
BOSTON CONFERENCE
06-07 DECEMBER 2016
Securing the User: Winning Hearts & Minds to Drive Secure Behavior
Thomas Skill, CIO University of Dayt
Spencer Mott, CIO-CISO Amg
Dawn Sherizad, product manager of security, Macy
Eleanor Dallaway, Editor & Publish
Infosecurity Magazi
info security
STRATEGY | INSIGHT | TECHNOLOGY

New Realities of Cybersecurity

1. We can't solely **"engineer" our way to comprehensive cybersecurity**
   - *But we must continue innovating with technologies that better monitor, predict and protect.*
2. We can't solely **rely on central command & control to enforce effective cybersecurity**
   - *But we must continue establishing and enforcing best practices*
3. We can't **achieve highly reliable cybersecurity solely through <u>compliance-focused</u> education programs**
   - *But we must continue mandating continuous learning*

- **"Solutions" like 2FA can falsely assure users that "security is now solved!"**
  - 2FA does not prevent:
    - Ransomware, spear-phishing, legacy system access, vishing, malicious code attacks
- **"Box-checking" training & education** will not advance our efforts if we fail to engage users or sustain desired behaviors.

Leveraging empirically-derived social-scientific theories and models

What do we know about shaping attitudes & impacting behaviors?

Theroetical Domain	*Guiding Principle*
Communication Theory	All Messages Contain **Content & Context** Information
Health Belief Model	Users need to be convinced that **cyber-threats are real and highly impactful** on them
Cognitive Response	Cyber-Mindfulness Requires that Users Engage in **Central & Salient Information Processing Behaviors -** not Peripheral Processing
Diffusion of Innovations	**Identify Change Agents & Opinion Leaders** as Strategic Influencers, Focus on Values Compatibiltiy
Persuasion Theory	**Innoculate the User Communtiy** Against Threats & Attacks through Persistent & Changing Exercises, Increase Efficacy

Framing the Cyber-Mindfulness Strategy

- Our goal is to ***transform our user community from high-risk cyber targets to high-achieving "first alert allies"***
- Evolve from "culture of compliance" to a "culture of mindfulness"
  - Rebooting education/training strategies and practices
  - Providing proactive – rather than reactive – information
  - Encouraging and facilitating community dialogue

Cyber-Mindfulness:
Desired Changes and Outcomes

1. **Increased Awareness:**
   "I know that cybersecurity threats are real, persistent & dangerous"

2. **Improved Attitudes:**
   "I believe that these risks are important and meaningful to me."

3. **Effective Behaviors:**
   "I will take actions to reduce risks to me and my community – and I have practiced them!"

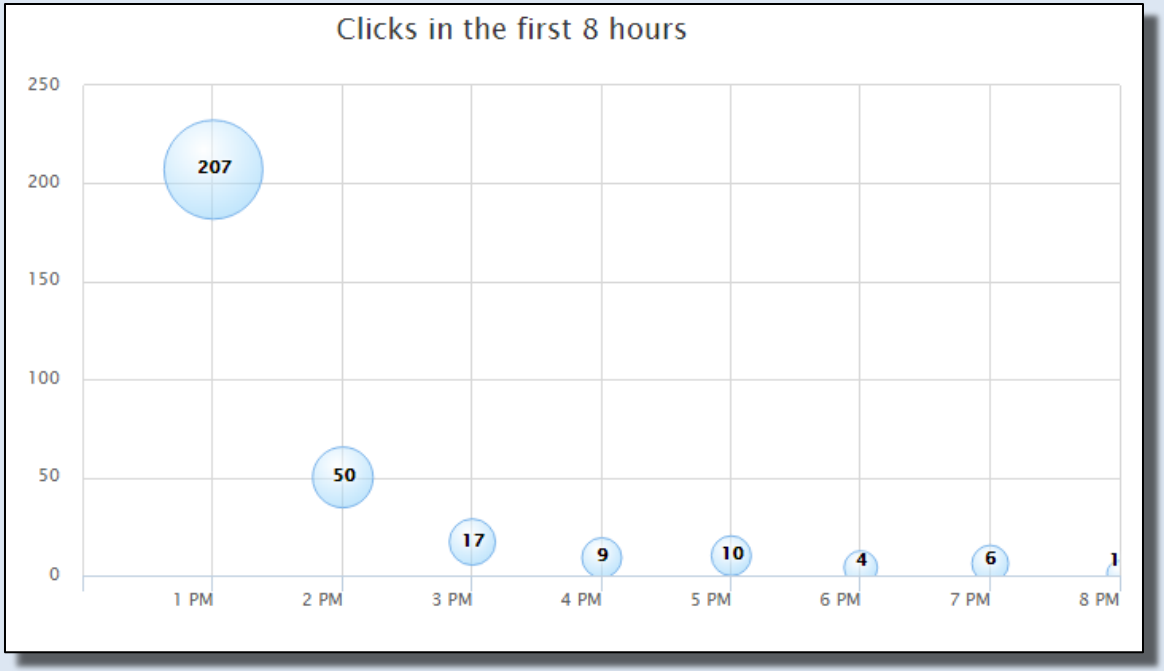
Audience Benchmarking
Phishing Behavior

Lesson Learned:

Cyber-mindfulness matters!

Most ***"click-first and think-later"*** behaviors happen <u>within the first hour</u> of a phishing message. . .

"early alerts" can't come soon enough.



Cyber-Mindfulness: Key Messages

- Safe computing is an important attitude and skill professionally AND personally
- Cybersecurity is not only the responsibility of IT professionals and IT systems; end-users are the most important safeguard
- Safe computing habits are not too technical to be learned; everyone can find ways to participate and improve
- Enterprise IT staff are a friendly partner in equipping users with safe computing skills and knowledge
- 2FA is one important tool for fighting cyber crime and everyone's participation makes significant impact against threats

Cyber-Mindfulness: Tactical Engagement
Shaping the Message & Overcoming Fatigue

- Gain trust and remove barriers with a friendly, approachable voice
  - We are accessible IT people who speak in everyday words about technical subjects without judgement or arrogance.
- Take a fun yet pragmatic tone
- Speak to the novice and the intermediate user in messaging and events
- Offer solid & credible information to highly technical users
- Appeal to both personal and work-related needs
- Provide a variety of entry points for communication
  - Multiple ways for people to connect with the information
  - Reinforce messaging through repeated use of the monthly theme

Sentinels Puts Information Center Stage, Enabling Staff to Better Protect It

The Sentinels Program: ***Staff outreach initiative; it's all about protecting our ability to serve patients.***

Our Goal: ***Create a global community of staff from across the organization whose focus is to help raise local awareness about information threats and to encourage and demonstrate information protection best practices.***

Chief Sentinels

- Strategic partners with Information Security & Risk Management team
- One per business area
- Information Protection advocates and enthusiasts
- Thinking 'global' but acting 'local'

689 Chief Sentinels

Staff Sentinels

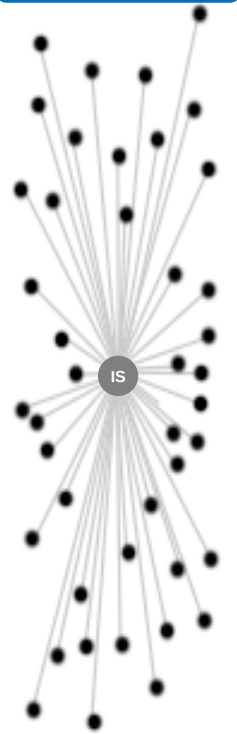
- What we should all do every day as good corporate citizens:
  - ✓ Be alert
  - ✓ Respond to issues
  - ✓ Advocate the use of information protection best practices
- 'Security 101' – The Essentials Security and Privacy Awareness (SAPA) Training

11,717 Staff Sentinels trained

"Keep up the great work – if all companies were as progressive as Amgen, I'd have less work to do." *– FBI Cyber supervisors comment on the Sentinels Program*

Networked Advocacy Approach is Key

Centralized → De-centralized



"Security is best achieved by the everyday actions of employees across the enterprise."

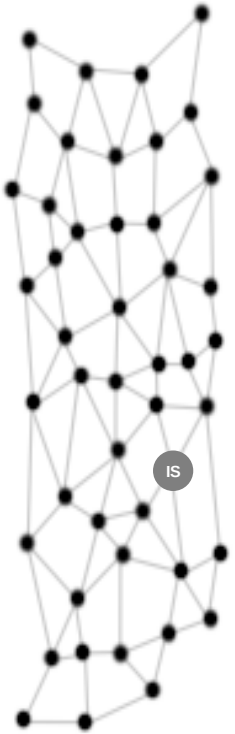
Sentinels is:

- A long-term program to put information protection center stage and ensure staff understand their role and what they need to do differently
- A global community of staff creating a network of information protection eyes and ears
- An integral part of the Information Security portfolio

Goals

- Ensure all staff, contractors and vendors understand the importance and actions required to protect critical information.
- Ensure Information Protection is seen as a competitive advantage and best practice behaviors become embedded.

Sentinels = Cyberhood Watch



Strength Through Collaboration & Knowledge Sharing

Sentinels + **Information Security** = **Protected**

Staff know their business area better than anyone else and play a crucial role protecting information **locally.**

A Sentinels role is:

- Be **alert** to potential breaches
- **Respond** to Information Protection issues
- **Advocate** and use Information Protection best practice in everything we do

Protects the global business, assets, products and people.

Information Security's role is to:

- Further strengthen controls
- Better identify and protect information
- Engage staff to increase awareness and advocacy
- Strengthen information systems infrastructure and security tools
- Work collaboratively within their industry on shared risk

In a recent 2014 PwC report it stated “Over 95% of breaches involve human error” so information protection must involve staff.

ISO27002 - 7.2.2: Deliver information security awareness during employment.

Sentinels in Action

Core Principles of Cyber-Mindfulness

- Users are at the center of sustainable cybersecurity
- Use what we know about human behavior from the disciplines
- Train our technical community how to engage with users.
  - Positive reinforcement must lead the way -- shaming or blaming will fail
- Maintain an ongoing, engaging dialogue with your user community
- Assess tactics & outcomes: measure, evaluate & adjust

Organization-Wide Security Awareness

- Role-based, short, sticky, frequent
- Long term, sustainable, high impact, behavior change

Top Human Risks/Topics

- Phishing
- Spoofing
- Password
- PCI Awareness
- Malware
- Network security
- File sharing

Spencer Mott

Thomas Skill

@skilltd

skilltd

Dawn Sheirzad

@DSheirzad