Friending Your Life Away

Ira Winkler, CISSP

Codenomicom

Session ID: EXP-203

Session Classification: General Interest

RSACONFERENCE2012

It Would be Easy to do a Presentation on Stupidity

- This is an issue that has been around long before Facebook or Twitter
- Facebook and Twitter are just more known at the moment
- Fundamentally people are people
- The younger generations are more likely to have a different version of privacy
- Current technology just allows stupidity to travel faster
- Allows for abuse faster

Responsible Use, Not No Use

Unfortunately…

- The harm might be to the individual making the mistake
    - I don’t care about this
- The harm can easily be to third parties
- This is what matters to me
- One indiscretion can affect millions
- One indiscretion can be a matter of life and death

Historical Perspective

- BBS
- IRC
  - Still in use
  - Birthplace of Anonymous
- Usenet Newsgroups
- Mailing lists
- Compuserve, AOL
- Dating sites
- Blogs

Cybercrime Enabled

- Usenet created the ability for online relationships
- This enabled cyberstalking
- People posting corporate info created a potential for computer and IP compromise
- Started making the work of criminals easier

The C4I-Pro List

- All intel experts
- Custom to put out your bio
- I thought it was strange
- Someone from China posted
- I commented that it was a bad idea to post intel backgrounds
- Was flamed about my comments being against the open nature of the group
- No show of support

Companies Are Afraid to Comment

- Companies afraid to comment about activities off company time
- Afraid to play Big Brother
- Companies didn’t create policies
- Some consultants advised companies to let all their employees comment on the Internet
- Basically, unless it’s porn, it’s OK.

Are Companies Dumber Than Employees?

- They are putting info out as quickly as the employees
- Marketing putting out information, while security is told to stay away
- It’s not just companies
- USS Briscoe (?) posted crew information after attacking al Qaeda

MySpace Started a Trend

- MySpace started adding pictures
- People started talking of plans in advance
- Wholesale release of information
- Took level of embarrassment to a whole new level
- Started employers doing research on employees
- Again, hesitant to talk to current employees

YouTube

- Became the second most popular search engine behind Google
- Videos went up destroying lives

Twitter Brought Things to a New Level

- Almost the ultimate in vanity
- People started to announce every aspect of their life
- People started to write things at will
- No consideration to context or repercussions
- Too easy to distribute pictures
- Flash crimes

Other Viral Sites

- “Dog Poop Girl”

Facebook

- Became a Killer App
- Is essentially the embodiment of everything wrong and right with all other social media
- Farmville and Zynga as a whole tells us how people waste their time
- What people post is scary
- It places themselves and, more important, others at risk

The Ones I Really Worry About

- FourSquare
- TripIt
- Blippy- WTF???
  - I will never figure this one out
- Google Latitude
- Lovestruck
- Datesnearme
- Skout

Google

- Refer to my Is Google Evil? presentation
- YouTube has your age and proclivities
- Google knows what you are thinking
- Calendar knows where you will be and who you will be with
- Latitude knows where you are
- Checkout knows what you are buying
- Gmail knows your friends
- Google Apps knows your business

LinkedIn

- LinkedIn is limited, but has specific information that can be used for social engineering purposes
  - Used by APT for targeting
  - Education, employers, coworkers, titles, interests, travel, etc.
- Beginning social networking ability with discussions, groups, etc.
- Beginning to use Facebook like ads with your info
- Can tell when someone is looking for a job by new connections and referrals

Data Aggregators

- There are a lot of services out there that can put together a profile based on Social Networking sites
- Google can almost be an aggregator
- Can put together friends, family, business, interests, etc
- Maltego for example
- Icanstalku.com
- Pleaserobme.com

icanstalku.com

UGOsweeps: I am currently nearby http://maps.google.com/?q=40.7635,-73.9823333333

less then a minute ago · Map Location · View Tweet · View Picture · Reply to UGOsweeps

kerrysimon: I am currently nearby http://maps.google.com/?q=36.1146666667,-115.193666667

1 minute ago · Map Location · View Tweet · View Picture · Reply to kerrysimon

faraichideya: I am currently nearby http://maps.google.com/?q=31.9493333333,-111.866666667

4 minutes ago · Map Location · View Tweet · View Picture · Reply to faraichideya

fragileheart: I am currently nearby http://maps.google.com/?q=43.6411666667,-79.422

6 minutes ago · Map Location · View Tweet · View Picture · Reply to fragileheart

Implications of Location Posting Services

- Business locations
- Knowing where you are
- Knowing where you are not
- Do you really want the world being able to track you?

Facebook/Social Network Enabled Crimes

- Documented cases include couple in Indiana, family in Arizona
- Recent criminal posting that he actually did rob a house in Oregon
- In previous case, they IDed the perpetrator as a recent Friend
- Probably many other cases but hard to track
- “Not a Harvard graduate” posting pictures of kid duct taped
- Ashton Kutcher catching Twitter hacker through FourSquare

Notable Crimes

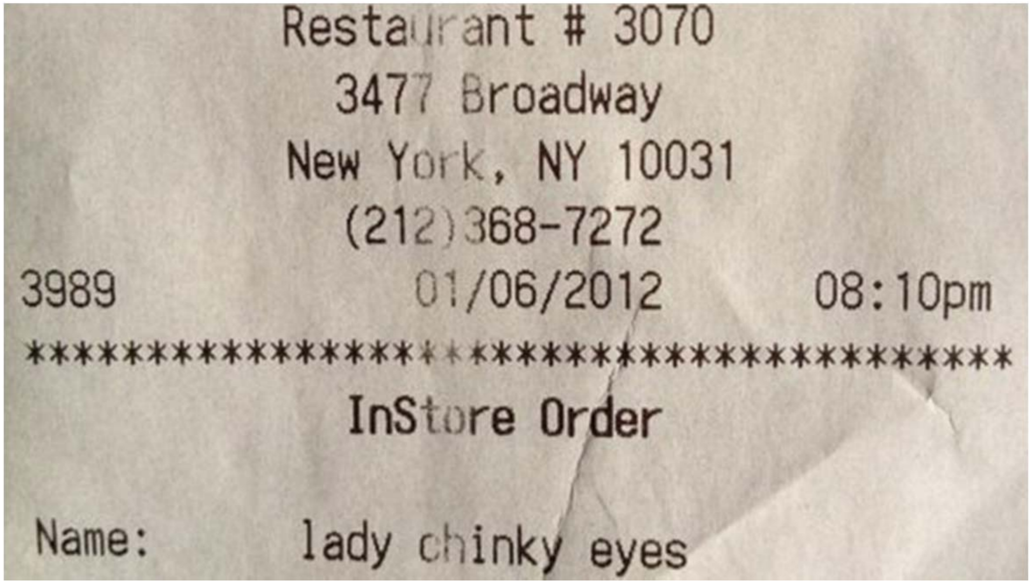
- APT Attacks LinkedIn enabled
  - Use LinkedIn for spear phishing targeting
- Twitter Hack
  - Used Social Media to guess Yahoo! password reset question
- Sarah Palin Hack
  - Used Social Media to get answer to password reset question
- Hugh Thompson
  - Scientific American article to reset bank passwords

More Serious Issues

- Israeli Military
  - Soldier posted location of an upcoming raid
- McConnell Gubernatorial Campaign
  - Web designer tweeted that he was working on a website prior to formal announcement
- Wife of British Intelligence operative posting issues on social media

Employee Issues Go Viral

- Fedex delivery guy video
- UPS delivery guy video
- Papa John’s



Restaurant # 3070
3477 Broadway
New York, NY 10031
(212)368-7272

3989 01/06/2012 08:10pm

****

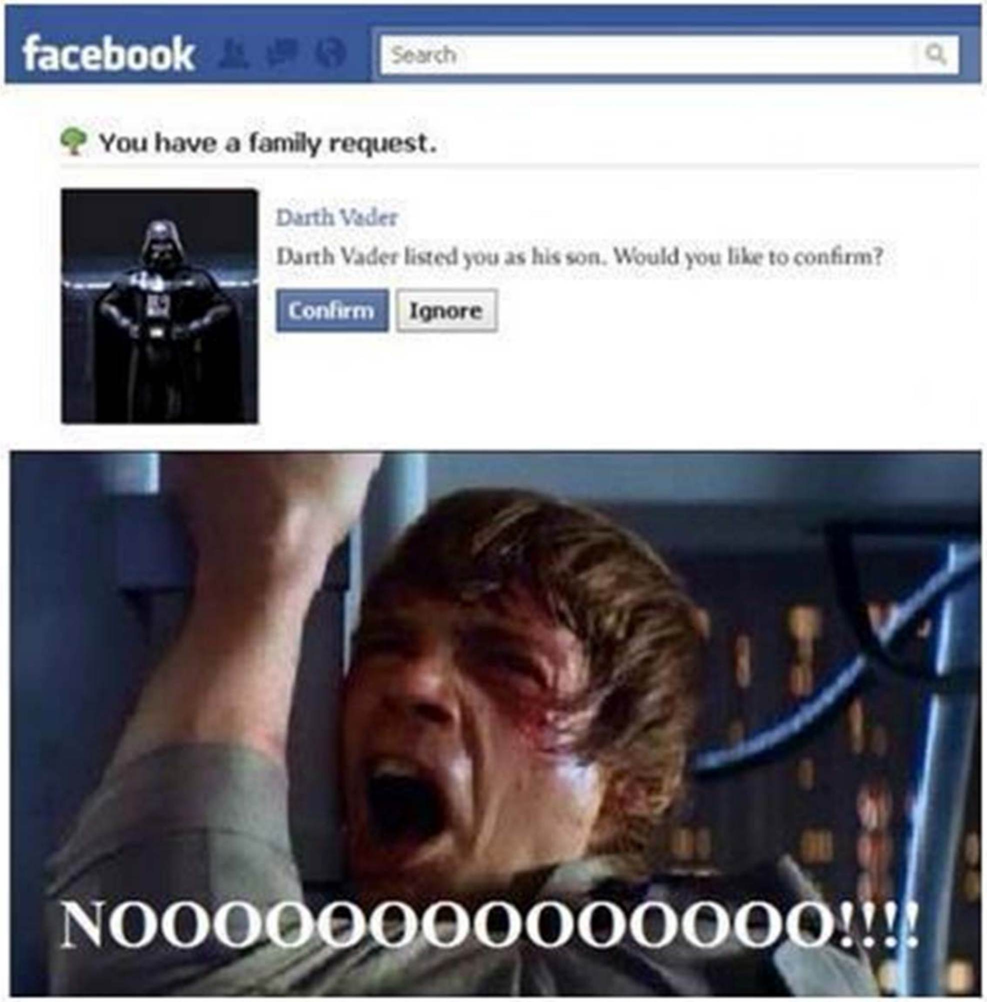
InStore Order

Name: lady chinky eyes

Third Party Indiscretions

- Posting Bachelorette party photos, tagging bride, and ruined wedding
- Constant posting about other people to appear unprofessional

Other People Posting About You



You have a family request.

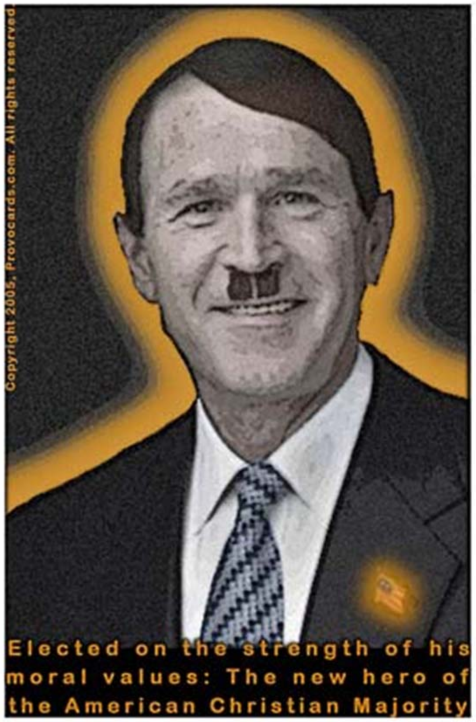
Darth Vader

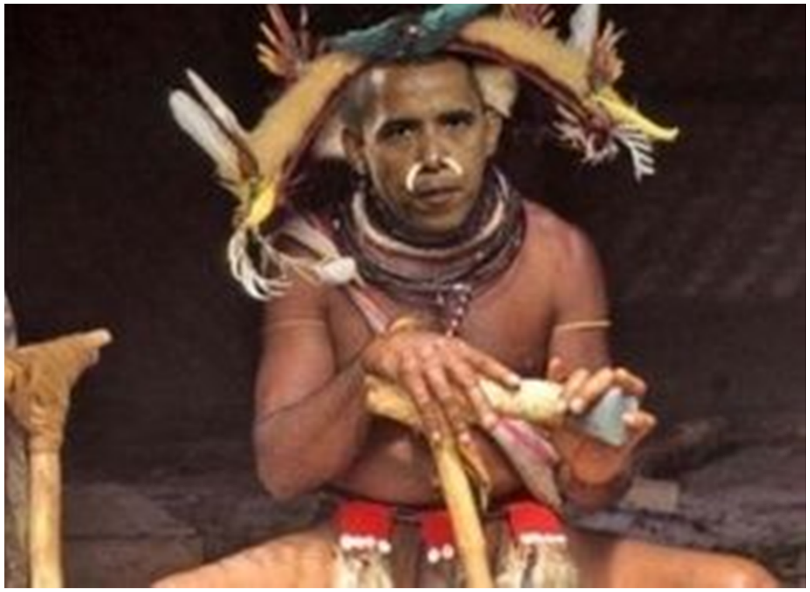
Darth Vader listed you as his son. Would you like to confirm?

Business Implications

- Do I want to know about your psychological disorder?
- Can I sit down across from you professionally, when you express extreme political or social views?
- Does your company have a right to temper your behaviors that can impact your customer interactions?
- What is the implication of your off hours?
- What is your brand?

Consider If These are on Your Profile


Copyright 2005, Provocards.com. All rights reserved.
Elected on the strength of his moral values: The new hero of the American Christian Majority



Security People as Bad as Others

- Implications of lack of professionalism
  - More interested in fighting each other than the bad guys
  - Much more than in other fields
- Maybe even indicate psychological problems
- You would think security professionals realize that that Twitter is not a closed forum and lasts forever
- Shows questionable proclivities
- Shows desire to associate with hacker underground
- Easy to violate ethics codes

Tweets About Me

- Idiots watch whole presentation they supposedly hate – Consultant/college professor and industry association board member

WOW! The first bit of truth in Ira Winkler's presentation is on 48:35. "I guess they want me to be useful for a change“

That presentation had me baffled too, painful to watch. This time I'll try to get through it. I walked out in person.

- **Wouldn’t a normal person not watch?**

Malware Introduction

- Malicious links via Twitter, Facebook and other sites
  - Short URLs
  - Easy to post, send and IM
- Malicious ads in Facebook
  - Embeds malware, even if Facebook denies it
- Introduction to malicious websites

It is More Than Security

- Lost productivity is immense
- I personally lose too much time if I leave Facebook on
  - I even make a lot of money via Facebook
- IMs less time efficient than calling, but allow for non-work related calls
- Brand image can be ruined

This is Still Nothing New

- Despite the recent incidents, this is nothing new
- Yes, I gave a history of the Internet
- We need to learn from the past to see what can be successful now
- Again, expect the same to be transmitted faster

Boils Down to Operational Security

- Companies frequently don’t have a social media policy
- They don’t want to interfere with their employees’ private lives
- US military even afraid to set a strong policy despite problems
- Companies afraid to even stop Facebook access

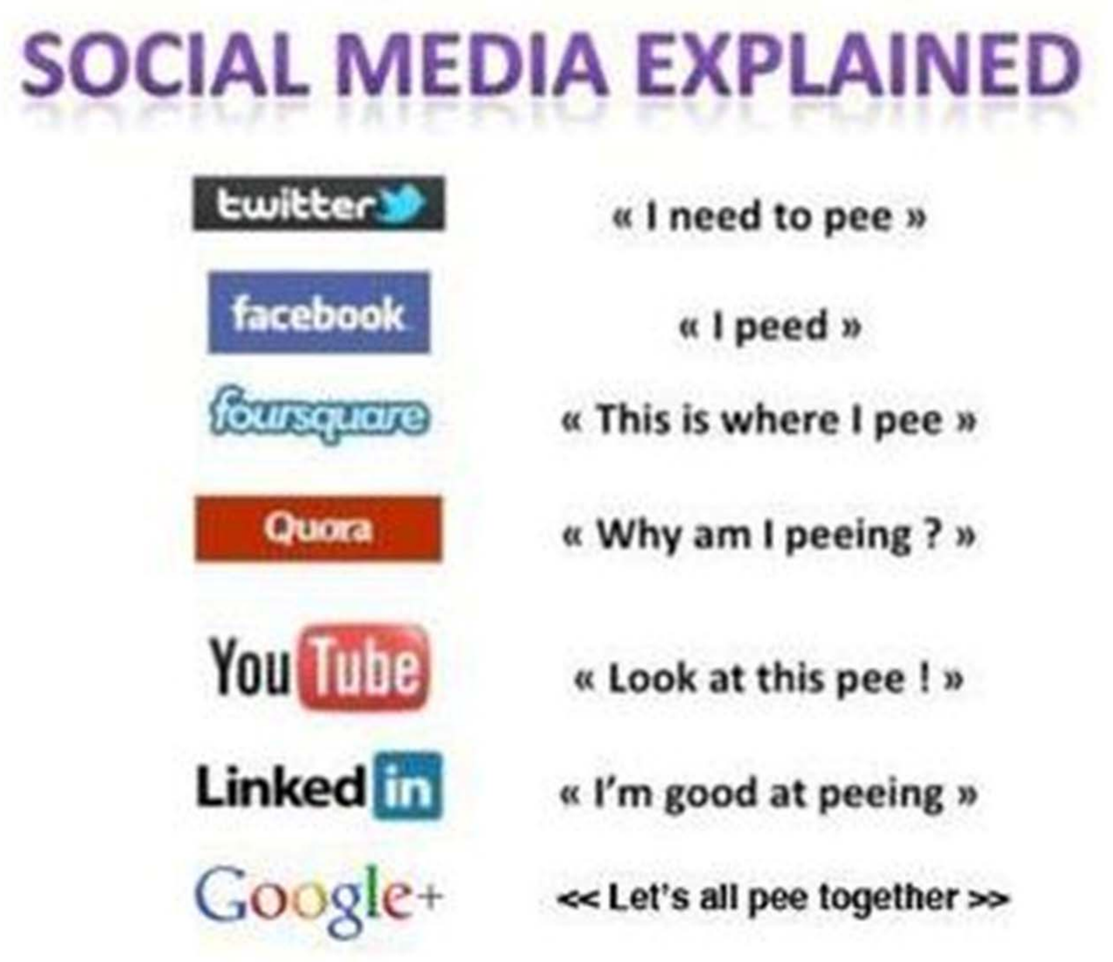
Is the Job Market That Good?

- Companies afraid that if they don’t allow Facebook and IM, they are going to lose young employees
- Do you really want an employee who cares more about social networking than their job?
- How much does social networking really help most positions?
- Again, it is OK if there is a use for it

Responsible Use, Not No Use

- Ban Social Media unless required at work
- Stress and enforce ban against discussing work related issues outside of work
- Enforce the policy as you need consistent enforcement or it is technically unenforceable
- Awareness programs that rely on employee self-interests, as they overlap with yours
- I really wish there was more to say, but the problem is that there is more a lack of will to do things right
- There are worse things than porn

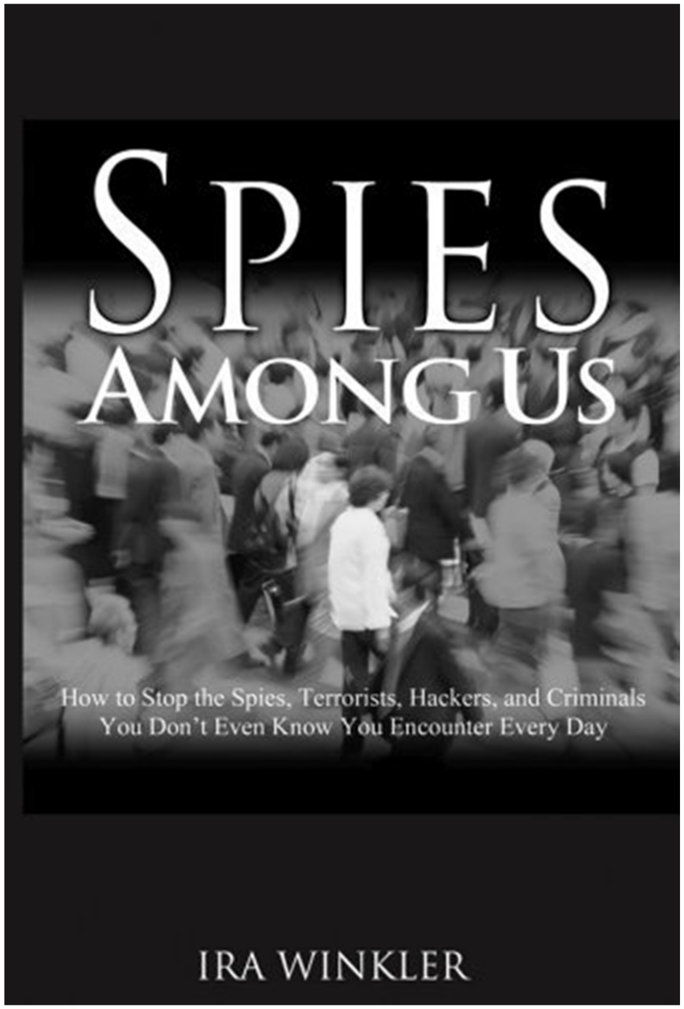
Just in Case

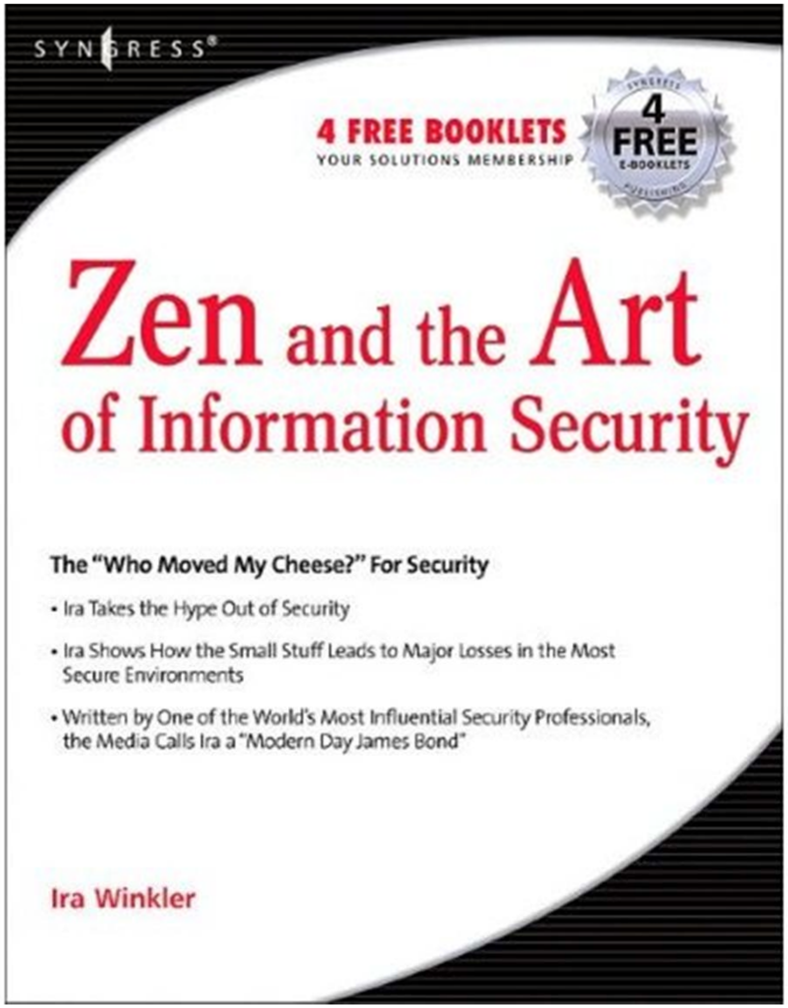


SOCIAL MEDIA EXPLAINED

twitter	« I need to pee »
facebook	« I peed »
foursquare	« This is where I pee »
Quora	« Why am I peeing ? »
YouTube	« Look at this pee ! »
Linked in	« I'm good at peeing »
Google+	<< Let's all pee together >>

For Your Reading Pleasure


SPIES
AMONG US
How to Stop the Spies, Terrorists, Hackers, and Criminals You Don't Even Know You Encounter Every Day
IRA WINKLER


SYNGRESS®
4 FREE BOOKLETS
YOUR SOLUTIONS MEMBERSHIP
4 FREE E-BOOKLETS
Zen and the Art of Information Security
The "Who Moved My Cheese?" For Security
• Ira Takes the Hype Out of Security
• Ira Shows How the Small Stuff Leads to Major Losses in the Most Secure Environments
• Written by One of the World's Most Influential Security Professionals, the Media Calls Ira a "Modern Day James Bond"
Ira Winkler

Book Signing

- After Internet Regulation Debate in Crypto Commons
  - Thursday 12:00 – 12:50
- Thursday 1:15 – 1:45
- RSA Bookstore

For More Information

Ira Winkler, CISSP

ira@codenomicon.com

+1-410-544-3435

www.facebook.com/ira.winkler

@irawinkler

www.linkedin.com/in/irawinkler