



Investigations Council

February 2010

Investigations Council Members

Steve Wager, CPP
Chairman

Peter Psarouthakis
Vice Chair

Pawanjit Ahuwalla

Marty Bishop, CPP

Darrell Chaneyfield, CPP

Jack Chu

Nuno Miguel Guita

Michael Krausz, CPP

Rashid Ali Malik

Charlie Meade, CPP

Harm Osteen, CPP

Tim Reddick, CPP, CFE, PCI

Vincent Sheridan, CPP, CFE

Jim Whitaker, CPP, CFE, PCI

Jeff Williams, CPP

Mike Osborne CPP
Council Vice President

Chairman's Comments

I am grateful for the opportunity to serve as the Chairman of the Investigations Council, and I am indebted to Marty Bishop, the previous Chairman, for all the support he has given me while I served as Vice Chairman and in our recent leadership transition. I would also like to welcome Peter Psarouthakis to the important role as the Vice Chair.

The Investigations Council's priority is to provide you with relevant information that can help in coping with investigations and timely legislative insight as it pertains to this field.

I believe that we are fortunate to have a distinct international flavor in the Investigations Council, with members from eight different countries including the United States. One of the Council's goals this year is to provide the ASIS membership with views on investigations as they are seen and worked on in other countries across the globe. We will also try to focus on international best practices as they are implemented both inside and outside of the United States.

In the past, the Investigations Council has been a relatively small Council, but the present Council members will be concentrating on increasing the current membership to at least 25 members prior to the end of the year. Certainly, if any reader is interested in joining the Investigations Council, we would encourage that person to contact the Council for additional information, along with an application.

I would like to thank each Council member beforehand for the support and commitment they will provide to the Council in 2010.

Information Security Breaches

These days, dealing with information security breaches has moved from an emergency activity invoked every now and then to something you need to have standing operating procedures for. With the latest developments in Switzerland, where dealing with bank data belonging to those who have evaded paying taxes in their home countries has become a new branch of business, it is ever more important that

companies seriously consider the risks associated with breaches of the confidentiality, integrity or availability of company proprietary information. Apart from the public embarrassment, if a breach is high-profile enough, material and immaterial damages can easily reach the six- or seven- figure range. Based on a 10-year evaluation of my own case files (containing more than 100 cases), the following picture has emerged:

- For companies relying on the Internet for generating their revenue, about 60% of all breaches are committed by outsiders, 20% by insiders with 10% being accidental. These companies need to protect against hackers and crackers and need to make sure their source code is tested extensively, if companies use source codes of their own making for Web applications.
- Companies that do not need the Internet to generate revenue are usually defrauded by their own staff (in more than 80% of the cases) with outsiders only contributing to 5% of incidents. About 15% of breaches proved to be accidental.
- Organizations such as public offices (ministries, federal agencies) are mainly hit by accidental or intentional breaches committed by their third party suppliers. In these cases, disks that should be shredded end up for auction on eBay.
- Companies handling critical infrastructure or operating in the defense sector need to cover all aspects of information security with the same vigor: from IT access control to physical access control and eavesdropping protection at the very minimum.
- Companies with a strong focus on research need to be aware of their risk environment, independent of their size. The smallest company affected on file was a 15-person company who provided critical know-how for the Hubble Space Telescope. That company had to confront several incidents of attempted spying aimed at procuring sensitive information.
- In at least five traumatically severe cases, call centers were suspected to be the original location of the leaks.

All this suggests the need for detailed legal regulations, stiff contractual penalties and a strict audit regimen on behalf of the corporate customers using the call center. It also calls for a good data leakage prevention (DLP) solution. The good news is that many of these products have reached market maturity by now.

Michael Krausz
Member of ASIS Investigations Council

Legislative Update

The Changing Climate. This past January's special election of Massachusetts Senator Scott Brown has cost the Democrats their important 60th vote. The potential climate change blowing from the election to fill the vacancy of the late Senator Ted Kennedy bodes well for investigative and security professionals in Washington on a number of bills which are of concern to professional investigators.

Contract security companies and large corporate clients of professional investigators are concerned with HR 1409/S560, the Employee Free Choice Act of 2009. Republicans, who are opposed to this bill, now have the 41st vote which allows them to filibuster bills in the Senate. Passage of EFCA would allow labor unions to organize via the use of "card check", thus denying employees the right to a secret ballot. The bill also mandates an arbitration scheme thought to be more favorable to unions.

There has been some concern over HR 4173, the Wall Street Reform and Consumer Protection Act of 2009, calling for the creation of a Consumer Financial Services Protection Agency. This provision is being challenged by the financial services industry, and the election of Senator Brown will impact the chances of creating such an agency in the Senate Banking Committee's bill. The proposed Senate bill, if passed, will be yet another "legacy bill" of Committee Chairman Senator Chris Dodd, Democrat of Connecticut who has opted not to run for re-election this fall. Professional investigator trade associations have been, and will continue, to maintain their positive rapport, developed over years of meeting with the Federal Trade Commission, which has jurisdiction over specific aspects regulating segments of the investigative profession and at the same time will continue to develop its rapport with the Department of Justice, Treasury Department, Homeland Security and other agencies which might be tasked with regulating aspects of the investigative and security industry.

Of continued importance to professional investigators this year is "access to information" legislation. As you all are aware, our profession has been battling against legislation for years now that would curtail our access to information that is critical for us to do our jobs (SSNs, DOB, Court records...). Several bills were once again introduced that could be potentially harmful if not monitored closely.

Below are some bills being monitored closely by the investigative profession during this congressional session:

- H.R. 122: Protecting the Privacy of Social Security Numbers Act of 2009 (Sponsor Rep. Rodney Frelinghuysen R-NJ)
- S. 141: Protecting the Privacy of Social Security Numbers Act (Sponsor Sen. Dianne Feinstein D-CA)
- S. 1618: Safeguarding Social Security Numbers Act of 2009 (Sponsor Sen. Charles Schumer D-NY)
- H.R. 3306: Social Security Number Privacy and Identity Theft Prevention Act of 2009 (Sponsor John Tanner D-TN)

- H.R. 3126: Consumer Financial Protection Agency Act of 2009 (Sponsor Barney Frank D-MA)
- H.R. 4173: Wall Street Reform and Consumer Protection Act of 2009 (Sponsor Barney Frank D-MA)

For more detailed information on these bills and other legislative information related to professional investigators and security professions, go to the following two websites:

www.ispla.org

www.govtrack.org

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 fifteen 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 Oosten, 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