

Fall Newsletter 2007 -- Continuum Worldwide

**Insider Threats: We met the enemy and they are us.**

By: Don Kohtz, Director of Investigative & Compliance Solutions

The title sounds like some scary horror movie, the name of a rock album, or Stephen King's latest novel. Unfortunately, I'm referring to the sanctity of the environment most of go to everyday – our workplace.

Threats: External vs. Internal

A “threat” is commonly known as an indicator of danger or other harm. When I hear the word “threat” it conjures up thoughts of people from outside an organization attempting to do bad things to an organization, like corporate espionage or using a Trojan horse to disable a network with a virus. Stealing corporate trade secrets, customer lists, drug formulas, undisclosed news about a forthcoming merger and acquisition can be done by an “external” source, but it's much easier accomplished by someone inside the organization. An internal employee does not have to penetrate the physical security levels of the organization. The internal employee may not even have to penetrate the information security layers established by an organization, if they engage in a little social engineering to dodge the traps and landmines of the security features of their company's network.

Once we really start thinking about it, insider threats are all around us. Some organizations look the other way; for others, it hasn't even crossed the minds of some C-level officers that their own employees or business partners are risks; and other organizations have implemented a risk mitigation plan addressing “insider threats.”

Risks We Face Today In the Workplace

**Bully's in the Workplace**

Have you ever worked with a bully? A bully is someone who is arrogant, loud, pushy, abrupt, abusive, mental states ranging from highs to lows, hard to get along with, not a people person? Do we worry how long will we have to put up with the bully at work until he blows his top? All too often we turn on the 6:00 O'clock news and hear of violence in the workplace. The workplace used to be a safe haven, a place we go to everyday to make a product or provide a service and then go home. What is the bully likely to do when he blows his top? When an organization recognizes they have a bully, what should they be doing?

**Dating**

If you read the newspapers of the small cities here in Nebraska, they usually have a section for Engagement Announcements. In the announcement of the joyous occasion, the couple will list where each other works or their line of business. Many times the couple works together at the same organization. Does your company have a policy

addressing dating of co-workers? Does your company allow Managers and Supervisors to date people they manage? Do you have C-level officers within your organization dating employees? What are the risks associated with employees dating one another? Will each dating situation have a happy ending like in the fairy tales? Probably not. Then what happens, and who is at risk from the fallout---the employees or the organization? What other workplace issues place organizations at risk?

### **Security Policies & Procedures**

At new employee orientation, most organizations have new employee's sign that they will abide by the organization's information security policies and procedures (ISPP). Most ISPPs address the Email system and inform the employee that they have no expectation of privacy associated with the organization's Email, networks, and applications. Email today is out of control. Some people are declaring email bankruptcy and deleting all their emails. In the course of all the emails we send and receive at work, have you ever gotten a joke, picture, cartoon, or video clip someone else thought you might enjoy, but it had unwanted sexual or racist overtones that you deemed inappropriate. Do your employees have access to network drives or systems that they have no business having access to? Even if you have a policy addressing user access to systems for business purposes only, do you enforce it; do you monitor or conduct audits to determine if the policy is being followed?

### **Employees Conducting Their Personal Business at Work**

Are your employees doing their personal investing at work? Are they running a second business from their cubicle using the organization's email and phone system? Are your employees cutting and pasting from your proprietary documents stored on your company network and sending data outside the walls and doors of your company? Does your organization monitor the computers of individuals who have given their 2 week notice to prevent confidential or proprietary data from leaving the organization when it shouldn't?

### **Senior Level Executives**

Does your organization protect its C-level officers, board of directors, or other highly compensated employees by monitoring the content of data they send and receive. If not, why not? Is someone internally or externally extorting or threatening your C-level officer, a board member, or a highly compensated individual? By managing insider threats, i.e., monitoring the content of inbound and/or outbound emails and other use of the systems, an organization can detect, prevent, block, deter, or place someone on alert that there is an incident that is in violation of your organization's security policies. The violation may have been accidental or it may have been intentional. If an external violation was detected, it may have been targeted or it may have been random.

### **Reality**

Will we come home at the end of the day with a business to go back to in the morning? This may sound crazy, but not too long ago in the United States, we experienced the

collapse of a business called Enron, in its prime, one of the most powerful energy companies in North America.

Are you tired of seeing another business, college, or governmental agency on the 6:00 O'clock news the victim of another security breach? What constitutes a security breach? Who is tracking all this data? What do you if your organization is breached? How do you prevent security breaches? Are you ever safe from internal (accidental, intentional) or external breaches (targeted, random)?

We could go one for pages about the various risks organizations face today in the workplace. What we don't know will cost us.

### Educate Yourself

To prevent some of the harm and address the risks mentioned above, Continuum Worldwide is holding an educational Summit: **Insider Threats in the Workplace**

### CONTINUUM WORLDWIDE --- Insider Threat Summit

When: October 23, 2007  
7:30am – 4:30pm  
6.5 hours of CPE

Where: Holiday Inn (72<sup>nd</sup> & Grover) Omaha, Nebraska

Why: What we don't know will cost us

What: Speaker Line-Up

- Registration and Continental Breakfast
  - 7:30am ---8:30am
- Jeffrey Schreiner, President of Continuum Worldwide
  - 8:30am---8:40am, Opening Remarks
  - Operational Risk Management (past, present, and future)
- Lee Pierce, Consultant of Continuum Worldwide
  - 8:40am---8:45am
  - Setting the stage for the Summit
- Gary Plank, Plank Forensic Services
  - Workplace Violence: Prevention is Everyone's Responsibility
  - 8:45am---10:15am
- Break & Networking
  - 10:15am---10:30am
- Bob Lepp of McGill, Gotsdiner, Workman & Lepp, P.C., L.L.O.
  - Inappropriate Relationships & Disciplinary Matters
  - 10:30am---12:00pm

- Lunch, 12:00—1:15pm
  - Lunch Speakers: Craig Lambson & Cristina Ciovia of Oakley Networks, Inc.
  - Workplace Technology: Managing Insider Risks
- Break & Networking
  - 1:15pm---1:30pm
- Bob Kirchner of R.L. Kirchner & Associates, Inc.
  - 1:30pm---3:00pm
  - Forensic Accounting: The CSI of Accounting
- Break & Networking
  - 3:00pm---3:15pm
- William Dixon & Don Kohtz of Continuum Worldwide
  - Security Breaches: Lost Workplace Information is Just a Click Away
  - 3:15pm---4:00pm
- Don Kohtz & Lee Pierce of Continuum Worldwide
  - 4:00pm—4:15pm
  - Wrap Up

How: Please go to our website to **register at [continuumww.com](http://continuumww.com)**

- Seating is limited
- This Summit caters to all levels of expertise
- You have the opportunity to ask these renowned speakers for tangible solutions to reduce your organization's risks