

14-Mar	Track 1	Track 2	Track 3
730-800	Conference Introduction		
0800 – 0900	Arnold Johnson - NIST FISMA		
0910 - 1010	CISO Panel		
1015 - 1115	Kevin Kampman – Burton Group Practical Role Management	Pete Allor – ISS Best Practices for Safeguarding your Customer Information	
1115 - 1200	Networking / Vendor Floor / Break		
1200 - 1330	Lunch / Keynote Irfan Chaudhry – Microsoft Security in the Software Development Lifecycle (SDLC)		
1345 - 1445	Bruce Aarons – CA Integrated Threat Management	Jimmy Noll – Systems Designs Group Building a Comprehensive IT Security Program	Dave Wean – Digital Controls Making Security Policies Fit
1500 - 1600	Matt Curtin – Interhack Electronic Evidence in Criminal Defense	Kevin Kampman – Burton Group Identity and Security Architecture – Why it Matters	Bill Yang - WDY Enterprises Lessons Learned from Katrina Continuity and Recovery Operations

15-Mar	Track 1	Track 2	Track 3
0800 - 0830	Breakfast and recap		
0830 - 0930	Emily Frolick – KPMG Business Continuity Management 101	Bryan Fite – Lexis Nexis Corporate Identity Fraud: When Script Kiddies Grow Up	Mike Skelton – University of Dayton Posture Assessment and Host Remediation
0945 - 1045	Mark Beckmeyer – Computer Horizons Intersection of Information Security and Business Continuity	Pat Moulder Wireless LAN Hackers	Jennifer Vallarauto - Wright Line Physical Security for Your Data Center
1100 - 1200	Keith Fricke, Business Continuity aspects of HIPPA	Marty Gillespie - Network Perimeter Defense	Gregg Gunsch – GG & Company Identity Theft 201
1200 - 1330	Irene Moore – ContinuityLink, Inc. BCP Keynote – DRP, BCP, BCM, what's the difference – What do you need to do it?		
1345 - 1445	Becky Crackel – Columbus Children's Hospital IT Recovery Assessment: How Ready Are You?	Michael Radigan – Cisco Building a Compelling Business Case for Information Security Solutions	Blaine Wilson – Reynolds and Reynolds Application Security Demo
1500 - 1600	Jody Davis-Curless – LexisNexis Business Impact Analysis – A Practical Approach	Tim Wright – LexisNexis Auditing the Network Infrastructure	

Building More Secure Information Systems: A Strategy for Effectively Applying the Provisions of FISMA

Arnold Johnson, Senior IT Security Specialist
National Institute of Standards & Technology (NIST)

The NIST FISMA Implementation project is the development of a suite of Federal Information Processing Standards (FIPS) and guidelines that support the implementation of FISMA and associated OMB requirements. The presentation will include a top level view of the project, how it applies to FISMA, and a brief overview of the key FIPS and guidelines supporting FISMA.

Practical Role Management - How Roles Support Access and Authorization, and How to Develop Effective Roles

Kevin Kampman, Practice Manager and Senior Consultant
Burton Group

The adoption of the recent ANSI standard for Role Based Access Control (ANSI RBAC), the need to provide accountability regarding authorization to resources, and the desire to streamline resource provisioning implementations have resulted in a renewed interest in RBAC in organizations. Developing a role management strategy and approach, however, can be a daunting challenge. ANSI RBAC is theoretical in nature, has limited adoption in applications, and RBAC itself indicates the need for a lifecycle management approach to roles in the enterprise. Learn how organizations are tackling roles, discover approaches and alternatives, and hear recommendations about how to initiate a roles program for your organization.

Best Practices for Safeguarding your Customer Data

Pete Allor, Manager, X-Force Threat Intelligence Services
Internet Security Systems (ISS)

Audience members will learn:

- How multi-national cyber-crime syndicates use state-of-the-art techniques to steal data
 - What questions to ask your staff about your data security
 - How to prevent Spyware and its impact on your network
 - How to recognize and avoid Phishing attacks
 - How improved security will protect your reputation, brand and bottom line
-

Keynote Presentation

Security Development Lifecycle – IT

Irfan Chaudhry, Group Program Manager, Application Consulting and Engineering
Microsoft Corporation

A key aspect to building secure applications is the integration of security into the Software Development Life Cycle (SDLC). This session provides an overview of the Security Development Lifecycle-IT (SDL-IT) implemented within Microsoft. SDL-IT is focused towards Microsoft's mission critical line of business applications and is a process that Microsoft has leveraged over the last four years to review more than 1000 applications.

Malware Convergence: From Point Security Solutions to Total Threat Management

Bruce Aarons, Senior Security Solution Strategist
Computer Associates (CA)

The security market is fractured, with a few point-vendors dominant around point solutions. In spite of trends and pressure, the Threat and Malware defense markets continue to balkanize, to increase costs and have effectively demonstrated the same characteristics of markets under monopoly. All that is changing with the advent of new threat types and new players.

Building Security Program Regulatory Requirements

Jimmy Noll, Senior Technology Consultant
Systems Design Group

Is your organization “secure enough”? Find out how to ensure regulatory compliance and appropriate information security by building a security program that addresses prevention,

detection, response and recovery. Determine what you need to implement effective and efficient security controls. From end-user computing to applications, storage, networking and servers, you'll see why a comprehensive, straightforward model for your company is a necessity and can make complying with Sarbanes-Oxley, GLBA, HIPPA and other regulatory mandates easier.

Electronic Evidence in Criminal Defense

Matt Curtin, Founder
Interhack Corporation

Many have wondered who is policing the Internet. Law enforcement is, in fact, actively developing cybercrime investigation capability. Digital evidence is new to the legal system; this talk will discuss a real criminal case: its investigation, prosecution, and defense from the speaker's own forensic computing practice.

Federated Identity

Kevin Kampman, Practice Manager and Senior Consultant
Burton Group

As organizations bridge identity to extend their data and privileges to others internally and in the extended enterprise, the use of federation capabilities for access management is becoming more common. In this session, we'll discuss the state of the federation marketplace, how organizations are establishing a federation infrastructure, the enabling standards, and initiatives that are bringing federation into the mainstream. In addition, we'll discuss the barriers and recommendations for how to proceed with your federation initiative.

Business Continuity Management 101

Emily Frolick, Manager, Risk Advisory Services
KPMG LLP

What is Business Continuity Management: Terminology Definitions, Historical Information, Levels of Preparedness. Phases in developing a Business Continuity Plan, the importance of a thorough Business Impact Analysis, prioritization of key business processes to include in continuity plans, and recovery criteria to consider as plans are developed. Discuss the difference between Business Continuity Planning and Disaster Recovery Planning. Discuss highlights of best practices in Business Continuity; summarize results of recent Benchmarking study conducted by Continuity Insights and KPMG (Factors influencing Business Continuity Management Programs). Discuss practical examples of documented procedures used to continue critical business processes during a disaster and while system recovery and resumption is in place."

Corporate Identity Fraud – When Script Kiddies Grow Up

Bryan Fite, Global Security Architect
Reed Elsevier

Have you ever wondered why there are fewer outbreaks of malware with destructive payloads but more SPAM then ever flowing through port 25? We will examine the evolving face of eCrime, G-Commerce and the underlying economic forces that are transforming misguided hobbyists into International criminals for hire.

Posture Assessment and Host Remediation

Mike Skelton, Principle Architect
University of Dayton

With the many roles a university network must play and the various needs it provides to it's customers, how can functional security be implemented? This session will discuss the various methods available to ensure hosts meet minimum security standards as well as the manner in which the university chose the best fit for it's environment. Additionally, a network admission system can compliment many other security and network devices, such as firewalls, intrusion detection systems, intrusion prevention systems, and even QoS devices. The session will also cover the university's implementation plan for a network admission system and how such a system can provide maximum functionality while complimenting such devices.

Intersection of Information Security and Business Continuity

Mark Beckmeyer, Information Security Practice National Director
Computer Horizons Corp.

The presentation will provide an in-depth discussion on the relationship of Business Continuity Planning in developing a comprehensive information security (IS) program. The focus will include an emphasis on the "Availability" facet of an organization's IS program and how it relates to the two other facets, i.e., "Confidentiality" and "Integrity". Specifically, we will discuss assessing the criticality of business functions and information technology (IT) functions as it relates to protecting the overall security posture of an organization. We will also discuss how an IS program will have an effect on other Business Continuity Planning issues such as selecting recovery strategies, plan development, testing and training.

We will discuss how to initially incorporate Business Continuity Planning into the overall design of an organization's IS program and where it will need to be reviewed and updated. Additionally, we will look at how to design and establish a Business Continuity Planning entity within the organization and how it will operate. The objective of this presentation will be to give the audience a clear understanding of how Business Continuity Planning is an essential aspect of establishing and maintaining a comprehensive and effective IS program.

What You Really Need to Know About Wireless LAN Hackers

Pat Moulder, Principle Security Engineer
ManTech Security and Mission Assurance

This presentation will cover the skills, and hacking tools that hackers use to exploit vulnerabilities in 802.11 wireless LANs. The information presented is a set of already known vulnerabilities and risks to wireless LANs. This presentation will provide a good understanding of hacker tools, techniques and vulnerabilities. The information presented here on wireless exploits will allow home wireless users and security managers to take proactive steps to properly mitigate the security risks in corporate and home wireless networks

Physical Security for Your Data Center

Jennifer Vallarauto, Senior Account Manager
Wright Line

Brad Dyke, Former Network Administrator, MSG/Region 9

In working with high security data centers both commercially and at government facilities, there are many weak spots in the physical design of data centers that lead to breach of security, network downtime, and network failure. Through the successful design and redesign of data centers, we focused on the physical characteristics to eliminate existing issues and prevent future incidents.

What Elements Make Up A Good DR Program?

Keith Fricke, Data Security Administration
Cleveland Clinic Health System

Topics covered include getting back to basics, creating a disaster recovery life cycle, developing a quick start guide and creating a testing program. Keith's presentation also includes a technical discussion of how testing led to an innovative solution for recovering their Active Directory infrastructure after experiencing numerous technical difficulties using traditional recovery methods.

Network Perimeter Defense – An Overview

Marty Gillespie, System Security Engineer
ManTech Security and Mission Assurance

In this "Defense-in-Depth" course, an overview of current network perimeter defense strategies to include firewalls, load balancing, server farms, wireless access, web security issues and intrusion

detection will be provided to prepare the audience with the basic tools to understand the overarching principles of network perimeter defenses.

Identity Theft 201

Gregg Gunsch, President
GG & Company

Identity Theft – fraud performed using another’s personal information as cover – has received abundant, well-deserved, yet simplistic media attention aimed at the masses. This session will explore several less-familiar approaches to acquire your personal information, conduct in-depth analyses of phishing and pharming, and present resources to aid with recovery.

DRP, BCP, BCM, what’s the difference? What do you need to do...?

Irene Moore,
ContinuityLink

Review of various terms and definitions used in the BCM world, along with history of the BCM industry. The overall Business Continuity Program Implementation Cycle will be discussed, along with success factors and challenges that organization face when implementing it.

IT Recovery Assessment – How Ready Are You?

Becky Crackel, IS Disaster Recovery Program Coordinator
Children’s Hospital, Columbus OH

A session designed for those interested in measuring and managing IT’s Recovery Readiness. Recovery Assessment is both risk analysis and GAP analysis, measuring IS readiness to recover systems. This seminar explains its place in the CP methodology, how to conduct a Recovery Assessment, and develop measures for your DR program.

Building a Compelling Business Case for Information Security Solutions:

Michael Radigan, Security Business Consultant
Cisco Systems

Every dollar of your budget is ultimately weighed against the value it could bring if invested in other aspects of the business. This is most apparent when your projects are competing for funding approval from business leaders. How can you build a credible business case and gain internal support for your initiatives? Can you define and articulate the business value in terms the decision makers will understand? Attendees will learn how to position their projects for executive sponsorship, understand the value assessment methodology and know the elements required to create a compelling business case.

Under the Hood – How an Attack Works

Blaine Wilson, Technical Systems Engineer
Reynolds and Reynolds

Technical discussion of how common attacks work and steps to take to reduce the risk. Common attacks (buffer overflow, SQL injection, cross site script injection, decompiling and memory reading) will be introduced, explained, demonstrated, and mitigated.

Business Impact Analysis – A Practical Approach

Jody Davis-Curless, Business Continuity Manager
LexisNexis

Your recovery strategies are only good if the requirements used to drive the strategies are solid. The Business Impact Analysis is the foundation for determining those business requirements. Join this session to hear about how to approach a BIA that results in strong, business supported requirements. The approach to be discussed has been proven effective for LexisNexis disaster recovery strategy planning and implementation.

Auditing the Network Infrastructure

Tim Wright, Network Services Security Auditor

LexisNexis

During this presentation we will discuss how an engineer can create an audit process that reviews the network infrastructure for risks. Also, we will discuss techniques that are used to discover unwanted or un-needed services and protocols that are running within the network fabric.

Several of the key topic areas include routing protocols, VLAN's, SNMP, TFTP and how to mitigate risk associated with these services. We will also discuss how network systems that have been improperly secured can lead to a system compromise.

How to Develop Security Policies that Fit

David Wean, Systems Engineer, Digital Controls

Discuss the following concepts:

- Areas of threats and vulnerabilities
 - Current security strategy practice assessment
 - Security Models and Policy Requirements
 - Levels of Control
 - Policy Creation, Implementation and Enforcement
-