

Security, BCP & Technology Risk Management - Agenda

**Exhibit Hall Reception -
sponsored by McAfee, Inc.
- please join us in the exhibit
hall at 3:00PM for refreshments**

Conference Sessions 3rd floor, Exhibit Hall 2nd Floor

08:00am - **Conference Registration and WSTA Introduction**
08:45am

08:45am - **Security Architecture 2006: Learning to Love the Death of Perimeters**
09:15am *F. Christian Byrnes, Sr. Vice President, Security Practice Lead, META Group*

Perimeters no longer work. Someday all of the technology we acquire will be inherently secure, but that day is not soon. And end users (particularly executives) will always be resistant to changing insecure behaviors. This conference keynote presentation will start by outlining the major forces and trends that dictate how we approach security. It will then describe one proven response to this deperimeterization known as Trust Domain Architecture. This architected security approach changes how network and security technologies are deployed in order to better match the acceptable residual risk levels of the organization.

09:20am - **Conference Sessions**
12:00pm

TRACK 1

09:20am - **Safeguarding IT Infrastructure:
Meeting the Technical &
Organizational Demands of a
Business**

*Peter Burghardt, Chief Operating
Officer & Joseph Nadan, Chief
Technology Officer, AIGT*

Joseph Nadan, Chief Technology Officer, and Peter Burghardt, Chief Operating Officer, of AIG Technologies will present together to give attendees both the business and technical perspective regarding disaster recovery solutions. This session will address how to

TRACK 2

09:20am - **Keys to a Secure and Manageable
Wireless Enterprise**

*Sumit Deshpande, Vice President,
Wireless Solutions Group, Computer
Associates*

Wireless computing is rapidly becoming a critical and integral part of the enterprise business process. A WLAN that is not managed and secured properly is a serious threat to the integrity and efficiency of the network. There are several vulnerabilities in 802.11 or Wi-Fi technology that affect security and management - weak encryption, propensity

develop and implement a disaster recovery solution that meets the technical and organizational needs of a business. Attendees will also learn about best practices and trends ranging from the importance of disaster recovery testing to continuous program improvement.

for intrusion attacks, and rudimentary management standards are just a few. Having the right understanding of the technology and business environment as well as utilizing the appropriate enterprise management solutions is critical to ensure a secure and manageable wireless computing environment. This session looks at the fundamental issues with WLANs and reveals the keys to implementing a successful WLAN environment. Case studies will also be discussed.

09:50am - **Bringing Added Value to Your Disaster Recovery Architecture**
10:20am *Tim Saunders, VP Product Mgt., Enterprise Networks Division, ADTRAN*

A disaster recovery plan can be an option for some businesses, but is a necessity for financial institutions. You know the importance of a well-planned and easily executable disaster recovery plan, because in your business, every minute of downtime could cost you millions of dollars. This session will take a look at some of the most common disaster recovery mechanisms and show you how to more effectively utilize network resources to plan for disaster situations while improving the day-to-day productivity of your operation. Some of the architectures to be addressed will include dual network solutions, redundant circuits, and using the Internet as a source for backup. The session will also address issues to consider when selecting network hardware and show how feature selection can enhance your disaster recovery options and day-to-day operations without sacrificing the bottom line.

09:50am - **SSL Based Access: Breakthrough in Secure Remote Access Technology**
10:20am *Joseph Steinberg, CISSP, Director of Technical Services, Whale Communications*

This session will discuss advances in remote-access technology that afford firms in the financial industry new opportunities to enhance worker productivity, achieve greater top-line revenues, and better address business-continuity needs. Security issues related to implementing remote access will be an integral part of the presentation.

10:20am - **Break**
10:30am

TRACK 1

10:30am - **Security Best Practices and Technologies Enterprise IP Telephony**

Jim Marussich, Product Sales Specialist for Security at Cisco Systems

Numerous threats, from device failures to worms, viruses and malicious attacks, affect the uptime of networks. With the reliance on the IP network for telephony, IP-based threats must be mitigated. In an IP telephony environment we must guarantee the ability for hundreds or thousands of IP phones to dial emergency services and conduct business with a very high degree of reliability and security. In this session we will discuss the techniques to mitigate these attacks, providing best practices for IP telephony systems.

11:00am - **Increasing Network Survivability via Optical Networks**

Rich Goode, Product Marketing Director, Lucent Technologies

CIO organizations today are facing increased pressures to ensure that business interruptions due to network infrastructure failures are minimal, even after catastrophic events. Geographic diversification has increased the demand for Storage Area Networking Services in the MAN/WAN and created new business opportunities for telecommunications service providers. This presentation discusses how emerging Storage-Over-SONET solutions are the likely solution of choice for medium / large enterprises to interconnect SANs when a small number of storage interfaces are needed per site or where complete node protection is desired.

TRACK 2

10:30am - **Securing Networks Against a New Generation of Threats**

Craig Carpenter, Director, Field Marketing, Fortinet

Traditional perimeter security approaches are no longer enough to protect vital data and offer the wide variety of security services demanded by users: What's needed is a comprehensive multi-tiered complete content protection security defense. This presentation covers dynamic threat prevention and what's required to detect and eliminate the most damaging, threats without degrading network performance.

11:00am - **Proactive Network Based Identification of Threats**

David Cottingham, Director, AT&T Managed Security Services

In today's network environment administrators are struggling to make sense of the constant barrage of IT Security threats. Daily vulnerability announcements can keep a network administrator in a constant cycle of system patching, anti-virus updates, and threat assessment across their network infrastructure. This session will provide an overview of some high profile worm and anti-virus events from the last year and more importantly describe a methodology and set of analysis and protection tools that provide early warning and mitigation of security incidents. Learn how through the use of these tools network administrators can receive notification of developing attacks and large scale vulnerability exploits far in advance (sometimes as much as 30 days) prior to wide scale impact of the vulnerability. The session

will cover an end to end methodology for deployment and management of security infrastructure and processes ranging from high bandwidth optical carriers to individual workstations.

11:30am - **Secure Networking**

12:00pm *John Roese, CTO, Enterasys Networks*

Traditional perimeter security is not sufficient and scalable to defend against today's sophisticated threats

Threats are converging:

Viruses, Worms, Denial of Service, Intellectual Property Theft, Regulated Compliance Reputation

Value Propositions are converging:

Compliance, Consolidation, Control, Context, Continuity, Capacity, Connectivity, Cost

Technology is converging:

Storage Over IP, Video Over IP, Voice Over IP, End systems, Appliances, Software, Network

Users are converging:

Business Appliances, Household Appliances, Internet & Intranet, Sub-Contractors, Customers, Visitors, Suppliers, Partners

Is Security pervasive in your network?

This session will take a look at important security solutions that address these demands on your network.

11:30am - **Ensuring Business Continuity**

12:00pm **During Worm Storms**
T. Kent Elliott, CEO, ForeScout Technologies

Network worms' automated spreading mechanism increases network load, consuming so much bandwidth that it chokes out legitimate traffic, resulting in revenue and productivity losses. Despite the best efforts of the security community, total protection against network worms has proven to be elusive. A new approach is required that: recognizes how difficult it is to stop worms from entering the network, contains the infection to stop it from propagating enterprise-wide, ensures ongoing business continuity during times of worm outbreaks, and gives IT administrators time to patch relevant machines.

12:00pm - **Exhibit Hall (2nd Floor)**

1:00pm *Conference Attendees Only*

The exhibit hall and luncheon will be open to conference attendees only during this time.

1:00pm - **Exhibit Hall (2nd Floor)**

4:00pm *Open to Conference Attendees, Exhibit Hall Registrants and Financial Industry Professionals.*

Site designed and maintained by: [Checco Services, Inc.](#)

