

## “LowTech InfoSec”

### John T. Collins, In-Depth Security

#### Introduction

Companies today spend millions on talent and technology to protect their digital assets and intellectual property. And while trying to eliminate all human error regarding the protection of our digital assets is commendable, it's really PEOPLE who have the biggest impact on the success of technology measures.

According to Network World:

- Approximately 80-90% of security breaches originate from within the corporate firewall from employees.
- More than 20% of attacks on the corporate WEB sites are coming from the inside.
- Almost 30% of companies, experience more than 5 attacks from the inside per year.

The net - sometimes a little planning and communication can accomplish more than a great technological tool. So statistically speaking, it may be more cost effective to spend your security budget on training your people instead of installing tools.

No matter the comprehensiveness of a tool, it is just too easy for unaware employee, vendor, or contractor to compromise security controls put in place. Aligning your technical controls with a well informed workforce will significantly reduce the frequency and impact of security events in your organization.

So how should you get the word out to create significant change? The days of mandates without explanation to employees aren't as successful as they were in the past. Training and communication must take into account the culture of an organization. Employees today are more willing to embrace change if they know why the changes are being put in place as well as the benefit to the company, their co-workers, and themselves. When developing your communication and training plans, make sure you address the employee's motivation for attending or completing the activity:

- Loyalty to company and profession
- Fear or consequences of not participating or breaking policies
- Ethical, honest, social, and good business actions
- Personal or departmental loss due to security behavior
- Company, co-worker loss due to security behavior
- Excel or promotion in company
- Rewards and recognition for participation

- Protection from or loss of individual investment of effort, money, assets
- Protection or furtherance of personal and employer's reputations
- Speed and ease of use

Variety is the spice of life. It also helps spread the security word. The following are just a few ideas on tools and techniques for creating and maintaining a consistent security posture:

- A Security Awareness Handbook
- Security Alerts from Network Systems
- Mass Email
- Lunch & Learn
- Security Presentations or Instructor Led Training
- e-Learning
- Messages Boards/Banners
- Videoconferences or Videos
- Screen Savers
- How to Guides
- Brochures
- Security Themed Events
- Security Themed Contests

There are many comprehensive tools, techniques and methodologies that can assist in creating and maintaining an education and awareness program. Start with these basics and you can begin to create a custom-tailored solution that works within your business goals and budget.

John Collins is the Director of Training Services with In-Depth Security and currently serves as the Education Director for the Austin Chapter of the Information Systems Security Association.