ISACA
Trust in, and value from, information systems
San Francisco Chapter

2014 SF ISACA Fall Conference
Speaker Information

How to Improve Your Risk Assessments with Attacker-Centric Threat Modeling

TONY MARTIN-VEGUE
Sr. Manager of Cyber-Crime & Business Continuity, Gap, Inc.

Governance, Risk, and Compliance – G33

Session Abstract

CISO's and risk analysts alike often get caught up in checking boxes on a list of control objectives in order to satisfy compliance and regulatory requirements. However, companies that only view risk through a narrow, regulatory or compliance-focused lens have the potential to overlook a myriad of threats that could impact business continuity, customer privacy and security and financial solvency. The last several high-profile data breaches prove that compliance does not equal security.

There are many ways to assess risk in a meaningful, efficient way that drives business value. Many top companies are moving away from control-based and vulnerability-based risk assessments and are instead putting themselves in the shoes of an attacker. In order to keep up with the rapidly evolving world of cyber criminals and crime rings, organizations are learning to utilize threat intelligence to ascertain the methods, goals, and objectives of threat agents that are targeting their firm or similar firms in their sector. This helps an organization produce focused risk assessments that take a business-centric approach.

This is a beginner to intermediate-level presentation designed to provide an introduction to threat modeling, a primer on threat modeling techniques, ways to integrate threat modeling into risk management frameworks (such as FAIR and NIST), and how to build a library of threat agents specific to one's firm. Attendees will learn hands-on techniques to perform threat modeling that they will be able to immediately integrate into their risk assessment processes.

Target Audience

Risk analysts, IT auditors, information security professionals and anyone else managing risk would benefit from the presentation. Basic knowledge of risk management is helpful, but not required.

Speaker Bio

Tony Martin-Vegue is Sr. Manager of Cyber-Crime & Business Continuity at Gap, Inc. His enterprise risk and security analyses are informed by his 20 years of technical expertise in areas such as network operations, cryptography and system administration. He has worked for First Republic Bank, Wells Fargo, Cigna and CoreLogic. His current research areas involve improving risk assessments and the risk treatment process, threat modeling and bridging the gap between business needs and information security. He has a BS in Business Economics from the University of San Francisco and holds the CISSP, CISM, CEH, GCIH and GSEC certifications.

Speaker Details (optional):	
Email	tony.martinvegue@gmail.com
Facebook URL	
Twitter URL	https://twitter.com/tdmv
LinkedIn URL	www.linkedin.com/in/tonymartinvegue/
Website	