

Meeting Agenda

The Tampa Bay Chapters of **ISSA**, **InfraGard**, and **ISACA** will be hosting an all day event on Friday June **19, 2009**, at **9:00 a.m.** at Tech Data Corporation, Clearwater, Florida. Below is the agenda for the speakers and breaks. Continental breakfast will be served along with a box lunch.

Location: Tech Data Corporation, 5350 Tech Data Drive, **Raymund Center (old Building A)**, Clearwater, Florida.

Directions: See below. Also on http://www.techdata.com/content/visitor/abouttd/td_map.aspx

Time: Friday, June 19th, 2009 - 9:00 a.m. to 4:30 p.m.

Agenda:

8:30 - 9:00	Registration and Coffee/Donuts
9:00 - 10:50	Topic 1: Kevin Mandia - Mandiant Corporation
11:00 - 11:10	Break/prize drawing
11:10 - 12:00	Topic 2: Jeremiah Grossman - WhiteHat Security
12:00 - 12:50	Lunch Served
1:00 - 1:50	Topic 3: Jim Tiller – British Telecom of North America
2:00 - 2:10	Break/prize drawing
2:10 - 3:00	Topic 4: Janice Murray – Inovia LLC
3:00 - 3:10	Break/prize drawing
3:10 – 4:00	Topic 5: C.J. Bast - ITpreneurs
4:00 – 4:10	Break/prize drawing
4:10 – 5:00	Topic 6: Rob Curls - Tribridge
5:00	Wrap up/prize drawing

If you have any other questions, please contact:

Stephen Jones, ISSA at (813) 217-3622 stej0n3s@gmail.com
John Medaska, InfraGard at (727) 692-4493 jm@tampabay.rr.com
Pierre Joseph, ISACA at (813) 844-7939 pjoseph@gmail.com

Presentation and Speakers

Presentation 1: Kevin Mandia - Mandiant Corporation

Bio: Kevin founded Mandiant Corporation in 2004 as an elite team of incident responders. Prior to joining Foundstone, Kevin was a Special Agent with the Air Force Office of Special Investigations (AFOSI), where he specialized in computer intrusion cases. Upon leaving the AFOSI, he developed a computer intrusion response course specifically requested by the FBI. Kevin has trained more than 400 FBI agents as well as personnel from the State Department, the CIA, NASA, the U.S. Postal Service, the Air Force, and other government agencies. He is a regular speaker at numerous forums, including Network+Interop, Blackhat, Infragard, HTCIA, SC Magazine's Information Security Forum, and Techno Security. He is a guest Professorial Lecturer at Carnegie Mellon University and The George Washington University. Kevin has responded to more than 40 computer security incidents in the last 3 years, running the gamut from international computer intrusion to theft of Intellectual Property. The author of two essential books on incident response by McGraw-Hill, Kevin holds a B.S. in Computer Science from Lafayette College and a M.S. in Forensic Science from the George Washington University.

Topic: The State of the Hack

During this presentation, we discuss the technical and authentic details of computer security incidents that have occurred at large organizations within the last 5 months. We demonstrate how these organizations have been responding to these incidents, and the emerging technologies that can assist both the Government and corporate America in responding in a more efficient and effective manner. We provide low-level technical details during the case studies for the audience to witness first hand the activities of current day intruders. We will demonstrate freely available Incident Response software, and discuss its application in improving the timeliness and effectiveness of Incident Response.

Specifically, the presentation follows this format:

1. Case Studies providing a hands-on look at the computer security incidents we have responded to since July 2006. All case material discussed is from July 2006 until the present.
2. Performing Agile Data Collection.
3. In-depth discussion of several attacker tool sets and their techniques once they gained access to the victim hosts. This includes a discussion of how the attacker's tools and techniques have impacted our Incident Response methods.
4. The logical evolution of Incident Response; specifically outlining the tools and techniques that need to be developed/deployed to meet the ongoing threat of computer intrusions.

Presentation 2: Jeremiah Grossman - WhiteHat Security

Bio: Jeremiah Grossman, chief technology officer and founder of WhiteHat Security

Topic: Sequel to the much acclaimed "Get Rich or Die Trying" (BlackHat USA 2008) presentation.

This time around we're not going to restrict ourselves to the super simple, legal gray area, or even those previously exploited in the real-world. The theoretical is fast becoming dangerously likely and we can't wait until it becomes a reality for them to be examined.

Many people still mistakenly believe profiting illicitly or causing serious damage on the Web requires elite, ninja-level hacking skills.

Nothing could be further from the truth. In fact, given the ever- increasing complexity of Web technology, using sophisticated vulnerability scanners can make the monetization process more difficult, noisy, and arguably less lucrative. While scanners and code reviews can lend themselves to identifying SQL Injection and Cross- Site Scripting, which can lead to significant harm and financial loss, so too can the issues they consistently miss -- business logic flaws.

Business logic flaws, or an oversight in the way a system is designed to work or can be made to work, is one that typically can be gamed in low-tech ways. In the real world, these attacks have lead to between four and nine-figure paydays with nothing more than basic analytical skills required. Furthermore these are attacks that Intrusion Detection Systems (IDS) will miss, Web application firewalls can't block, and Web application vulnerability scanners fail to identify.

Attacks so subtle that most organizations will not know they've been hit until a financial audit uncovers a discrepancy, they receive angry customer calls, or when they become headline news.

The presentation will explore how poorly thought out online marketing promotions are taken advantage of: obtaining free conference badges through insecure registration processes; drafting Web visitors into a botnet army via advertising affiliates; profit by pillaging global natural resources; and more.

Presentation 3: Jim Tiller – British Telecom of North America

Bio: Jim Tiller is the Vice President of Security for BT in North America. An internationally recognized security expert, Tiller oversees a broad information security practice for BT, working with customers in the development of comprehensive security programs targeted at risk optimization and business enablement. Tiller has over 16 years of information security experience and has an accomplished record of innovation including an unprecedented #1 worldwide information security rating from the NSA. He is the author of numerous publications including two books, “Technical Guide to IPsec VPNs” and “The Ethical Hack”, contributed to the “Official (ISC)² Guide to the CBK”, and the “Information Security Management Handbook” for the last seven years. Tiller holds three patent applications detailing methods and technology concerning security policy and management and the interaction with employees systems and applications and has collaborated on solutions with top security vendors such as Cisco and Check Point. Tiller regularly speaks for global organizations, government, and industry events and has been interviewed by leading publications such as Network World, Information Security Magazine and Microsoft Security 360. Tiller holds several security certifications including CISSP, CISA, CISM, and NSA, is a member of ISSA, Infragard, and ISACA and is on the advisory board of Auerbach Publications.

Jim Says:

“Information security is and should be about the threats. These can come to you as a hacker in the night or a disgruntled employee; or materialize as gaps in compliance or the inability to meet a business demand. Security is omnipresent and is inexorably tied to the success of an organization in the 21st century. Security is no longer just about the technology. It’s about the ability to accurately apply, test, and effectively manage and monitor controls across people, process, and technology in a manner that enables the business to thrive in a threat-rich, global environment.”

Topic: Maintaining Security During an Economic Fallout

Growing reliance on complex information technology, expanding stores of information and increasing compliance requirements have collided with aggressive and sophisticated security threats, both internal and external. The result: enterprises are facing a monumental risk that cannot be ignored - even in times of financial distress. Fortunately, when many security budgets are under stress, adaptable security practices that are complementary to and supportive of business dynamics can actually increase security effectiveness without new investments.

Topics to be discussed include:

- Aligning strategic, financial and tactical initiatives
- Understanding interdependencies and threats
- Optimizing people, processes and technology
- Analyzing and prioritizing security investments
- Defining appropriate solutions

Presentation 4: Janice Murray – Inovia LLC

Bio: Janice Murray

Janice has been helping businesses improve their bottom line for over 20 years. In 2000, Janice formed Inovia, LLC, a consultancy focused on strategic development and project management, and relocated that business from New York to Florida in 2007. Over the years, as compliance and risk management have become more important to her clients, she has included IT risk management and privacy in her scope, focusing on information risk management, including for Sarbanes-Oxley, IT policy development and deployment, application security and privacy compliance, as well as project management consulting and training.

She has managed projects in financial services, insurance, business process outsourcing, energy and telecommunications, working with such companies as AT&T, Citibank, Con Edison, EUR Systems (now Intec) and MetLife. As a professional, Janice has a clear understanding of business processes and technology as well as the risks and issues faced by management in using and protecting information.

Janice is experienced in managing global projects and cross-cultural teams, facilitating the integration of a broad range of experience, background and beliefs, to develop successful strategies, processes and solutions. She has collaborated across business and IT to successfully deliver projects throughout the world. This has required coordinating multiple programs and projects with multiple business groups and functional groups and engaging higher management and leadership with differing goals and culture.

Janice holds certifications as a Certified Internal Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), Project Management Professional (PMP) and most recently achieved certification as a CIPP (Certified Information Privacy Professional), providing the range of competencies to support information security. She has an MBA in Finance from NYU – Stern School of Business, and attended the Thunderbird School, receiving a certificate in Global Business Development.

Topic: Information Security – Not Just IT Anymore

Despite the efforts of security professionals, the number and scope of data breaches has grown, and are not limited to hacking into networks. As perimeters have been made more secure, and access control at both the physical and logical areas is improved, other tunnels are being driven into the sources of information, including application access and people error. Data breaches not only create a reactive need to identify and remediate any damage, but cause long term fear at the consumer level and negative impact at the business level for reputation. It isn't enough to provide detection and remediation – preventive measures must improve. The number of stakeholders in this effort, with differing agendas, directions and goals, increases the complexity of the effort to protect data.

This presentation will explore the concerns of the many business stakeholders in information security, identify some of the issues that are emerging and make some recommendations how IT security professionals can integrate with other stakeholders as they develop new preventive actions, developing a new converged focus on information risk management.

Presentation 5: C.J. Bast - ITpreneurs

Bio: C.J. Bast M.Sc. - Corjan is Global Product Manager for the COBIT education portfolio at ITpreneurs, a global content and instructor provider for IT best practices training. Before joining ITpreneurs, he was a

Business Development Manager and IT Consultant for a firm that focused on assisting organizations with implementing IT Governance frameworks such as COBIT and Val IT. He frequently collaborates with other professionals to publish articles regarding IT Governance. He holds a Masters in Technology & Innovation Management from the University of Technology in Eindhoven, the Netherlands and currently resides in Florida.

Topic: An overview and demonstration of the COBIT Education Portfolio

Content: Control Objectives for Information and Related Technology (COBIT) is an IT Governance framework which has been developed since 1996 onwards and has become the de facto standard for overall IT control. Since it maps strongly to all major, related standards, many organizations have introduced COBIT within their organization.

Specific ISACA COBIT Training has been developed to assist companies with their COBIT implementations. From Virtual Learning (cobitcampus.isaca.org) and Classroom Courses (www.itpreneurs.com) to Business Simulations like the COBIT Games (www.cobitgames.com).

This 45 minute presentation will be a mixture of slides, quizzes, videos and demonstrations.

Presentation 6: Rob Curls - Tribridge

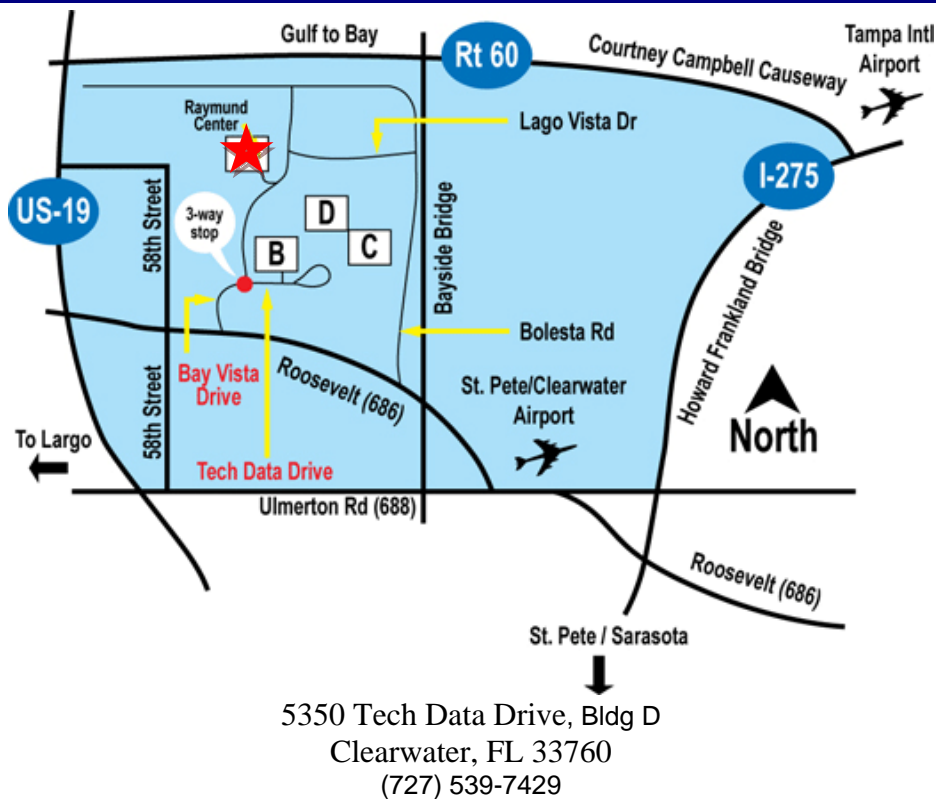
Bio: Rob Curls is a Technical Manager in the Tribridge Security and Infrastructure practice. A Microsoft specialist and part of the Microsoft Delta Force for Server 2008 and Hyper-V virtualization, Rob's expertise includes Messaging, Domain Consolidation, Virtualization, Microsoft Clustering Services, and SQL server. He has helped local clients including Moffitt Cancer Center, Hard Rock Café, the Orlando Magic, WCI Communities, the University of South Florida and 21st Century Oncology design and deploy advanced messaging and virtualization solutions.

Prior to joining Tribridge in 2007, Rob served as the Senior Exchange Administrator for a healthcare organization with over 10,000 employees nationwide.

Topic: Security considerations in a virtualized environment covering issues such as backup and recovery, process isolation, virtual networks and monitoring.

Map/Directions:

Tech Data Corporation, Clearwater



Directions for the Raymund Center (old Building A): At the three-way stop, turn left onto Bay Vista Drive. Continue straight until you reach a 4-story building with flags on your left.

Directions to Corporate Campus

From Tampa, Orlando, and east:

Take I-275 South across the Howard Franklin Bridge. Exit on Ulmerton Road (688). Follow 688 until you see signs for 686 (Largo/Clearwater.) Take 686 west to Bay Vista Business Center. Turn right into the entrance and follow the road until you reach a 3-way stop.

From St. Petersburg and south:

Take I-275 north to exit 16, Roosevelt Blvd. (Largo/686 west). Follow Roosevelt to Bay Vista Business Center. Turn right into the entrance and follow the road until you reach a 3-way stop.

From Clearwater and north:

Take U.S. 19 south to Roosevelt Blvd. (686). Turn left on Roosevelt Blvd. and head east until you reach Bay Vista Business Center. Turn left into the entrance and follow the road until you reach a 3-way stop.