

Winn Schwartau

Keynotes, Seminars and Interactive Presentations

Winn Schwartau is an engaging speaker who involves his audience in his presentations. No matter how technical the subject, lay audiences come away with a powerful and complete understanding in terms they can handle. Schwartau often includes interactive training, audience participation, role-playing and situational dynamics to make his sessions memorable.

His presentations run the gamut from Information Warfare, (from his books) to Information Security 101, Espionage, Personal Privacy, Effects of Technology on Society and Corporations and a host of related topics. The newer material that he has developed is even more exciting and dynamic than the original materials that 'made' his reputation as a world-class speaker, trainer and indeed, entertainer. These are a sample of the presentations that he custom tailors for your organization. If you have other needs and ideas for keynotes, seminars or similar training, please contact Winn at 727.393.6600.

- **Information Warfare and Cyberterrorism**
 - How and Why Infowar Occurs
 - Global, US and Commercial Perspective
 - Defensive postures for nations and companies
- **Real World Security Awareness**
 - Ma, Pa and the Corporate Clueless
 - Successful Employee User Participation in Corporate/Gov't Security
 - Fun, fascinating and effective
- **Computer Ethics for Kids, Companies and Governments**
 - Bringing it all home... down to the basics
 - Ideal for educators, parents and family support groups
 - Highly interactive, provocative and audience debate laden
- **Protecting Kids and Families on the Internet**
 - Step by step how to!
 - Non-technical as it can be.
- **Security 101**
 - The basics of information security for beginners, non-technical and management.
- **General's Abdication**

- How senior military and civilian leaders have given up control of their organizations to people that are somewhere between incompetent and disloyal. Who is really in charge of the company, the country and the networks? What do you know about them and their allegiances? This politically incorrect presentation will raise hackles... and make you think or rethink everything you thought you knew about information security.
- What can we do about it? Schwartau expands on the principles of Time Based Security, tosses in a new Security Triad and shows us the only real way to secure networks and businesses today.
- **Rear Echelon Attacks: Asymmetrical Adversarialism**
 - No one is going to attack the USA with conventional weapons. The Chinese have declared Unrestricted War against the U.S. in time of conflict.
 - The 'bad guys' are going to attack the unclassified, rear support lines to reduce our operational capability. Fascinating and scary.
- **Time Based Security**
 - Quantifiable Methods for Developing Enterprise-wide Security
 - Helps technicians and management understand security as a risk and then how to measure it for mitigation. Corp and mil audiences ideal.
- **Corporate Vigilantism: Right, Wrong or Necessary?**
 - When law enforcement won't respond to or investigate cyber-attacks, what should we do? Take the law into our own hands? Many people are. Did you know it is illegal to disarm your adversary in Cyberspace?
 - Surveys, Results and Opinions. Great for Interaction and debate
- **RF Weapons, HERF Guns and EMP Bombs:**
 - A Tutorial on The State of the Art for Terrorist Attacks Against Infrastructure, Business and Government
 - The first and only unclassified taxonomy on these advanced weapons of mass disruption.
- **Cyber-Disaster Exercises**
 - Coping With Cyber-Attacks, Responses and Role-Playing (Highly Interactive, Tension Filled and Fun)
 - Commercial, Government, Municipal, Military and International Scenarios and Games
 - Contingency and Consequence Management
- **Personal, Corporate and National Survival in Cyberspace**
- **An Electronic Bill of Right and National Information Policy**
 - Personal Privacy, Creeping Government, Identity Theft and What to Do About It.
 - In Cyberspace, You Are Guilty Until Proven Innocent: Protecting Your Privacy in a Digital World

- **Hackers, Hacking and Their Weapons**
 - Demonstrations
 - If you want hackers, we bring hackers!
- **Developing a Workable Corporate Security Policy**
- **Information Security**
 - All Levels
- **Using Deception in Network and Infrastructure Defense**
 - Applying Successful Military History and Techniques to Network Security
- **Non-technical Information Security**
 - There are lots of non-tech, low-tech and very low cost ways to improve security postures
- **Defending Critical Infrastructures in Cyberspace**

Computer Forensics 101

Almost every crime committed today involves computers, networks and/or portable-mobile smart devices. In the investigation, digital evidence must be collected to make a case. Highly trained electronic forensics experts are often required to collect, analyze and interpret the evidence. In this session, we will examine the basics of computer forensics for the non-technical professional. And perhaps, just as importantly, we will discuss what 'Not To Do' at any crime scene that involves digital evidence.

The Future of InfoSec?

Schwartz looks into his crystal ball and predicts the future of information security, information warfare, cyberterrorism and the coming technologies we will be facing. It's not always pleasant, either.

Bumblebots and nanotechnology. High Energy RF Weapons. Deception. Wireless? What are the impacts on business and productivity? **Corporate Vigilantism: Right, Wrong or Necessary?** When law enforcement won't respond to or investigate cyber-attacks, what should we do? Take the law into our own hands? Many people are. Did you know it is illegal to disarm your adversary in Cyberspace?

All about the New! Security Triad: People, Physical and Cyber. How do con-focal vulnerabilities affect corporate, national and global economic security?

And what about Graceful Degradation? The Ultimate and safest means to protect networks in worse case scenarios.

Controversial. Important. Don't miss it.

Time Based Security

According to Winn Schwartau and an increasing group of believers, we've been doing it all wrong. The last 30 years and \$30Billion we've all spent on Information Security and Assurance has fundamental flaws so drastic, they cannot be fixed.

Bring your paper and pencil! Schwartau will walk you through a new security model, Time Based Security, which rids us of the shackles of the old inefficiencies and impossibilities that Fortress Mentality represent. In fact, he will give you simple mathematical formulas which can be used to determine just how secure an enterprise is, and how to turn that assessment into risk and hard dollar evaluation. His models are applicable for networks, critical infrastructures, banking and national defense.

This leading edge work is the subject of Schwartau's latest cutting edge hit book, "Time Based Security," ISBN: 0-9628700-4-8. Absolutely fascinating! Be prepared to sit in the front row and become another one of his audience 'victims'. ☺

The Metrics of Offensive Information Warfare

The concepts of Time Based Security find particular application with the military for national cyber-defense as well as conflict and offensive tactics. The mathematics of TBS can be modified to work with offensive IW, illuminating both a defender's weaknesses how to take advantage of them by an opponent.

Whether the offensive behavior is conducted by a military Cyber-Force or renegade hackers, the premises are the same. The math is simple, the concepts profound, and a great time will be had by all!

Corporate Vigilantism

When a company is under cyber-attack, what should it do? According to the premises of Time Based Security, an organization must be ready, will and able to react to any of a range of assaults against its networks or its infrastructures. But, how far are companies willing to go, and what are the options?

The Pentagon actively struck back at on-line hackers with their hostile perimeters, and now the hackers are threatening to sue the US Government. Or, is the approach of Lou Cipher the right one: use physical force for a quick, decisive end of any cyber attacks.

This is an emotionally charged session which divides the audience based upon legalities, morals and ethics. Don't miss it!

Using Military Approaches to Network Security

Using the basics of Time Based Security, Schwartau will walk you back through the annals of military successes, the great spy adventures and show you to simply add clear cut intelligence strategies to the defense of your networks. Amazing? Yup! But clearly at the cutting edge where Schwartau shines best. The concepts of Sun Tzu (c. 225 BC, China) in the Art of War will help the audience better understand the Deception protocols that Schwartau advocates.

Graceful Degradation: The Acts of Man versus Y2K

Instead of trying to presciently divine what the future will bring, isn't there a better way to plan for unforeseen contingencies? We seem to be able to handle the Acts of God; hurricanes, floods, fires and such. But what about the Acts of Man – and those unforeseen accidents caused by Man, such as Y2K? How do we plan for them and defend against their consequences?

Security Awareness for Ma, Pa, the Kids and the Corporate Clueless

It's a brave new world out there (unfortunately) and that means we are all going to have to do our part in protecting ourselves, our companies and our country.

Winn Schwartau has been a national leader in Security Awareness for almost two decades, also warning Congress about the specter of an impending Electronic Pearl Harbor.

Today, that threat is the same (and perhaps worse!), but now we need the assistance of everyone to become part of the solution instead of part of the problem: Ma, Pa, the Kids, Schools, Parents and every Information Age Worker.

In this compelling session, you will see first hand how and why every citizen and family member can contribute to their own security and privacy as well as act as a First Line of Defense against CyberTerrorism and Information Warfare.

- How You Can Help With the New National Security!
- How To Expand Your Environmental Awareness: People, Physical and Cyber
- Home and Personal Security: Top 10 Things You Need To Know
- Internet and Computer Ethics for Kids, Teachers and Parents (Without a Clue)
- Becoming a Security Aware Corporate Citizen

You do not want to miss this opportunity to notch up your security awareness for your organization, agency or educational institution. Highly entertaining and interactive. If you haven't seen a 'Winn-Style' presentation, don't miss this one!

Non-Technical Security

Security can be tough, especially for companies with apathy and arrogance. But, with a little imagination, the security posture can be dramatically improved – with little or no additional expense or headache.

Schwartau has amassed an intriguing collection of techniques and methods for enhancing network security without huge expenditures of time, money and manpower. See how many of these will work for you!