The Net Effect offers a "Cyber Self Defense" series of one-hour sessions, with new lessons constantly added. *We also offer more extensive presentations covering the essential topics outlined in this brochure.*

Both the one-hour series and the extensive presentations are based on industry standard best practices, current threat analysis, and real-world security practices that every end-user (whether technical or not) can implement personally and professionally.

Cyber Self Defense Series

(one-hour modules):

- How Does That Work Exactly?
- The Ways We Leak Data
- The Challenges of Authentication
- Social Engineering Defense
- The Traveler's Dilemma
- Password Management Techniques
- Protecting Online Identity
- Phishing, Spearphishing, & Whaling Attacks
- Assessing & Securing Third Party Risks

Audiences for these highly-acclaimed Security Awareness Training sessions have ranged from professional organizations (legal, governmental, judicial, security, financial, HR/personnel) to private entities including defense contractors, local government, retail, accounting and legal firms, manufacturing entities, and more.

Standalone presentations are typically 60-120 minutes and may be certified for CEU credits by many professional organizations.

the net effect

Where business needs and technology intersect

The Net Effect provides technology consulting services on information security and project management to commercial, non-profit and governmental organizations. Our team of experts work with our clients' IT staff and third-party vendors to develop optimal solutions to operational challenges.

Glenda R. Snodgrass has been lead consultant and project manager at The Net Effect since the company's inception in 1996.

Ms. Snodgrass is primarily engaged in cyber security training, threat analysis and mitigation for small- and medium-sized businesses. In addition to conducting security-related workshops, corporate training and delivering cyber security defense presentations at professional conferences and conventions, she spends time drafting network security protocols and developing employee security awareness training programs for clients.

Ms. Snodgrass is President of the Gulf Coast Industrial Security Awareness Council. She is involved in InfraGard, ASIS International, and Gulf Coast Technology Council, as well as numerous civic organizations. She holds a B.A. from the University of South Alabama (1986) and a maîtrise from Université de Paris I - Panthéon-Sorbonne in Paris, France (1989).

The Net Effect, L.L.C.
56 South Conception Street
Post Office Box 885
Mobile, Alabama 36601-0885
Phone (251) 433-0196
Fax (251) 433-5371
http://www.theneteffect.com
Email grs@theneteffect.com

Information Security is a people problem.

Effective training is your best protection.

Introducing effective training seminars.

the net effect

Where business needs and technology intersect

Expert Security Awareness Training from the experts in Information Security

Ransomware & Other Wares

Ransomware is now top of the charts for malware infections worlwide, and the US is hit the hardest of all. This overview of Ransomware and other "wares" will help you develop the skills necessary to detect and prevent possible ransomware infections, along with emergency mitigation strategies in the event of infection.

You Can't Secure It If

In this seminar, we step through some of the issues we have encountered in helping clients assess risk. For example, you can't secure it if you don't know you have it, you don't understand how it works, you don't know who has access to it, and more.

Cyber Crime & Social Engineering

As the stakes have increased (cyber crime is now more profitable than the drug trade worldwide!), so has the investment criminal gangs are making — and Social Engineering is now the hot ticket for easy cyber heists. From whaling to typosquatting and Man in the Middle attacks, come explore successful strategies for social engineering with real-world examples of data breaches we've investigated.

Protecting Personal Information in the Digital Age

Cyber crime is now more profitable than the global trade in marijuana, cocaine and heroin combined. Attacks come from all angles—not just computers, but also mobile devices, public wi-fi, social media, malvertising and other forms of social engineering.

Protecting your online identity requires understanding both the form of current threats and effective prevention measures:

- Situational Awareness
- Social Media
- Wi-fi and other wireless tech
- Password hygiene & multi-factor authentication
- Social Engineering attacks

Cyber crime is just that—crime!—but you can avoid being a victim through education and awareness.

Shibboleths and Secrets

Authentication is one of the greatest challenges in providing secure access to information when needed. This course takes a look at various authentication methods and options, from password hygiene and good management techniques to biometrics and tokens.

Mitigating Cyber Security Risk

"It's not just an IT problem." Risk management in cyber space requires administrative, physical and technical controls. Using a three-pronged approach, you can learn to mitigate cyber security risk in your organization and in your home.

The Evolution of Big Data

Big Data isn't just "bigger" or "more"—it's different. This overview of the evolution of how data is collected, stored and analyzed will help even the non-technical person understand the world of Big Data and Predictive Analytics in which we now live and work.

Big Data and the Internet of Things

Putting "Things" on the Internet—from appliances to security systems to machinery to human bodies—is exponentially increasing the amount of data that can be collected, stored and analyzed. The evolution of Big Data has made this possible, and it's changing our world in ways we never envisioned.

Corporate Account Takeover: Don't Be the Next Headline

Security experts agree that the weakest link in any organization is the user. In fact, IBM Security Services investigations determined that human error was involved in more than 95% of the security incidents in 2013. Learn how to improve your security posture by decreasing risky behavior. This session will analyze recent major breaches and target the human errors which caused them.

the net effect

Where business needs and technology intersect

Training CEU Certifications Alabama State Bar Association ■ Association of Certified Fraud Examiners (ACFE) ■ Financial Planning Association (FPA) ■ Society of Industrial Security Professionals (NCMS) ■ Project Management Institute (PMI) ■ Society for Human Resource Management (SHRM) ■ The Florida Bar ■ The Mississippi Bar