ONE-SIZE-FITS-ALL TRAINING AND EDUCATION IS NOT THE ANSWER

PRESENTED BY BRIAN LAU
Appliedinfo Partners, Inc. (AIP) is an MWBE technology-based business that focuses in:

- eLearning Technology
- Multimedia Development
- Mobile Applications and Training
- Cybersecurity Training
- Corporate Communications
- Digital Communication Strategies

Our Somerset, NJ headquarters is a 50,000 sq. ft. building facility with a filming studio, green screen studio, 4 HD Editing Suites and other video and 3D technology support.
Our Clients
The Cybersecurity threat landscape

- **33%** of corporations & **43%** healthcare companies in the US has experienced a data breach in 2014, up by **10%** from 2013. **71%** of these breaches are in small business

- At least **27%** of companies do not have any data breach response plan or team in place

*Source: ITRC 2015 Data Breach Report*
Small Business are an easy target

- **87%** of SMBs do not have a formal written Internet security policy for employees, while **69%** don’t have any Internet security policy for employees

- Nearly **59%** of SMB in US don’t have a contingency plan that outlines procedures for responding to and communicating data breach losses

- **18%** of SMB owners/operators say they would not know if their computer network was compromised (i.e. infected with a virus, private information stolen, etc.)

- **11%** of SMB owners/operators say no one is responsible for online and cybersecurity at their business.

*Source: ITRC 2015 Data Breach Report*
Where did most of the breaches come from?

- Nearly **80%** of these breaches resulted from “**Dave**”
Why Education and Training is Important

Companies **without** security training for new hires reported average annual financial losses of **$683,000** while those with training only experienced financial losses averaging **$162,000**.

*PwC, “US cybercrime: Rising risks, reduced readiness.”*

Monte Carlo Analysis Reveals That **Changing Employee Behavior** Reduces the Risk of a Security Breach by **45% to 70%**

- Significant investments in **security technology are diluted** when there is a **lack of investment in security awareness and training**

- For an organization with **$200M** in annual revenue there is an **80%** likelihood that infections from employee behavior will result in total costs of **$2.5M** per year under the status quo; and a **20%** likelihood that the costs from errant employee behavior could exceed **$8M**

Our DNA

• **In-house Cybersecurity Subject Matter Expertise**
  - Core content developed by our cybersecurity Subject Matter Experts (SMEs)
  - Senior staff have many years of network planning, Internet technology management and cybersecurity product development experience
  - Our SMEs have worked with NOC, CIRT, and Forensic teams with Fortune-500 companies

• **In-house multimedia production facility**
  - Green screen studio
  - Multiple video editing suites
  - Gaming development

• **In-house Defense-grade online training (DIF) platform**
  - Standard tool within the US Army
  - Enterprise collaboration
  - Rapidly updatable
  - Global repository of reusable cybersecurity modules
The AETC Process

**Analyze**
- Site survey to analyze and assess some of the existing operational/behavioral gaps
- Basis for customizing training to address the identified gaps in instrumentation and practice

**Educate**
- “Common Core” cybersecurity knowledge as the educational foundation building block
- Ensuring employees are up to date on the latest cyber criminals tactics and procedures

**Train**
- Training for each specific employee and division within each organization
- Skill-based exercises on company specific policies and procedures
- Preventing and/or mitigating specific cyber breaches

**Communicate**
- Repetitive messaging over time is a vital key to learning
- Communication should be an ongoing exercise, not a discreet event
Employees are not all the same, why should their courseware be?

Analyzing variances in employee and industry is key to developing effective, habit changing training.

- **Industry Specific Training**
  Utility, Financial, Healthcare, Technology organizations etc. all have different pieces of information a cyber criminal would want to access, and all are protective differently.

- **Specific role and position training for employees**
  From CEOs to assistants, information is distributed differently across the spectrum of each organization, and while there are common guidelines that to need to be established, each position needs to understand their responsibility and mitigation response to a cyber threat.

- **Organization Policies Differ**
  Every company has varying levels of policies and procedures in place and none, are exactly the same. In order to truly change behavior, your organization needs to put their stamp on their Cybersecurity message.
Focused and Engaging Training

Education and training that is uniquely focused to specific industries and employee roles – the “One size fits all” approach is no longer sufficient to address organizations Cybersecurity needs. We need to deliver training at the “Point of need”

- Development of a “Common Core” which unifies the education and messaging across an organization that is easily updatable and scalable to different divisions and positions within a company.

- Create job specific training for managers, team leads, employees down to custodians. No employee should be looked over.

- Provide monthly/quarterly targeted education and training vignettes to employees, not all employees will receive the same information in order to improve the efficiency of the training focus.

- Create engaging courseware that is efficient, impactful, entertaining and most importantly, that changes an employees habits and a companies culture.
Example of our work: Mobile Security
Example of our work: Passwords

LESSON 2  PASSWORD/PASSPHRASE REPETITION

The second greatest challenge in secure password creation is resisting the temptation to reuse a single password or phrase for all of your online accounts.

ONE PASSWORD
Example of our work: Hackul8or

**LESSON 2** PASSWORD HACKUL8OR

Create your Email Account

Username
New.Staffmember @smbiz.net

Password
**************

😊 MODERATE

It can take up to 5.22 years to crack your password!
What can D2 Cybersecurity do for you?

- Analyze the **cybersecurity gaps** which will drive instruction and implement a process that addresses your organization cyber shortfalls.

- Use **instructional and creative design principles** to transform organization’s policies and procedures into **individually tailored interactive** training and education.

- Develop **creative, cutting edge courseware** with graphics, videos, games, and other technology solutions for engaging courseware that addresses the critical needs of each employees.

- Update content periodically for **consistently current** courseware.

- Produce a persistent, proven communication package that will **change the culture and behavior** within an organization.
Questions