The University of Findlay

7th Annual Information Assurance Forum:

Smart Beginnings

Wednesday, October 29, 2008, 9:00 AM – 3:30 PM
North Multi-Purpose Room, AMU

Sponsored by:
The Center for Information Assurance Education (CIAE)
The Area of Technology Management
The Technology Infrastructure Committee (TIC) of GreaterFindlay, Inc

9:00 - 9:15	**Introductions** **Forum Agenda** **Certificate Presentations:** *Travis Clark, Jonathan Eisenhart, Jon Hutman, Jason Ruhlen, Michael Shaffer,* and *Drew Snow*
9:15 – 9:30	***"Demographics & Computer Information"*** David Greenslait, Erik Birkholz, Jessica Sheline, Zac Utendorf, Lora Williams
9:30 – 9:45	***"Enterprise Resource Planning (ERP) & Small Business"*** Tanya Smith, Leanna Jahr, Luong Tong, Monica Miller, Andy Smith
9:45 – 10:00	***"The Importance of a Business Plan"*** Josh Fox, Garrett Allwes, Curtis Haggard, Kelly Beamer, Jill Beining
10:00 – 10:15	***"Flood Implications on Business"*** Stephanie Heydinger, Laurie Neiling, Whitney Best, Natasha Brinkman
10:15 – 10:30	***"Computer Protection – Is It Worth It?"*** Essex Berry, Raechel Vaughn, Erik Chapin, Brant Finney
10:30 – 10:45	***"Data Backup & Company Preparedness"*** Meryl Olson, Matt Weber, Daniel Williams, Megan Thomson, Mike Roach
10:45 – 11:00	(Break)
11:00 – 11:50	"***The Oops Factor – Accidents Do Happen***" Mitchell W. Brown, Senior Solutions Architect, Open Systems Technologies
12:00 – 12:50	Lunch Presentation ***"Turning a Liability Into an Asset"*** Anthony P. Iriti, NW Ohio Flood Mitigation Partnership
1:00 – 1:50	"***The Big One –How to Prepare for and Recover from a Big Disaster***" Mitchell W. Brown, Senior Solutions Architect, Open Systems Technologies
1:50 – 2:00	Break
2:10 – 3:00	"***Using A Taxonomy to Analyze Recent Data Losses***" Lee T. Ayres, CISSP, Interhack Corporation
3:00 – 3:30	Wrap up & Networking

RSVP Lunch Reservations to – Bev Roth 419-434-4637 or roth@findlay.edu
Office of Computer Science and Technology Management

The Oops Factor – Accidents Do Happen
Mitchell W. Brown, Senior Solutions Architect, Open Systems Technologies

This session will take a somewhat humorous track discussing accidents that have happened in IT organizations and their aftermath. This session will show, using examples, how the human factor integrates into our disaster preparedness plans, and how to evaluate the risk/reward of preparing for such disasters. This session paves the way for a more complete discussion on preparing for disasters in "The Big One".

Turning a Liability Into an Asset
Anthony P. Iriti, President, NW OHIO Flood Mitigation Partnership

How our organization came together, where we are today, and where we are going. This session will share information regarding the work of the Flood Mitigation Partnership and progress made to date. In addition, Tony will provide insights regarding the result of the flooding upon business along with how information assurance applies to protect professional and personal assets in order to assure continuity of business during disasters such as floods.

The Big One – How to Prepare for and Recover from a Big Disaster
Mitchell W. Brown, Senior Solutions Architect, Open Systems Technologies

Disasters come in many forms; natural disasters, regional problems, accidents, terrorism, etc. In this session we will discuss how to evaluate the risks facing your IT enterprise and how to evaluate and quantify these risks so you can determine how to prepare for and respond to disasters. We will focus on two main topics: how to determine if your business should or should not prepare for a particular type of disaster. Secondly, we will discuss the major elements required to successfully prepare and recover from a disaster.

Using A Taxonomy to Analyze Recent Data Losses
Lee T. Ayres, CISSP, Interhack Corporation

Malicious hackers tend to steal headlines, but do their stories correlate to the threats that are most prevalent in your industry? Reviewing a selection of publicized security incidents from 2005-2007, we propose a taxonomy of breaches based on the concept of the threat/vulnerability pair. We explore the proportion of incidents of each type in several broadly defined industries, followed by analysis and discussion of effective technical, procedural, and administrative controls. The data and analysis provided will assist business leaders in making informed decisions regarding the distribution of limited information security assets.