Leadership

Dan Botsch, President

As President and one of the founders of the company, Mr. Botsch oversees all aspects of the organization.

Prior to joining TrapWire, Dan served 11 years as an Intelligence Officer with the Central Intelligence Agency, focusing on Russian and Eastern European affairs. He also has experience in corporate security, having served as the Deputy Director of a Business Intelligence Group that monitored political, economic, security and market dynamics for a Global 100 energy company. Dan holds an MBA from the University of Chicago's Graduate School of Business; a Masters degree in International Affairs from Boston University; and a Bachelor's degree in Mathematics and Political Science from Bates College.

Michael Maness, Director of Business Development

As Senior Director, Mr. Maness is currently responsible for the Business Development activities of TrapWire. During the formation of the company he made important contributions to the development of the TrapWire Critical Infrastructure system rules engine and its unique, structured reporting formats. Additionally, he contributed to the design and development of some of our training programs, and provides counterterrorism and surveillance expertise in support of TrapWire system deployments.

Mike joined TrapWire following 20 years of service with the Central Intelligence Agency, where he directed counterterrorism and security operations in the Middle-East, the Balkans and Europe. As a senior operations officer and field operations manager, he was instrumental in combating Al-Qaeda's operational units in the immediate wake of the September 11 terrorist attacks. He has also been recognized by the CIA for his work in Bosnia and Kosovo during the crises there. Fluent in several languages, Mike is a graduate of Texas State University where he was awarded degrees in International Relations and Foreign Languages.

Michael K. Chang, Director of Operations
As Director of Operations, Mr. Chang is responsible for all TrapWire training programs and TrapWire system deployments. Prior to joining TrapWire in 2005, Mike served 12 years with the Central Intelligence Agency as a counterterrorism operations officer and security officer. He designed and implemented numerous, multifaceted counterterrorism operations and training programs and worked closely with various military, intelligence, and law enforcement agencies across the globe.

He also served as an Assistant Team Leader and Special Agent on the personal security detail of the Director and Deputy Director of Central Intelligence. Mike has served as a senior instructor for various field training programs, including Counterterrorism Operations, Protective Operations, and Surveillance Detection. He is also a CIA certified firearms and weapons instructor. He has an M.A. in Forensic Science from George Washington University and a B.S. in Administration of Justice from Pennsylvania State University.

Paul Chadha, Director of Information Technology

As Director of Information Technology, Mr. Chadha manages TrapWire's corporate-wide technology infrastructure, including the operation and maintenance of TrapWire Data Centers worldwide. Paul is responsible for ensuring information security and high system availability to meet the demanding requirements of our government and private sector clients. Paul is also responsible for managing the software development of the TrapWire suite of products, ongoing Client Support Services, and technical integration efforts for TrapWire system deployments.

Paul has more than a decade of experience in the Information Technology arena and has led numerous efforts to overhaul corporate networks in need of tighter security and added reliability. Paul currently holds the Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and EC-Council Certified Security Analyst (ECSA) certifications.
SAFE HARBOR PRIVACY POLICY

Scope
This Policy outlines our general policy and practices regarding personal information entered into our United States based systems by European Economic Area (“EEA”) subscribing customers, and personal information entered into our EEA based systems which may be accessed from the United States.

Definitions
For purposes of this Policy, the following definitions apply:

“TrapWire” means TrapWire Inc., a Reston, VA based company in the United States.

“Personal Information” means any information or set of information (such as name, address, date of birth, social security number, etc.) that may be used to identify an individual. Personal information does not include information that is encoded or anonymized, or publically available information that has not been combined with non-public information.

“Sensitive Personal Information” means personal information that confirms race, ethnic origin, political opinions, religious or philosophical beliefs, or trade union memberships, or that concerns health or sex life.

TrapWire complies with the U.S.-EU Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries. TrapWire has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. To learn more about the Safe Harbor program, and to view TrapWire’s certification, please visit http://www.export.gov/safeharbor/.

Notice
TrapWire is a risk mitigation technology and services company that designs, builds and markets software products intended to prevent terrorist and other criminal attacks directed against critical infrastructure, key assets and personnel. Our flagship product, the TrapWire software system, has been designed to provide a simple yet powerful means of collecting and recording suspicious activity reports. Once a suspicious activity is entered into the system it is analyzed and compared with data entered from other areas within a network for the purpose of identifying patterns of behavior that are indicative of pre-attack planning. Generally, no Personal Information or Sensitive Personal Information is recorded by the TrapWire system, and no such information is used by the system to perform its various functions. In the event a system user were to enter either Personal Information or Sensitive Personal Information in a comments field, TrapWire will not share or expose that information to any other subscriber on the system, unless required by law, and, in any case, will otherwise adhere to Safe Harbor Privacy Principles with respect to that information.

Choice
Since TrapWire systems, in general, do not capture or store Personal or Sensitive Personal Information, there will be very few (if any) opportunities to offer opt-in or opt-out choices to individuals. On the rare occasion where such information is entered into the system, it is likely to be recorded as law enforcement sensitive and will not be shared outside the law enforcement community. To the extent Personal or Sensitive Personal Information is entered into the TrapWire system, and is not designated as law enforcement sensitive, TrapWire will not share that information with any third party.

Transfer To Third Parties
The TrapWire system is designed to share only suspicious activity data which does not include any Personal or Sensitive Personal Information. In the event Personal or Sensitive Personal Information is
recorded by a system user, that information will not be shared or transferred to other than law enforcement or other authorized agencies as required by law.

**Security**
The data center housing the TrapWire infrastructure was constructed to the highest level of physical security standards. Access to the facility is controlled and logged through a system of biometric hand geometry readers, and the facility is carefully monitored by security officials on guard 24 hours per day, 7 days per week, 365 a year.

System Security is also of critical importance and is designed into all levels of the TrapWire application and infrastructure. All connections to the TrapWire application are made through a 256-bit encrypted SSL connection which terminates in a network DMZ. User authentication is performed from the DMZ and must be successful before a connection to TrapWire is permitted. Implemented security processes are intended to protect any information in the TrapWire system from loss, misuse, unauthorized access, disclosure, alteration or destruction.

**Data Integrity**
TrapWire, by design and intent, attempts to avoid the collection of Personal or Sensitive Personal Information by the products it produces. However, when such information is entered into a TrapWire system, reasonable steps are taken to assure that information is relevant for the purposes for which it is to be used. We do, however, depend on our users to update and correct any information they enter.

**Enforcement**
TrapWire has established procedures for periodically verifying the implementation of and compliance with the Safe Harbor principles. We conduct an annual self-assessment of our practices with respect to Personal and Sensitive Personal Information to verify that representations we make about our privacy practices are true and that related privacy policies have been implemented as represented.

Individuals may file a complaint with our Privacy Office at the address below. TrapWire will investigate and attempt to resolve complaints and disputes in accordance with the principles contained in this Policy. If a dispute cannot be resolved by this process we will participate in the dispute resolution procedures of the panel established by the European Data Protection Authorities.

**Limitations**
Adherence by TrapWire to these Safe Harbor Principles may be limited (a) to the extent required to respond to a legal or ethical obligation; and (b) to the extent expressly permitted by an applicable law, rule or regulation.

**Contact Information**
Please direct any questions or comments regarding this Policy to our corporate office:

TrapWire Inc.
1875 Campus Commons Drive – Suite 301
Reston, VA 20191
Attn: Legal Department/Safe Harbor

**Amendments**
This policy may be amended from time to time to remain consistent with the requirements of the Safe Harbor Principles. A notice will be posted on our website (www.trapwire.com) for 60 days whenever this Safe Harbor Policy is changed in any material way.

**Effective Date**
6 June 2012