TECHNO-CRIME INSTITUTE

Walt Manning

Investigations Futurist

Keynotes and unique training programs related to:

- Technology crime
- Investigations
- Law enforcement
- Fraud
- Security

21-year veteran of the Dallas Police Department
Founder, Techno-Crime Institute
Founder, Investigations MD
Certified Fraud Examiner
Member of International Faculty, Association of Certified Fraud Examiners
Founding member, Digital Forensics Certification Board

WALT MANNING

Walt.Manning@Technocrime.com
972.768.4134
Twitter@WaltManning1

Speaking Topics

The Technology Explosion and the Future of Crime

A self-driving car is being packed with explosives and programmed to be a remote-controlled bomb (no suicide bomber needed). Someone is using a drone to stalk you with video cameras, microphones and GPS. Your biometric data is being collected for lots of different purposes. Should we be thinking about how that data is being secured, because once a thief has your data how possible will it be for you to replace your fingerprints or your DNA? 3D printing will make it possible to counterfeit almost everything…from drugs and guns to designer clothing and jewelry. And these are situations that are already possible with today's technology. What about the technology of tomorrow? It will create entirely new types of crime. Although the explosion of technology will produce tremendous benefits, it will also raise the potential for abuse and crime. Now is the time to think about whether existing laws and enforcement methods will work in the coming years, or if completely new strategies will be needed.

The Internet of Things: Technology Risks When Everything Is Connected

Your father's pacemaker has just been hacked. Control of the car being driven by your daughter is intercepted by someone miles away, who decides to slam on the brakes while she is driving on a high-speed freeway. You are using your new smart home controller to make online purchases and conduct banking transactions, but you may not realize that someone else has access to all of the data being transmitted. Millions of new "smart" devices in your home and office will always be watching and listening to everything you say and do. Industrial sensors to monitor and control automated systems, connected vehicles, medical devices, fitness trackers, security systems and cameras are increasingly able to communicate wirelessly with their cloud-based hosts as well as with each other. How will this technology affect your privacy and personal security? It conceivably could change crime and investigations forever in ways that nobody has even imagined.

The Darknets: What You Don't Know

There are underground networks where any type of drug or weapon can be purchased and the transactions can be difficult (if not impossible) to trace. Credit card and bank account data, counterfeit currency, medical records, and even assassins are available. Human trafficking and child pornography can also be found here, along with tutorials to commit any type of crime. We call these networks Darknets, and we'll show you how they work and explain how they are being used by criminals and terrorists all over the world.

Walt Manning

Walt.Manning@Technocrime.com
972.768.4134
Twitter@WaltManning1

Untraceable Links: How Criminals Use Technology to Cover Their Tracks

Can you catch an invisible crook that leaves no evidence or clues? Technology now provides new tools and techniques for criminals to cover their tracks. Services and apps that provide private and secure communication are more widely used and are even growing in general popularity. Some of these apps send messages that self-destruct. There are new "mesh" network apps that allow all mobile devices running the app to create their own network, and users can communicate without ever using the Internet. Virtual Private Networks (VPNs) can give users the ability to look as if they're located in more than two places at the same time. Many of these new apps and services have built-in encryption. To increase your chances of finding people and evidence, you need to learn about how they try to create these untraceable links.

Virtual Currencies and Investigations

What if there was an easier way to launder money or hide it? Do you think the crooks would take advantage? Virtual currencies like Bitcoin are being increasingly used in both the real world in virtual worlds to purchase almost anything. In almost all cases, virtual currencies can be converted back into real world currency. They have been used to transfer and launder funds across international borders and to fund terrorism, and there are almost no laws or enforcement in this area. Few law enforcement agencies and investigators know much about virtual currencies, and there is no consistency in how international law treats this new technology. "Following the money" in an investigation will now be much harder…if it will even be possible.

The Future of Investigations: Virtual Reality, Virtual Worlds, Virtual Crime

If you could go to a new world where you could be anyone you want to be, would you go? What about instantly changing your looks, physique and personality to someone completely different? Virtual reality technology can let you live experiences that have never been possible before. The line between the virtual world and the real world is blurring. Research is showing great psychological benefits from the technology, from managing pain to simulating situations in a virtual environment to help with therapy. There are virtual worlds where a person can live a parallel life...complete with a career, family and home. What we used to think of as online games has evolved into something much larger and more sophisticated. People will have multiple identities in these different virtual environments, and every type of real-world business will also exist in numerous virtual worlds. Will real-world laws apply or only the hosting company's terms of service? How will legal jurisdiction be decided, and who will investigate virtual crimes?

Walt Manning

Walt.Manning@Technocrime.com
972.768.4134
Twitter@WaltManning1

The Most Dangerous Threat To Your Data and Privacy? Your Mobile Devices

You didn't know that the mobile app you just installed gave the developer permission to upload your contacts, read your text and email messages, and track your location? Your brother's phone has been infected with malware, and a group is using his mobile banking app to drain the funds from his bank account, but changed the data on his screen to show only the expected transactions and balances in the account. These risks already exist and have been used to commit crime. Lost or stolen mobile devices have contributed to over one-half of all reported data breaches. Most people aren't aware that connecting a device to unsecured public Wi-Fi signals can give an attacker access to confidential business and personal data. Malware can seize complete control of a mobile device. Let us show you some of these risks and how to protect yourself and your company.

Bring Your Own Device Programs and Mobile Device Forensics

How do you conduct an investigation involving personally owned mobile devices? Some of these may be the devices of outside contractors or vendors. Can you preserve the data on these devices without violating the individual's personal privacy? Organizations with BYOD programs frequently didn't think about the possible problems that would be caused for investigations and litigation matters. Digital forensics tools can't keep up with the ever-changing operating systems, the new secure apps that provide end-to-end encryption for voice calls and messaging, or the use of encryption to protect any physical access to the device's data. There is no one forensic tool that can extract and preserve every type of electronic evidence from every device, and new devices appear on the market daily.

Cosmos Computing

Do you know where all of your data is stored today? Many people already use more than one cloud computing service, and even with those you may not ever know where the data is physically stored. Even the same provider could store data on virtual servers in different countries. Cloud computing creates challenges for investigators, because the potential electronic evidence could not be fragmented and maintained by multiple service providers, with different computing platforms and in other countries with different legal systems. However, there are already companies who are developing satellite platforms to provide Wi-Fi communication capability to the entire planet from space. Also using these satellites to store data would make the problem of identifying and preserving electronic evidence even worse. In addition, there are new distributed networks being developed that will break any computer file into small pieces, each of which is encrypted, and the pieces scattered across every device connected to the network for storage. The days of finding a complete data file stored on a single device will demand new types of specialist investigators with new skills and new tools that don't exist today.

WALT MANNING

Walt.Manning@Technocrime.com
972.768.4134
Twitter@WaltManning1

Testimonials

Walt Manning's presentations highlighting the risks and dangers of fraud and cybercrime on the Dark Web is a must have training course for 21st century fraud fighters. Anti-fraud professionals must be knowledgeable of where the criminals are operating and the techniques that they are currently employing. The information received through Mr. Manning's presentations is engaging, eye-opening, and downright frightening.

-- Ryan C. Hubbs, ACFE Faculty Member and President of the Houston Chapter of the ACFE"

Even after the lunch gong sound people wanted to hear more. Your presentation at the ACFE meeting in San Antonio was a highlight.

– K. Easton

I can say this was the best seminar I`ve attended, ever, on any topic. Walt was expressive in his presentation, without being over the top. This topic is very interesting to me."

Best CFE program I have attended including the two our firm has given over the last two years!!!! Walt was awesome!!"

-- Attendees from Kansas City Seminar, October 2015

Wow! What an eye-opening presentation!

– K. Poplin

I had the opportunity to attend a workshop that Walt presented at the 2015 ACFE Global Fraud Conference, and was blown away by his material. Walt is extremely knowledgeable on highly technical and complex subject, but is able to "de-mystify" the information so that those seeking an introduction or skills expansion on these subjects come away with useful and actionable knowledge. I highly recommend Walt for technology related fraud training!

-- Melissa Smart, President, Central Ohio Chapter ACFE

I have had the pleasure of associating with Walt for over 20 years. I continue to be amazed at his understanding of the digital world and all of its pitfalls and variabilities. And what is even more amazing is that he can explain it in such a manner that even a layman like me can understand what he is saying. In my opinion, Walt is the consummate professional in his field.

If you are looking for an individual to train your staff in any area related to digital technology or for someone to assist you in designing a security system for your IT network, without question, Walt is your man.

-- Dennis F. Dycus, CFE, CPA, CGFM, Director (Retired)

WALT MANNING

Walt.Manning@Technocrime.com
972.768.4134
Twitter@WaltManning1

Bio

Walt Manning is an investigations futurist who researches how technology is transforming crime, and how governments, legal systems, law enforcement and investigations will need to evolve to meet these new challenges. In his almost 40 years of experience in law enforcement and private practice he has consulted with or given presentations to organizations that include:

- Defense Intelligence Agency
- General Accounting Office
- Federal Financial Institutions Examination Council
- Texas Department of Public Safety
- Dallas Police Department
- Inter-American Development Bank
- LexisNexis
- Orange
- EDS
- Texas Instruments
- The Halliburton Company
- Association of Certified Fraud Examiners
- Institute of Internal Auditors
- ISACA

Walt's articles have appeared in:

- Police Chief Magazine (International Association of Chiefs of Police)
- The FBI Law Enforcement Bulletin
- Fraud Examiner Magazine (Association of Certified Fraud Examiners)
- The ABI Journal (American Bankruptcy Institute)
- ACFE Insights blog (Association of Certified Fraud Examiners)

He has been interviewed or quoted by:

- Forbes Magazine
- SC Magazine
- Security Magazine
- Computerworld
- Information Week
- The Dallas Morning News
- The Australian newspaper
- Fraud Intelligence
- Strategic Finance magazine
- Financier Worldwide

Walt Manning started his career as a police officer in Dallas, Texas, and later created the department's first unit to provide support for criminal cases involving technology. After twenty years in law enforcement, Walt founded a consulting firm that specialized in providing digital forensics services in both civil and criminal cases. He later served as a Director with the AlixPartners e-Discovery practice, where he helped to manage e-discovery and digital forensics services in major international criminal and civil litigation matters. Walt's goal is to "drive and inspire the evolution of investigations," by helping investigators and organizations to prepare to meet these new legal and investigative challenges of the future.