



Investigations Council

August 2011

Investigations Council Members

Steve Wager, CPP
Chairman

Peter Psarouthakis
Vice Chair

Pawanjit Ahuwalia

Marty Bishop, CPP

Darrell Chaneyfield, CPP

Jack Chu

Paul Dank, PCI

Nuno Miguel Guita

Barry K. Horvick

Michael Krausz, CPP

Rashid Ali Malik

Charlie Meade, CPP

Reginald J. Montgomery, CPP, CFE, PSP

Joseph J. Nieciecki

Harm Osteen, CPP

Tim Reddick, CPP, CFE, PCI

Frank Schurgers, CPP

Vincent Sheridan, CPP, CFE

Jim Whitaker, CPP, CFE, PCI

Jeff Williams, CPP

Chairman's Comments

I am pleased to report that we have added three new members to the Investigations Council since the beginning of the year. We now have 20 members in the Council. Of these 20 members, already 12 members have committed to attending the Annual Seminar in Orlando. Four Council members will be giving presentations at the Seminar and four others will be serving as moderators

We continue to recruit new members and work on maintaining our international representation. Council membership is now the highest it has been in years.

Some of the Council members are working on a webinar and others are working on developing a topic for an article in *Security Management*.

I would like to thank each Council member for their support and efforts during 2011 and hope you all can contribute more to the Council and ASIS before the end of the year. I also look forward to meeting with those members who are attending the Annual Seminar. Finally, I would like to congratulate Tim Reddick for being selected for the Certified Fraud Examiner of the Year award by the Certified Fraud Examiner Association.

Dodd-Frank Whistleblower Provisions and their Impact on Foreign Corrupt Practices Act (FCPA) Enforcement

According to Anton R. Valukas, a former US Attorney, appointed in 2009 as the Examiner for the Lehman Brothers Holdings bankruptcy, the onset of an economic recession, "brings with it a wave of white collar prosecutions and calls for tighter regulation."

In an effort to address the causes of the 2008 economic crisis, the federal government has taken action to prevent a repeat of the financial crisis that toppled Lehman Brothers Holdings Inc. The Dodd-Frank Wall Street Reform and Consumer Protection Act,

passed in July 2010, empowers regulators to guard against systemic risk and dismantle failing firms, said Sheila Bair, Chairman of the Federal Deposit Insurance Corporation.

The Dodd-Frank law also includes whistleblower provisions which have significant implications on FCPA Enforcement. Section 922 (SEC) and 748 (CFTC) include large rewards for employee whistleblowers. Some basic components of the provision include:

- The Commission shall pay awards to eligible whistleblowers who *voluntarily* provide the SEC or the CFTC with *original* information that leads to a *successful* enforcement action yielding monetary sanctions of over \$1 million. The award amount is required to be between 10 to 30 percent of the total monetary sanctions collected based on SEC/CFTC discretion.
- The Dodd-Frank Act also expressly prohibits retaliation by employers against whistleblowers and provides them with a private cause of action in Federal Court in the event that they are discharged or discriminated against by their employers in violation of the Act. It also provides remedies which include reinstatement, double back pay (SEC) or single back pay (CFTC) and payment of litigation costs.

The obvious concern regarding the whistleblower provisions are that they create perverse incentives for employees to bypass an employer's internal reporting mechanisms and go straight to the SEC or CFTC with information regarding potential securities violations, undermining the employers' ability to resolve complaints internally, and potentially generating frivolous complaints. The SEC and CFTC will issue final regulations by April 17, 2011 which are anticipated to address these concerns.

Proposed regulations by the SEC include providing employees a 90-day window during which the employee can report the original information internally (giving the employer time to resolve the complaint and the employee can preserve their status as an eligible whistleblower) and paying a higher percentage reward to those who do. The CFTC proposed rules are similar but do not pay a higher reward for reporting internally first.

The SEC previously forecasted they would receive 30,000 tips this year as a result of the new whistleblower provisions. In actuality, a FOIA request from the New York Post to the SEC indicated that the SEC had only received 168 complaints alleging corporate fraud between July 22, 2010 (when the Act was passed) and February 2, 2011, a rate of less than one complaint per day.

Lori Galvin
Member of ASIS Investigations Council

Recent Break-ins Emphasize the Need for Increased Security

The recent break-ins at Sony, Sega, the IWF, stolen CO2-Certificates have shown that companies must heed the call for better information security practices either based on international standards such as ISO27001, as well as a generic one applying to any information security management system or more specific ones such as PCI that apply to payment-processing environments. A company is certainly free to choose from any of the best practices available, but the following elements are key activities in order not to become victimized:

- **Asset and risk analysis:** It needs to be clear which assets require which level of protection and are exposed to which kinds of threat. Among these the most important assets are those that are directly required for revenue generation, but also systems that are of lesser obvious importance may contribute to severe damage, if penetrated and serving as an attack entry point.
- **Software security:** Nowadays, all web facing software needs to be programmed securely following software coding best practices, such as the checking of variables and their content in web interaction so not to allow SQL injection attacks,

which are the most frequent to be used for stealing data from companies through web sites.

Software that is rolled out to production systems must undergo security testing to ensure that no critical issues remain present in the software. It might be a challenge to delay the roll-out of a piece of software due to severe security bugs being found, but it is certainly better to delay a roll-out than to let insecure software become operational.

The OWASP model has proven its worth when it comes to checking software for security elements.

- Change management and change reconciliation of software: IT environments change in respect to the hardware used, operating system used as well as software used. All changes to software should undergo ITIL change management to ensure that only changes that have been planned, evaluated for their impact, risk assessed, and tested are rolled out. Using reconciliation tools it can be established if software (libraries, programs, etc.) that are found on a system can be traced back to a defined change and should therefore be present on a system or not. If not, an incident might be raised so that a potential penetration is detected and evaluated early on.
- Continuous audit: It is of paramount importance that all critical IT systems are routinely or even continuously scanned for weaknesses and vulnerabilities so that these can be remedied speedily. IT environments may change frequently and the audit activities undertaken need to take place as frequently as the environment changes. This may result in continuous audit for operating system weaknesses of servers, clients and network devices; “continuous” referring to daily scans even.

Michael Krausz, CPP
Member of Investigations Council

Legislative Update

Senate Security Breach Bill Introduced:

On July 28, Senators Tom Carper (D-DE.) and Roy Blunt (R-MO) reintroduced S. 1434, the Data Security Act of 2011, to protect consumers and businesses from identity theft and account fraud. The bill would require entities such as financial establishments, retailers, and federal agencies to safeguard sensitive information, investigate security breaches and notify consumers when there is a substantial risk of identity theft or account fraud. The requirements would apply to retailers who take credit card information, data brokers who compile private information, and government agencies that possess nonpublic personal information.

The bill’s sponsors state their proposed bill “better protects consumers by replacing the current patchwork of state laws and establishing one set of national requirements. Presently, 49 states and U.S. territories have enacted laws governing data security and data breach notification standards.”

Senator Carper reiterated an ever increasing theme in the media: “While we have reaped enormous benefits from this powerful technology and innovation, millions of Americans are at risk for identity theft because of the vulnerability surrounding sensitive personal information. It seems nearly every other day there is a report of American consumers’ highly sensitive personal information being compromised by a store, a school or some third party data center.”

“At the very least, identity fraud can cause worry and confusion, and at the very most it can cause serious financial harm,” continued Sen. Carper. “We need to replace the current patchwork of state and federal regulations for identity theft with a national law that provides uniform protections across the country. This comprehensive approach will better serve consumers by making it easier for businesses and government agencies to take the steps necessary to adequately protect all Americans from identity theft and account fraud.” Although some state laws are similar, many have inconsistent and conflicting standards, forcing businesses to comply with multiple regulations, and leaving many consumers without proper recourse and protections.

“New technologies have greatly expanded the ways we access information and conduct day-to-day business, but these new tools also pose new security challenges that we must address as a nation,” said Senator Blunt. “This bill will help ensure that businesses and government agencies have consistent national standards across the board as we work to protect consumers’ personal information and prevent identity theft.”

If the financial establishment, retailer, federal agency or other entity determines that sensitive information was compromised or may have been compromised, the proposed bill the entity to investigate the scope of the breach, the types of information compromised or potentially compromised, and determine whether the information will likely be used to cause an individual harm or bank fraud. If the event will cause harm, then the entity must notify the appropriate federal government regulatory agency, law enforcement, and national consumer reporting agencies where the breach affects over 5,000 consumers and all consumers affected by the breach.

The Data Security Act of 2011 is modeled after the data security and breach-response regime established under the Gramm-Leach-Bliley Act of 1999 and subsequent regulations. It builds on existing law to better ensure federal and state regulators comply with the law and to make sure that data security procedures are uniformly applied. Regulators of entities who do not comply would have the authority to levy finds, require corrective measures or even bar individuals from working in their respective industries.

Peter Psarouthakis
Investigation Council-Legislative Committee

Investigations Council Mission

Promotes ethical and thorough investigations by private, corporate, and government investigators by providing analyses of emerging investigative technology, techniques and trends in the global investigative arena.

Interested In Joining the Investigations Council?

The Investigations Council seeks qualified ASIS members with a professional investigative background to expand its membership to a full complement of twenty-five professional investigators. If you would like information about the Investigations Council or if you would like to be considered for membership on the Investigations Council as vacancies occur, please contact Membership Committee Co-Chairmen Harm Osteen, CPP at harm.oosten@contego.nl or Vincent Sheridan, CPP, CFE at vince@adventinvest.com.

We are a working Council and all members are expected to remain actively engaged to maintain membership.



1625 Prince Street
Alexandria, VA 22314-2818
USA
703-518-1447
Fax: 703-518-1517
Email: councils@asisonline.org