



# THE **SECURITY** CONFAB

Securing Your  
**ENTERPRISE**  
for the **Future**

April 15-17, 2012 • La Jolla, California

PRODUCED BY **CSO**

# Reducing Risk Through Next-Gen Cyber Awareness Training

**Dan Lohrmann**

CSO

State of Michigan

# A Quick Quiz . . .

Question 1: What do these headlines have in common?

The image shows three overlapping news snippets. The top-left snippet has the headline "Global Survey: Malware Attacks Up Because of Social Media; Organizations Lagging on Proper Protection" and includes social media icons for Facebook and Twitter. The top-right snippet is titled "TWITTER" and has the headline "40% of Social Network Users Attacked by Malware". The bottom-center snippet is a news article with the headline "More companies are OK with employees using Facebook at work" and sub-headline "One global consulting firm says allowing the use of social nets at work keeps workers happier". It is by Sharon Gaudin and dated March 26, 2012. It also shows 7 comments and 37 likes.

Global Survey: Malware Attacks Up Because of Social Media;  
Organizations Lagging on Proper Protection

Like Twitter Follow

Home > Applications > Enterprise Web 2.0/Collaboration

**News**

**More companies are OK with employees using Facebook at work**

One global consulting firm says allowing the use of social nets at work keeps workers happier

By Sharon Gaudin

March 26, 2012 02:22 PM ET

7 Comments Like 37

TWITTER

40% of Social Network Users Attacked by Malware

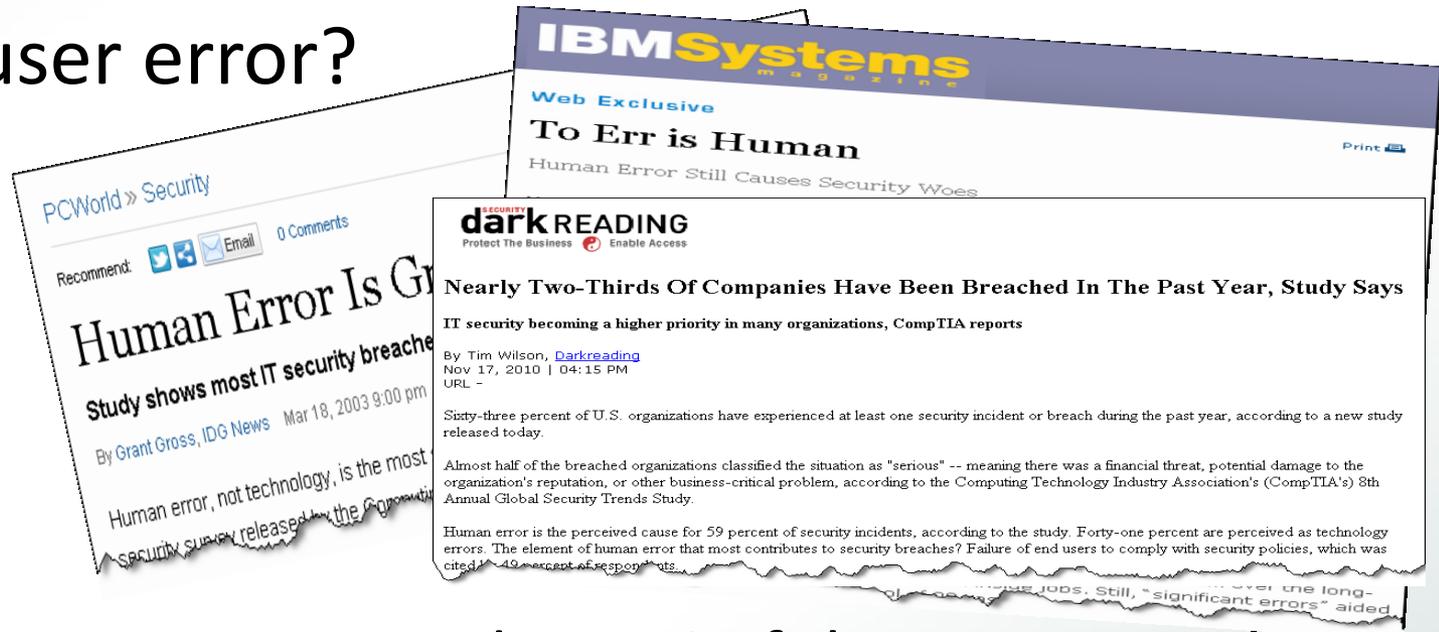
# A Quick Quiz . . .

Question 2: What percent of breaches are the result of user error?

25%

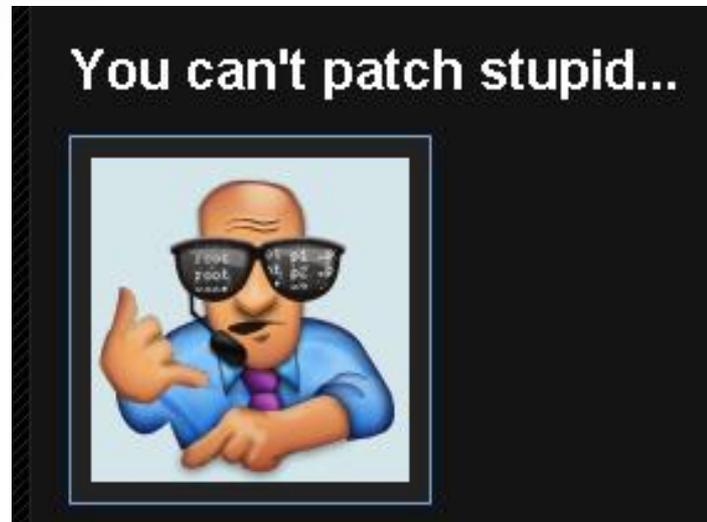
45%

59%



According to Comp TIA study, 96% of those surveyed would now recommend user training.

# How Have We Addressed It?



“PIC” – Problem in Chair

# The Right Approach

- Give employees the “carrot” and award a certificate . . .
- Or bring out the “stick” and deny access?



Answer: **A combination of both!**

# End-User Training is Broken

- Employees don't see the relevance.
- Training materials are outdated.
- Employees don't understand their role.
- Training is boring –  
    “Death by PowerPoint”
- Security is someone else's job.
- “Check the box” compliance exercise.



# Cyber Awareness Training 2.0

- Make the training sessions . . .
  - Intriguing
  - Relevant
  - Fun
  - Focused
  - Clear and easy to understand
  - Effective



# Use Stories to Make it Real

**Stories can give context to your training information.**

For example, a study of 114 major airports found that:

- Business travelers lost more than 16,000 laptops weekly.
- About half of all business travelers said their laptops contained confidential information that they did not take steps to protect or secure.
- About a third of all travelers took steps to protect their information, but they didn't know how it was protected.

# Fun Training?

Where is the #1 location for lost devices at the airport?

Security Checkpoint

Restroom

VIP Lounge

Food Court

None of the Above



# Michigan's Approach



Michigan is piloting next-generation cyber training that will help employees understand how to protect their computer assets – both at work and at home.



**Security Mentor**  
Brief, Frequent, Focused.™

Sign In My Account Contact Us

Training Resources News & Events Company Support

## The Security Mentor training advantage

Security Mentor's web-based security awareness training is innovative, training the way people learn.

- Brief – less than 7 minutes per lesson
- Frequent – a new lesson every week
- Focused – only one topic per lesson
- Delivered – training reminders in your inbox

[www.securitymentor.com](http://www.securitymentor.com)

Security awareness training that is:

- Brief
- Frequent
- Focused
- Engaging
- Interactive
- Memorable
- Relevant



## Awareness Training Overview



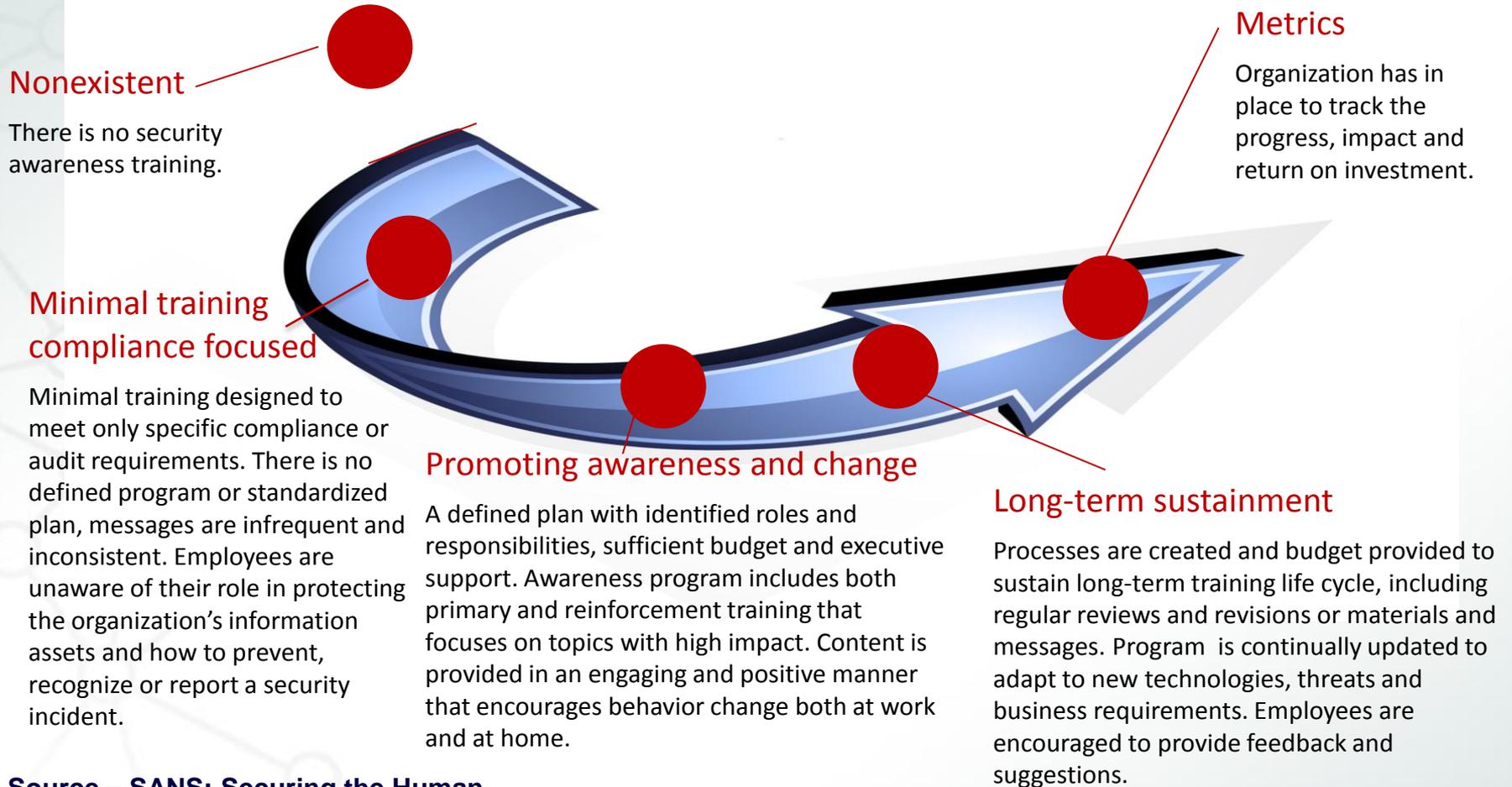
At Securing The Human our goal is to not only ensure you are compliant, but offer training that changes behaviors and reduces risk. We do this by using the 20 Critical Controls as the framework for our training. In addition, our awareness training is developed by a board of SANS most experienced SANS Instructors. This training is then reviewed and updated twice a year, ensuring you have the most current and engaging training possible. We then take this content and break each topic into a

Free Trial

Advantages of the  
SANS Securing The  
Human program  
include:

- Go beyond compliance and focus on changing behaviors.
- Training mapped against the 20 Critical Controls framework.
- Create your own program by choosing from over 30 different training modules.
- Meets mandated compliance requirements.
- Fully SCORM compliant, host on the SANS VLE or your own LMS.

# Security Awareness Maturity Model



Source – SANS: Securing the Human

# Final Thoughts

- Your staff is your organization's biggest asset and it's biggest vulnerability.
- Providing employees with effective training will enable them to become your cyber security partners.



# Questions?



Daniel J. Lohrmann, Michigan Chief Security Officer

[LohrmannD@michigan.gov](mailto:LohrmannD@michigan.gov)

(517) 241-4090



# THE **SECURITY** CONFAB

Securing Your  
**ENTERPRISE**  
for the **Future**

April 15-17, 2012 • La Jolla, California

PRODUCED BY **CSO**