Overview
Concurrent Technologies Corporation’s (CTC’s) Cyber Exercise is a three-day event designed to enhance the skills of network administrators in identifying and responding to cyber attacks in a near real-world setting. The exercise is conducted in a network enclave, which has been customized to mimic the network the participants encounter on a daily basis.

The Cyber Exercise places the participants in the role of the Network Defender. The Defenders are responsible for protecting the network enclave against the threat of cyber attacks. Through ongoing progress reviews by the observing team, the Defenders are guided throughout the exercise. As the effectiveness of the Defenders improves, events can be tailored to challenge them. The Defenders are evaluated on their ability to identify attacks and effectively counter against them.

Purpose
The purpose of this activity is to provide an exercise in which an organization’s security administrators are presented a “safe” environment where they can gain experience defending against network attacks. During the course of the Cyber Exercise, scenarios involving potential threats to a network enclave and depicting the real-world constraints that affect the decision process are presented to the participants.

Participants make decisions and initiate responses to protect servers, administrator workstations, user workstations, and network infrastructure components. The scenarios are selected based upon the participant’s network infrastructure and security policies. Working through these scenarios enables the participants to make critical decisions in a non-threatening environment.

Upon completion of the Cyber Exercise, participants will have increased skills in:
- Identifying potential attacks in progress
- Post-attack incident analysis
- Implementing preventive countermeasures for specific attacks
- Identifying vulnerabilities within a network
- Implementing solutions to protect network infrastructure
- Evaluating platforms for deploying new technologies
- Sharing lessons learned with other network administrators.

Target Audience
The target audience for the Cyber Exercise is Network and System Administrators who have been chosen to provide Network Security for an enclave network. The target audience may or may not have formal training on how to handle cyber attacks.

The Cyber Exercise is designed to accommodate participants with varying expertise levels within different security domains. Continual feedback during the exercise allows the observing team to tailor the scenarios to best challenge the participant’s capabilities.
Schedule
The Cyber Exercise takes place over the course of three days. A general course schedule includes:

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day 1 AM</td>
<td>Cyber Exercise Orientation</td>
</tr>
<tr>
<td>Day 1 PM</td>
<td>Network Analysis</td>
</tr>
<tr>
<td>Day 2 AM</td>
<td>Discover Probes</td>
</tr>
<tr>
<td>Day 2 PM</td>
<td>Network Compromise and Attack</td>
</tr>
<tr>
<td>Day 3 AM</td>
<td>Network Recovery and Forensics</td>
</tr>
<tr>
<td>Day 3 PM</td>
<td>Hot-Wash Session</td>
</tr>
</tbody>
</table>

In addition, participants will leave the Cyber Exercise equipped with a resource of reference materials to take back to their organizations.

For more information on CTC’s Cyber Exercise contact:

Kenneth Sweltz, CISSP, PMP  
Director, Assured Information Solutions  
(814) 269-2576  
sweltzk@ctc.com

Steven Tomasko, CISSP, PMP  
Manager, Emerging Solutions  
(814) 269-2671  
tomaskos@ctc.com

www.ctc.com