stream that includes risk or a risk adjusted (risk-reduced) cash flow. A lower discount rate would be expected if using a risk adjusted cash flow stream. In theory, an expert who uses a risk adjusted cash flow approach (lower discount rate) would not be expected to calculate a damages amount significantly different than that of an expert who discounts a related cash flow that includes risk (higher discount rate).

The article in *Dunn on Damages* (available at *www.valuationproducts.com/dunn.html*), written by CalCPA Forensic Services Section members Brian Brinig and Jeffrey Kinrich, reviews discounting expected future economic losses and includes a table comparing the present value of an expected value cash flow with risk-adjusted discount rate to a risk-adjusted cash flow with risk-free discount rate. The table highlights the amount a risk-adjusted cash flow needs to be adjusted (decreased) when using a risk-free discount rate compared to an expected value cash flow with a risk-adjusted discount rate to arrive at the same present value.The difference may surprise you.

The AICPA Practice Aid, which includes contributions from FSS members Christian Tregillis, Greg Regan, Everett Harry and Jed Greene, also discusses a hybrid approach where a risk-adjusted discount rate may be used with the development of an expected cash flows analysis to account for risks not addressed in the cash flow projection.

Each analysis is unique to the facts of the specific case.

Craig M. Enos, CPA, ABV, CFF, CFE *is Economic Damages Section chair and owner of Enos Forensics in Folsom.*

Family Law

by Dan Close, CPA

Los Angeles Family Courts are reorganizing in response to a $161 million budget deficit. As a result, CPAs who practice family law in Los Angeles are being asked to provide creative options for streamlined and less expensive alternatives to the services they offer the courts.

The Los Angeles Superior Court Family Law Division has increased productivity by implementing a new master calendar system. The goal of the system is that cases will be brought to trial or resolution sooner with the parties better prepared for trial. This is particularly important because an increasing number of litigants are unrepresented and not necessarily knowledgeable about court procedures. This results in delays of hearings, more time spent by bench officers educating the litigants and less time trying cases.

Superior Court Judge Holly Fujie stated that Supervising Judge Scott Gordon and other family law bench officers in Los Angeles have implemented new procedures for matters deemed ready for trial. When the parties or the judge determine that a case is ready for trial, the parties and/or attorneys are sent to Department 2 for a trial date under the new master calendar system. According to Judge Fujie, trial dates may be set as early as one month after this conference.

However, under the new system, a process has been implemented for sending those matters to Mandatory Settlement Conferences, Trial Readiness Workshops or Judgment Workshops before trial so the parties have ample opportunities either to settle their issues or prepare for trial. Now, instead of numerous continuances for a variety of reasons, parties should

be prepared for trial and have exhausted settlement possibilities.

The new procedure includes dividing the Family Law Departments into "A" Departments, which will hold trials on Mondays and Tuesdays, and "B" Departments, which will try cases on Thursdays and Fridays. Judge Fujie noted that, in the past, trials were scheduled on a time available basis, so that trials were often held over a number of non-consecutive dates that could extend for months depending on the schedules of the courts, the parties involved, the attorneys or the experts. Now, matters will be tried day-to-day, within the Monday-Tuesday or Thursday-Friday schedule, until completed.

Also, the courts are going to be more strict on the timing of trials. They will expect CPAs to be more flexible with their time and to assist the court with creative options in which their services can be scaled back or expedited to fit budgets and assist the litigants and the court with these much needed forensic services.

The challenge to forensic CPAs will be educating and working with the judges, attorneys and the litigants regarding the necessary documents and information needed to comply with the new requirements. This should provide ample material for discussion and debate at our Family Law Section meetings.

M. Daniel Close, CPA, ABV, CFF, CVA *is Family Law Section chair and a shareholder of EDR Valuations, Inc. with offices in Solana Beach and Ontario.*

MessagefromtheChair

by Peter Salomon, CPA

California state courts need adequate funding to provide equal and timely justice for all. The California court system is home to more than 2,000 judicial officials and administrators that hear more than 10 million cases each year. Over the past several years funding cuts have led to fewer courtrooms and diminished court services that have had a drastic effect on Californians and those involved in providing legal services. In May, Gov. Jerry Brown cut the state's court budget by more than a $500 million. These budget cuts have required layoffs of court workers and judges, shutting down many courtrooms and cutting special court programs that deal with domestic violence, indigent defendants, education and people that have economic and cultural barriers getting into court.

The reduced funding will significantly slow down the resolution of criminal, civil and family court cases. The impacts to our court system will be many. Wealthy litigants may hire arbitrators and retired judges to resolve disputes in a timely manner outside of the court system. Judges will be forced to prioritize cases and encourage other cases to settle without a day in court. Lawyers will manage their cases differently because of delays in getting motions heard and getting timely trial dates. The delays in getting to trial will increase the cost of litigating to the parties, potentially resulting in prejudicial settlements. Many cases will simply take too long to get a day in court, also prejudicing one or both of the parties.

The Family Law column on Page 2 discusses how the Los Angeles Superior Court Family Law Division has asked for input from Family Law CPAs as part of its task to improve services with significantly less funding. We should all be mindful of the impacts to the people involved in the California court system due to the significantly reduced state funding and consider ways we can individually give back to that system.

— **Peter A. Salomon, CPA, CFF** *is a principal with Hemming Morse LLP in Los Angeles.*

Fraud

by Peter W. Brown, CPA

The SEC's whistleblower program went into effect July 21, 2010, following the passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act. The Office of the Whistleblower was created to manage the program and conduct investigations and it is now up and running.

Under the new whistleblower rules, the SEC is authorized by Congress to provide monetary awards to eligible individuals who come forward with high-quality "original information." Original information is the whistleblower's independent knowledge or is derived from the whistleblower's independent analysis. To receive an award, the information must lead to an enforcement action with a minimum of $1 million in sanctions being ordered. The range for awards will be between 10 percent and 30 percent of the amounts collected.

The SEC will consider a number of factors when determining the amounts of the awards. Factors that may increase the amount of the awards include:

- The amount of assistance provided by the whistleblower;
- Successful enforcement actions; and
- The extent to which the whistleblower participated in his or her company's internal compliance program.

Factors that may decrease the amount of the awards include:

- If the whistleblower was a participant in or culpable for the securities law violation being reported;
- Unreasonable delays in reporting the violation to the SEC; and
- If the whistleblower interfered with the company's internal compliance and reporting systems, such as making false statements to the compliance department.

On Aug. 21, the SEC awarded the first whistle-blower award—nearly $50,000, which represented 30 percent of the amount collected pursuant to an SEC enforcement action.

In a press release announcing the award, Robert Khuzami, director of the SEC's Division of Enforcement, stated, "Had this whistleblower not helped to uncover the full dimensions of the scheme, it is very likely that many more investors would have been victimized." SEC Chair Mary L. Schapiro also commented that "we're seeing high-quality tips that are saving our investigators substantial time and resources."

Peter W. Brown, CPA *is Fraud Section chair and a director with PricewaterhouseCoopers in Los Angeles.*

Keepin' It Legal

Alimony Payments to Nonresidents

by Philip D. W. Hodgen, Esq.

Alimony payments to nonresidents can be tricky. The tax rules are similar enough to purely domestic situations to encourage complacency—but there are withholding, paperwork and penalty risks for the complacent.

The general rules that make the IRS treat a payment as alimony will apply. Assuming these requirements are satisfied, let's look at a U.S. person paying alimony to a nonresident alien former spouse.

Who is a Nonresident Alien?

The different rules apply only if the alimony recipient is a nonresident alien. This means he or she is not a U.S. citizen, and also is not a U.S. resident for income tax purposes.

Citizenship is easy to ascertain. A person either is or is not a U.S. citizen. Holding additional citizenships will not change U.S. citizen status. Resident status is not as simple to determine. For income tax purposes, a resident is someone who holds a green card (regardless of where they live), or who spends a sufficient number of days in the United States every year. For more information on the rules, see IRS Publication 519, U.S. Tax Guide for Aliens.

For the purposes of this article, let us assume you have done the necessary due diligence and confirmed that the recipient is neither a citizen nor a resident of the United States for U.S. income tax purposes.

Normal vs. Different

When the alimony recipient is a U.S. citizen or resident, the rule is easy: Alimony received is included in the recipient's income and deducted from the payor's income.

Paperwork is minimal. The payor reports the payment amount and recipient's Social Security number on his or her tax return.

Penalties are minimal. There is a $50 penalty on either party for failure to comply with these reporting requirements, which may be abated. The IRS cannot deny a deduction for alimony payment as an additional penalty for noncompliance with the requirement that the payor provide the recipient's Social Security number.

Things are different when the recipient is a nonresident alien:

- The tax rate applied to the alimony income will be different;
- The paperwork requirements for both parties will be different; and
- Penalty opportunities exist for the payor.

General Tax Rules

A person who is neither a citizen nor a resident of the United States is generally subjected to U.S. income tax only on income derived from U.S. sources.

Once you have determined that you have U.S. source income, you have to know how it is taxed. A nonresident alien's U.S.-source income will be subject to U.S. tax in one of two ways:

- Just like a resident's income (income minus allowable deductions, then apply the graduated tax rates), or
- At a flat 30 percent of gross income.

Income tax treaties can override both of these tax methods.

How the Recipient is Taxed

The source of alimony income is the residence of the person who makes the payments. Thus, alimony received from a U.S.-resident spouse or ex-spouse will be U.S.-source income to the recipient.

U.S. income tax is imposed on U.S.-source alimony at a flat 30 percent of the gross amount paid to the nonresident recipient. The tax is withheld by the payor and remitted to the IRS. This is the default U.S. income tax treatment that a nonresident alien recipient of alimony from a U.S. spouse or ex-spouse should expect.

Claiming benefits under a relevant income tax treaty, though, can alter results.

The United States has many income treaties with different countries. Some provide that alimony is taxable only in the recipient's home country. If there is an income tax treaty between the United States and recipient's home country, check to see whether it exempts U.S.-source alimony from U.S. tax. The treaties vary wildly, from ignoring the topic entirely to granting the payor's country of residence the exclusive right to tax alimony.

The alimony recipient's U.S. income tax liability will either be the rate mandated by the treaty (i.e., zero), or it will be 30 percent.

The Recipient's Paperwork

Having decided that the recipient will pay U.S. income tax on alimony received at either 30 percent or the treaty rate of 0 percent, the next thing to do is deal with the paperwork.

The payor needs to know two things: The recipient's nonresident alien status and the appropriate tax withholding rate to apply to the alimony payments. The recipient satisfies both needs with Form W-8BEN. Part I certifies the recipient is a nonresident alien. If applicable, the right to claim treaty benefits is provided in Part II. Form W-8BEN is given to the payor. It is not given to the IRS.

A U.S. tax return may or may not be required. If one is required, the nonresident alien alimony recipient will file Form 1040-NR. Assuming there is no other reason to file a U.S. income tax return other than to report the alimony, the filing requirements are:

- The required withholding was 30 percent, and it was fully satisfied by tax withheld. No U.S. income tax return is required to be filed by the recipient.
- The required withholding was 0 percent due to a claim of benefits under an income tax treaty. File Form 1040-NR, and attach Form 8833 to prove that the recipient is entitled to treaty benefits.
- The required withholding rate was 30 percent but the payor did not withhold enough tax to satisfy the tax liability. File Form 1040-NR and pay the extra tax liability that is due.
- The required withholding rate was 0 percent or 30 percent, and too much tax was withheld from the alimony payments. File Form 1040-NR to claim the appropriate refund. File Form 8833 if you are making the election under an income tax treaty to exempt the alimony received from U.S. income taxation.

How the Payor is Taxed

The payor's tax liability position is

continued on page 5

AICPA Alert

by Annette M. Stalker, CPA

The AICPA Forensic & Litigation Services (FLS) Committee has recently produced several resources, with more on the horizon.

New Practice Aids

- "Discount Rates, Risk and Uncertainty in Economic Damages Calculations" from the FLS Damages Task Force.
- "Mergers and Acquisitions Disputes" was an effort by the FLS Mergers & Acquisitions Task Force.
- In addition, the practice aid "Calculating Intellectual Property Infringement Damages" has been revised and updated, and is in final stages of the publication process.

New White Papers

- "How to Organize a Forensic Accounting Investigation" from the FLS Fraud Task Force.
- "Computer Forensic Services and the CPA Practitioner" from the FLS Forensic Technology Task Force.

Civil Justice Revolution

The IAALS project, a potential catalyst of civil justice reform, is well underway as originally reported by Greg Regan in the Summer/Fall 2011 issue of *The Witness Chair*. IAALS (*www.iaals.du.edu*) has developed a number of initiatives through collaboration with broad-based groups, including AICPA's Forensic and Valuation Services Executive Committee.

In 2011, the FVSEC formed the Civil Litigation Task Force (CLTF), chaired by Ron Durkin. The charge for CLTF is to work with IAALS to develop recommendations to maximize the effectiveness and efficiency of financial experts in the civil pretrial process.

The CLTF, with the support and collaboration of IAALS, designed and conducted a survey of AICPA FVS members. The results are reflected in "Another Voice: Financial Experts on Reducing Client Costs in Civil Litigation," available at the AICPA website, and includes key recommendations to stakeholders in the civil justice system. These recommendations, as implemented, may have a profound impact on the valuation and forensic accounting work performed by many of our Forensic Services Section members.

Annette M. Stalker, CPA, CFF, CITP, CFE *is a principal at Ueltzen & Company LLP in Sacramento.*

---

continued from page 4

unchanged. The payor may deduct alimony payments from income, even if the alimony is tax-free to the recipient. As usual, this is accomplished at Form 1040, Line 31.

The Payor's Paperwork

A U.S. person making alimony payments to a nonresident alien recipient is a withholding agent. The payor reports the amount of payments made, and withholds and remits the correct amount of tax. Filing or payment failures will cost the payor dearly, with the usual late payment or late filing penalties. Worse yet: A withholding agent is personally responsible for any withholding errors. If tax should have been withheld but was not, the IRS will look to the payor for satisfaction.

A withholding agent protection is paperwork from the recipient. If the recipient provides documentation that the payor does not know or suspect it to be false, there is no personal liability for withholding errors.

Form W-8BEN protects the withholding agent: the payor of alimony. Part I confirms the recipient's nonresident alien status. If Part II is completed, the payor can rely on it to eliminate tax withholding on the alimony. Otherwise, the payor should withhold 30 percent of the alimony payments.

The payor tells the IRS about the alimony payments made (and the withholding, if any) on Forms 1042 and 1042-S. These are the international remittance equivalents to Form 1099. These forms are filed even if no tax is withheld. If tax is withheld, taxes need to be remitted monthly, quarterly, or annually, depending on the amount. See the Instructions to Form 1042 to determine when you must deposit the withheld taxes.

Conclusion

Alimony payments to a nonresident alien spouse or ex-spouse requires extra care in set up and tax compliance. In addition to the normal documentation required to make the payment qualify as alimony, the "after the fact" tax and paperwork burdens need to be considered in setting the amount of alimony. Once the alimony amount has been set, the payor would be well-advised to have the withholding obligations handled professionally to avoid penalties.

Philip D. W. Hodgen, JD, LL.M *is the managing partner of HodgenLaw PC in Pasadena, which advises clients on matters of international tax exclusively. He is a frequent lecturer on international tax topics for the California Society of CPAs and other groups.*

New Fraud CPE Rules

CalCPA's Forensic Services Section proposed to the California Board of Accountancy changes related to fraud continuing education and what type of CE qualifies for fraud education.

The changes include inserting the word "prevention" and changing the word "in" to "affecting" in the regulations to read:

(e) A licensee who must complete continuing education pursuant to subsections (c) and/or (d) of this section shall also complete an additional eight hours of continuing education specifically related to the *prevention*, detection and/or reporting of fraud *in affecting* the financial statements. This continuing education shall be part of the 80 hours of continuing education required by subsection (a), but shall not be part of the continuing education required by subsections (c) or (d).

The recommendations were accepted by the CBA and should become effective at the start of 2013.

HAPPENINGS

FORENSIC SERVICES SECTION MEETINGS

Business Valuation	Thursday, Feb. 21, LAX
Economic Damages	Wednesday, Feb. 20, LAX
Family Law	Friday, Feb. 22, LAX
Fraud	Wednesday, Feb. 20, LAX

An individual meeting notice will be sent and you may register online at *www.calcpa.org*. For more information, call (818) 546-3502.

continued from page 1

institutions, state and local law enforcement agencies and others who are committed to sharing information and intelligence to prevent hostile acts against the United States.

- The USA PATRIOT Act of 2001 mandated the United States Secret Service (USSS) to create the Electronic Crimes Task Forces. These task forces are comprised of the USSS, businesses, academic institutions, state and local law enforcement agencies, and others focused on electronic crimes against financial institutions.
- The Department of Homeland Security formed the United States Computer Emergency Readiness Team in 2003. The team's mission includes the sharing of cyber security information with state and local governments, industry, researchers and the public.

It is also important to consider the most significant source of cyber threat intelligence: Your own IT environment, which can be transformed into a treasure trove of threat intelligence. Vast, rich and extensive cyber intelligence can be found from the best source of all—the company's private cyber space. Companies should collect data and monitor network traffic at every Internet access point to enhance detection and incident response efforts. Resources that understand the methods used by the cyber threat landscape should configure real-time network traffic monitoring technology. In addition to monitoring traffic to and from the Internet, consideration should also be given to monitoring critical internal data storage locations.

Organizations need a systematic and scheduled method for gathering live memory from internal systems to identify suspicious programs and associated behavior. Non-public custom malware will not have a signature that can be identified by signature-based detection and prevention technologies. This is an emerging and necessary capability, and, for the time being, live memory just may be the last stand on the cyber battlefield.

For any malware specimen discovered in private cyber space, there is a serious need to fully understand its capabilities and use that intelligence to further investigate the environment for breach indicators and to enhance security controls. The standard approach of letting software remove the malware and then let IT rebuild infected systems creates more cyber security blind spots. The availability of an internal capability or outside partner to analyze malware can reinforce a cyber security posture.

Analyzing logs from monitoring is an important element of cyber forensic investigations. However, these logs may not be properly maintained and often lack sufficient useful information. These technologies should be configured to log activity that is useful to detection and incident response; logs should never be overwritten, and they should be a part of the data backup program.

Some organizations are using technology to gather logs in a central location for more effective analysis. However, the technologies are often not configured to capture the right suspicious activity, the log aggregator is often not configured properly to provide alerts on suspicious activity, or the alerts are misinterpreted by inexperienced staff. Logs have to be aggregated in a way that permits a security analyst who understands the cyber threat landscape to continually analyze the logs with innovative methods to find the breach indicators.

An organization can implement enhanced cyber monitoring of insiders who have sensitive job responsibilities or access to sensitive data for unauthorized behavior to better prevent or detect data theft or leakage. Managing the insider threat to information means organizations must continually know which insiders are at risk, what information they have access to and increase both host- and network-based monitoring of those specific insiders. This is a critical intelligence gathering exercise that cannot be overlooked.

In the future, cyber security will have to integrate all of these intelligence sources in a state of perpetual analysis to enhance and safeguard operations. Cyber threat intelligence is a key component to transforming detection and incident response activities.

Shane Sims *is a director in the Advisory-Forensics practice at PricewaterhouseCoopers in the Washington, D.C. Metro area.*

The Witness Chair is published three times a year by the Forensic Services Section of the California Society of Certified Public Accountants.

Editor
Susan Bleecker

Associate Editors
Leslie O. Dawson
Maria N. Nazario

Section Chair
Peter A. Salomon

Individual Section Chairs

Business Valuation	Denise M. Frey
Economic Damages	Craig M. Enos
Family Law	M. Daniel Close
Fraud	Peter Brown

Nonmember subscription rate is $75 for one year. To subscribe, call CalCPA at (818) 546-3502 or (800) 922-5272.

We welcome your letters, articles, comments and suggestions, which may be sent to the editors at *bleeck@pacbell.net*.

The Witness Chair does not provide legal advice. The material published, unless otherwise specified, represents the views of the authors and the individuals quoted and not those of CalCPA or the AICPA.

www.calcpa.org/FSS