

*"The hackers are getting more malicious and more clever. Traditional security measures aren't working anymore, so you have to step up your vigilance and improve security"*

*-Andy Faris, Message Labs Inc.*



# CORPORATE NETWORK SECURITY

June 19-20, 2008 • WASHINGTON, DC

## Learn How Corporations Can Achieve Optimal Protection To Defend Themselves From Cyber Criminal Activity

Don't miss this National Forum created for those tasked with protecting personal and confidential information in a continuously changing technological environment. You will gain knowledge about the latest up-to-date information, tools, trends and strategies for addressing network security issues from case studies and expert lectures.

### DISTINGUISHED SPEAKING EXECUTIVES INCLUDE:

- Craig Lucca, Manager of Information Risk; **BLOOMBERG**
- Patrick Hale, Deputy Director, State of Michigan; **MICHIGAN DEPARTMENT OF INFORMATION TECHNOLOGY**
- Peter Allor, Program Manager for Intelligence & Vendor Relations and Special Assistant to the GM; **IBM INTERNET SECURITY SYSTEMS**
- Rian Campbell, Information Security; **FEDERAL RESERVE BANK**
- Roger Herbst, CISSP, Senior IT Security Specialist; **THE TIMKEN COMPANY**
- Steve Orrin, Director of Security Solutions; **INTEL CORPORATION**
- Steve Spak, Distinguished Member of Technical Staff; **VERIZON**
- Tara Kisson, Director of Information Security; **VISA, INCORPORATED**
- Tim Callahan, First Vice President, Technology Risk Management and CISO, **PEOPLE'S UNITED BANK**
- Tom Bowers, Senior Security Evangelist; **KASPERSKY LAB**
- C. Warren Axelrod, SVP; **BANK OF AMERICA**

### A TWO-DAY PREMIER INDUSTRY EVENT FOCUSING ON:

- Identifying and dealing with data leakage issues
- Examining the next generation of enterprise security
- Best practices for protecting sensitive information
- The Public-Private sector collaboration to developing a secure cyberspace
- Best carrier security practices for Voice over IP
- The benefits of protecting sensitive data
- Protecting your company from the malware epidemic
- Virtualization Security
- Federal Reserve's National Information Security Awareness Program



# CORPORATE NETWORK SECURITY

June 19-20, 2008 • WASHINGTON, DC

## CONFERENCE DAY ONE: JUNE 19, 2008

7:30 AM - 8:00 AM REGISTRATION AND CONTINENTAL BREAKFAST

8:00 AM - 8:15 AM CHAIRPERSON'S WELCOMING REMARKS

8:15 AM - 9:15 AM: \*OPENING KEYNOTE ADDRESS\* ON YOUR MARK... GET SET... SECURE! MAKING THE MOST OF EVERY IT PROJECT

Too often security teams are ineffective at making real change happen. System administrators and developers see security as a hurdle to overcome; a nuisance at best and a roadblock at worst. In this presentation, Patrick Hale will discuss security from the client's point of view. It will focus on best practices for creating a true partnership with Enterprise Security. Attendees will learn about the State of Michigan's IT journey; an unprecedented statewide consolidation of IT and the resulting security implications. They will also hear how Michigan IT professionals are moving past technology and creating true business partnerships across and beyond state government borders

Patrick Hale, Deputy Director, State of Michigan; **Michigan Department of Information Technology**

*The State of Michigan's infrastructure organization employs over 700 staff members and oversees an annual budget of \$160 million. Since becoming Director of Infrastructure for Michigan in 2005, Mr. Hale's teams have consolidated 17 data centers, eliminating over 1,000 servers in less than a year. They centralized messaging for the state's 57,000 employees, with an expected savings of over \$11 million in 4 years. They have developed an enterprise-wide backup and recovery strategy, backing up more than a billion objects a week. He has also led teams implementing VoIP for more than 6,500 employees in 78 locations, developing a wireless strategy for the state's network and migrating nearly a petabyte of state data to an enterprise storage solution. Patrick Hale has over 17 years experience as a technical architect, infrastructure manager, and strategic planner. He has a long track record of assisting public and private sector entities through large-scale technology integration efforts and has spoken at numerous trade groups and organizations about the importance of technology and its successful implementation.*

9:15 AM - 9:30 AM MORNING REFRESHMENT BREAK

9:30 AM - 10:30 AM THE SECURED ENTERPRISE: ENVISIONING A SAFER FUTURE

Today's online threat landscape is evolving at a pace that is quickly rendering traditional IT defenses ineffective. Financially-motivated hackers are becoming more stealth and targeted in their attacks, while threats originating from privileged insiders also continue to wreak havoc on companies' reputations and bottom lines.

This session will examine the next generation of enterprise security. In order for businesses to thrive, they must implement a security program that combines a strong foundation of policies and intelligent best practices with automated, intuitive security platforms. These must be designed to combat the myriad of online threats without continuous, budget-draining product purchases.

Peter Allor, Program Manager for Intelligence and Vendor Relations and Special Assistant to the GM; **IBM Internet Security Systems**

10:30 AM - 11:30 AM ENDPOINT SECURITY: A CONVERGENCE OF PROTECTION

Much of our business life today is spent out of the office. Our lives are stored on the devices we carry with us. Security for the company and personal data on our mobile devices requires a breadth of defenses that travel along with us. Those defenses have historically been provided by multiple discrete products, but vendors are seeking to provide the mobile worker with a suite of protection under one label. This session will look at what is included in endpoint security and the products and services that can provide that protection.

Roger Herbst, CISSP, Senior IT Security Specialist; **The Timken Company**

11:30 AM - 12:30 PM TRANSFORMING FROM VIRTUALIZATION VS SECURITY TO VIRTUALIZATION BASED SECURITY

This session will provide an overview of platform and application virtualization mechanisms and usages. The advances in virtualization technologies and top security issues of virtualization methodologies will be explored including the current solutions and strategies for dealing with these challenges as well as strategies for effective compliance and enforcement in virtualized environments. There will also be an introduction of new ways to secure platforms using virtualization, application isolation and sandboxing, and policy based execution environments.

Steve Orrin, Director of Security Solutions; **Intel Corporation**

12:30 PM - 1:30 PM LUNCHEON AND EXHIBITS



# CORPORATE NETWORK SECURITY

June 19-20, 2008 • WASHINGTON, DC

1:30 PM - 2:30 PM

## CASE STUDY: BUILDING A COMPREHENSIVE SECURITY AWARENESS PROGRAM: IF YOU BUILD IT, THEY WILL LISTEN

Kevin Mitnick said, "The methods that will most effectively minimize the ability of intruders to compromise information security are comprehensive user training and education." Security professionals agree that awareness is an important security tool, but developing and implementing a comprehensive program in a large enterprise is a daunting undertaking. Where do you begin? How do you maintain the program? The Federal Reserve has established an effective program aimed at increasing security awareness of more than 20,000 employees located all over the United States. This session will describe how to build the infrastructure and the components and resources needed to facilitate and support a comprehensive program.

Rian Campbell, Information Security; **Federal Reserve Bank**

2:30 PM - 3:00 PM

## AFTERNOON REFRESHMENT BREAK

3:00 PM - 4:00 PM

## CARRIER SECURITY PRACTICES FOR VOICE OVER IP

Protecting your Voice Over IP means following best practices in secure network design. In today's world, this demands more than placing a firewall between the LAN and the internet. In this presentation attendees will learn about the top security practices for Voice Over IP. Topics discussed include Network and Application Layer security, Session Border Control and Application Layer Firewall usage.

Steve Spak, Distinguished Member of Technical Staff; **Verizon**

4:00 PM - 5:00 PM

## HELPING CUSTOMERS PROTECT THEMSELVES

Financial services companies are continuously implementing programs and improving how they protect their customers. As a result, we are now seeing more instances where the customer's information is being taken directly from the customer and being used for electronic fraudulent activity. This is being done through phishing, pharming and the use of spyware. To help prevent this, we must now help our customers protect themselves. In this presentation attendees will learn effective methods employed to accomplish this.

They will explore all approaches to setting up a cyber defense program and learn the best ways to educate their customer.

Tim Callahan, First Vice President, Technology Risk Management and CISO; **People's United Bank**

5:00 PM

## CHAIRPERSON'S CLOSING REMARKS, Q&A AND GENERAL QUESTIONS

## CONFERENCE DAY TWO: JUNE 20, 2008

7:45 AM - 8:15 AM

## REGISTRATION AND CONTINENTAL BREAKFAST

8:15 AM - 8:30 AM

## CHAIRPERSON'S WELCOMING REMARKS

8:30 AM - 9:30 AM

## \*OPENING KEYNOTE ADDRESS\* PROTECTING THE CRITICAL INFRASTRUCTURE THROUGH THE PUBLIC-PRIVATE SECTOR COLLABORATION

With purportedly some 80 percent of the U.S. critical infrastructure under the control of the private sector, it is crucial that a high degree of collaboration and information-sharing take place between the government and the private sector. This presentation will examine questions such as who should take the lead in developing a secure cyberspace, who should participate and at what level, and what program should be instituted. Presidential and Homeland Security Directives and several national and sector National Plans have been published, putting the general guidelines in place. This presentation will examine what it will take to make the mandates and plans a reality.

C. Warren Axelrod, SVP; **Bank of America**

*Warren Axelrod is the Chief Privacy Officer and Business Information Security Officer for U.S. Trust. At U.S. Trust he interfaces with the firm's business units to identify and assess privacy and security risks and mitigate them, to have employees become familiar with security policies, standards, and procedures, and to ensure that they are followed.*

*He holds a PhD in managerial economics from the Johnson Graduate School of Management at Cornell University and honors bachelors and masters degrees in electrical engineering, economics and statistics from the University of Glasgow, Scotland. He is certified as a CISSP and CISM and has NASD Series 7 and Series 24 licenses.*

*Warren has worked in many areas of the financial services industry, at firms such as SIAC, HSBC Securities and Pershing. He is involved at both the industry and national level with security and critical infrastructure protection issues respectively. He is a member of the SIFMA Privacy Committee, SIFMA Information Security Subcommittee, FSSCC R&D Committee and several BITS risk and security working groups and has contributed to a number of SIFMA and BITS publications. He was honored with the prestigious Information Security Executive (ISE) Luminary Leadership Award 2007.*

**REGISTER TODAY!** Contact Akin Akinsanya at Phone: 414 221 1700 Ext: 137 Fax: 414 221 1900 Email: [aakinsanya@acius.net](mailto:aakinsanya@acius.net)



# CORPORATE NETWORK SECURITY

June 19-20, 2008 • WASHINGTON, DC

9:30 AM - 10:00 AM MORNING REFRESHMENT BREAK

10:00 AM - 11:00 AM CASE STUDY: IDENTIFYING AND DEALING WITH DATA LEAKAGE ISSUES: MITIGATING THE PAIN

This session will discuss the topic of data leakage and how to reduce the risks and consequences of these events. Case studies of data leakage and what could have been done to prevent them will be discussed. Attendees will also hear about the various methods of internal and external leakage and how to identify these. Additionally, they will learn the steps to minimize the exploitation of data leakage and what to do when it affects their organization.

Craig Lucca, Manager of Information Risk; **Bloomberg**

11:00 AM - 12:00 PM CASE STUDY: PROTECTING INFORMATION THROUGH STRONG ACCESS CONTROL

Logical access control is among the strongest preventative controls in protecting information assets. It is the science of ensuring that people or machines have the proper and minimum access required and ensuring unauthorized people or machines do not have access. Though important, this can be extremely hard. This case study will outline how employing an automated solution has ensured access control, compliance, and provided efficiency in managing access to networks, systems, and applications.

Tim Callahan, First Vice President, Technology Risk Management and CISO; **People's United Bank**

12:00 PM - 1:00 PM LUNCHEON AND EXHIBITS

1:00 PM - 2:00 PM

Presentation to be announced shortly

Tara Kissoon, Director of Information Security; **VISA, Incorporated**

2:00 PM - 3:00 PM CORPORATE IT SECURITY: HOW MALWARE IS GETTING DOWN TO BUSINESS

Today's malware imposes significant business risks due to the highly organized natures of its attacks; vulnerabilities over the internet have become a vital area to watch as part of any risk management program. Hackers are no longer kids trying to create a name for themselves. They are professionals with a vast network who are able to target one specific division within an entire enterprise. Many of these attacks are so stealthy that a corporate target may not even realize their machine has been compromised for days, weeks or even months. In this presentation attendees will get a better understanding of the malware ecosystem, its effects on business risk and what it means for IT security in today's corporate environment

Tom Bowers, Senior Security Evangelist; **Kaspersky Lab**

3:00 PM - 3:15 PM AFTERNOON REFRESHMENT BREAK

3:15 PM - 4:00 PM INTERACTIVE PANEL DISCUSSION

This panel will bring together security executives representing top corporations. Panelists will discuss their experiences with such issues as: enterprise security, endpoint security, security awareness, carrier security practices and malware. Further details on the panel members will be announced shortly.

4:00 PM END OF FORUM; CHAIRPERSON'S CLOSING REMARKS, Q&A AND GENERAL QUESTIONS



# CORPORATE NETWORK SECURITY

June 19-20, 2008 • WASHINGTON, DC

## CONTENT AND THEME

Cyber crime is rated the Number 3 priority for the FBI, behind only counter terrorism and counter espionage.

Nearly 672 electronic records containing confidential information are compromised every 5 minutes. These compromises are caused by internet hackers as well as internal errors. Some exposure of data is accidental, caused by administrative errors, insider abuse, stolen equipment and the like. Other times it comes from cyber thieves or disgruntled employees.

With Cyber terrorism continuing to escalate for the U.S. government and businesses of all sizes, computer experts recommend companies take the necessary steps to protect their valuable data. Some companies find it hard to justify spending money on network security, especially large amounts, however the financial burden will most likely be much higher if they don't protect themselves. Taking the necessary steps to defend themselves from hackers will not only help these companies protect themselves from criminals but also makes them less "attractive" to hackers and attacks.

Don't miss this national forum focused on exploring the most advanced and aggressive corporate network security defenses leading to a safe and secure enterprise and saving companies from financial loss and public embarrassment. It will highlight the best case studies and most advanced tools and strategies for addressing network security from top industry leaders. **Join us June 19th - 20th, 2008 in Washington, DC**, for a gathering of CSO's, CTO's, directors and managers. This two-day strategic business forum will explore security issues such as data leakage, protection for the mobile worker and company-wide security awareness programs.

## WHO WILL ATTEND:

This conference is created for security professionals of all levels including: Chief Security Officers, Chief Technology Officers, Directors and Managers representing corporations across all industries

### Key Title:

- Network Security
- Internet Security
- Information Technology
- Data Security Analyst
- Technical Operations
- Security Administrator
- Security Engineer
- Security Specialist

## CONFERENCE FEES AND REGISTRATION

Conference Fee: \$2,390 Conference Documentation CD: \$615  
(Documentation CD includes copies of all proceedings on CD and shipping is included)

**REGISTER 3 & GET 1 FREE!**

Any organization registering three persons at the same time will be entitled to a fourth registrant FREE of charge!