Welcome to Metricon 6, August 9th, 2011

8:30 - 9:10  ORM: Operation Risk Management
Richard Seiersen, Kaiser Permanente

9:10 - 9:50  Critical Control Security Metrics for Continuous Network Monitoring
Richard Lippmann, James Riordan, Cyber Systems and Technology Group, MIT Lincoln Laboratory

9:50 - 10:10  Break

10:10 - 10:50  Quantifying the Unquantifiable: When Risk Gets Messy
Wendy Nather, Senior Analyst, 451 Group

10:50 - 11:30  Moneysec: Applying the "Moneyball" philosophy to information security metrics
Brian Keefer, Jared Pfost

11:30 - 12:30  Lunch

12:30 - 1:05  That's So Meta: Gleaning Business Context In The Vulnerability Warehouse
Ed Bellis, HoneyApps

1:05 - 1:40  "Shall we play a game?" and other questions from Joshua
Joshua Corman

1:40 - 2:15  Corporate Threat Modeler
Dominic White, SensePost

2:15 - 2:35  Break

2:35 - 3:10  Measuring the Impact of Insider Activity
William Claycomb, Michael Hanley, CERT Insider Threat Center, Software Engineering Institute, Carnegie Mellon University

3:10 - 3:40  Is an organization without Cyber Liability insurance like a fish without a bicycle?
Jake Kouns, Director, Cyber Security and Technology Risks
Underwriting at Markel Corporation

3:40 - 4:10  Operationalizing Analytics
Allison Miller, Itai Zukerman

4:10 - 4:30  Break

4:30 - 5:30  Collecting and Sharing Security Metrics: Overcoming Fear (or not!)
Panel Moderated by Mike Rothman, Securosis

Thank you Alex Hutton for coordinating Metricon 6 this year!

Special thanks to all the volunteers that made Metricon 6 happen this year:
Chris Hayes, Jay Jacobs, Chris Walsh, Ray Kaplin, Pete Lindstrom, Allison Miller and Mike Dahn

Thanks also to Dan Geer, Andrew Jaquith and Jennifer Bayuk
ORM: Operation Risk Management
Richard Seiersen, Kaiser Permanente
Operational Risk Management (ORM) is the next generation application of business intelligence to the security domain within Kaiser. The main security dimensions within ORM are mitigating controls, vulnerabilities (up and in the stack) and business impact. "Risk tolerance rules" operate on the aforementioned security dimensions creating workflow and reporting related to augmenting systems' posture. The ORM framework is predicated on the automated collection and analysis of enterprise asset data (business portfolio to hardware/software components), vulnerability data (N systems), and mitigation policy data (NIPS/HIPS, memory protection etc.). This data is loaded into dimensional models with reporting and workflow occurring inside a web services based GRC framework.

Critical Control Security Metrics for Continuous Network Monitoring
Richard Lippmann, Cyber Systems and Technology Group, MIT Lincoln Laboratory; James Riordan, Cyber Systems and Technology Group, MIT Lincoln Laboratory
Our recent work on metrics is motivated by the SANS “20 Critical Security Controls” document that identifies the twenty most important cyber threats and also the critical security controls that protect against these threats. We have developed metrics that can be computed automatically and continuously on a network to assess how well four of these foundational controls protect against their corresponding threats. Each new metric is based on a realistic and well-defined mathematical adversary model, directly measures the effect of controls that mitigate adversaries, continuously estimates the risk from each adversary, and provides direct insight into what network changes must be made to improve security. Metrics are designed to address specific threats, maintain practicality and simplicity, and motivate risk reduction.

Quantifying the Unquantifiable: When Risk Gets Messy
Wendy Nather, Senior Analyst, 451 Group
Humans are always trying to control the uncontrollable by trying to predict it; if they can’t predict it, then by golly they’re at least going to surround it with numbers. There are two problems with this: they confute accuracy with precision – because numbers allow precision – and not everything can be described with a number. Describing the impact of an incident in terms of time and money is pretty straightforward, even given the inherent uncertainty. But additional impacts, such as reputational and political ones, don’t lend themselves well to numbers, and the risk is real, particularly in the public sector where it’s not about stock price or loss of sales.

Moneysec: Applying the "Moneyball" philosophy to information security metrics
Brian Keefer, Jared Pfost
In his bestselling book “Moneyball,” Michael Lewis showed how baseball GM Billy Beane built a highly-effective team with very little money, by identifying the statistics that correlated most closely with increased probability of winning. Similar to baseball several decades ago, we aren’t collecting enough information to be able to tell the difference between good decisions and pure chance. We’re at the “call to action” stage: start with the basics, demonstrate value, and justify further investment. Our talk will suggest new statistics for organizations to collect and track, similar to how baseball enthusiasts started tracking batted-ball trajectories & distances, and created FIP, WAR, Zone rating to get a better idea of the worth of individual players. By tracking this data, organizations will be able to better represent the value of individual controls and drive future security investment.

That’s So Meta: Gleaning Business Context In The Vulnerability Warehouse
Ed Bellis, HoneyApps
For years businesses have been mining and culling data warehouses to measure every layer of their business right down to the clickstream information of their web sites. These business intelligence tools have helped organizations identify points of poor product performance, highlighting areas of current and potential future demand, key performance indicators, etc. Imagine if you had a data warehouse covering all of your applications, infrastructure, logs, vulnerability assessments, incidents, financial information, and metadata. What could you do with this readily available information? In this talk, Ed will cover some of the many sources of security data publicly available and how to apply them to add context to your security data and tools to help make more intelligent decisions. Ed also points out a number of ways to repurpose information and tools your company is already using in order to glean a clearer view into your security program and the threats that may affect it.

"Shall we play a game?" and other questions from Joshua Corman
Are we going about this thing all wrong? We know we need to transcend the age of mysticism and faith based security, but are we sure our current path will lead us there? Are our fundamental models and assumptions helping or hurting our evolution? Is the earth the center of the solar system? We’ll attempt to get some perspective on the nature of this whole security "WOPR" of a complex system - so as to better aim our metrics endeavors.

Corporate Threat Modeler
Dominic White, SensePost
In 2007, SensePost introduced an attempt to take our years of penetration testing experience, and use it to model the likely results of multiple "pentests" performed across an environment. The methodology and tool were released as the Corporate Threat Modeler. Several years later, and the methodology has advanced significantly. Initially highly flexible to incorporate multiple approaches, it has been better aligned to existing risk management strategies, and bounded to a consistent approach that has been used at several customers. This talk will take attendees through this methodology, focusing on the key alignments with other strategies, and assumptions "bouncing" the methodology. We will also show how different our approach is to others, and why we feel it is a useful addition to the field. Additionally, we will release parts of the updated version of our tool encompassing these changes.

Measuring the Impact of Insider Activity
William Claycomb, Michael Hanley, CERT Insider Threat Center, Software Engineering Institute, Carnegie Mellon University
How does an organization measure the impact of an insider incident? Dollars? Loss of productivity? Embarrassment? Stock prices? Does a million dollar loss mean as much to a multi-national corporation as it does to a local "mom-and-pop" store? What about insiders that almost get away with stealing millions of dollars or a company’s deepest secrets, but are caught due to a fluke event? These are the types of challenging questions facing insider threat analysts concerned with measuring impact – questions CERT’s Insider Threat Center hopes to answer. In this presentation, we explore what quantitative and qualitative methods can be leveraged to help measure the impact of an insider attack on an