

**BOSTON CONFERENCE**

**06-07 DECEMBER 2016**

# **Securing the User: Winning Hearts & Minds to Drive Secure Behavior**

**Thomas Skill, CIO University of Dayton**

**Spencer Mott, CIO-CISO Amgen**

**Dawn Sherizad, product manager of security, Macy's**

**Eleanor Dallaway, Editor & Publisher**

**Infosecurity Magazine**

**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 compliance-focused 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?

<i><b>Theroetical Domain</b></i>	<i><b>Guiding Principle</b></i>
<b>Communication Theory</b>	All Messages Contain <b>Content &amp; Context</b> Information
<b>Health Belief Model</b>	Users need to be convinced that <b>cyber-threats are real and highly impactful</b> on them
<b>Cognitive Response</b>	Cyber-Mindfulness Requires that Users Engage in <b>Central &amp; Salient Information Processing Behaviors</b> - not Peripheral Processing
<b>Diffusion of Innovations</b>	<b>Identify Change Agents &amp; Opinion Leaders</b> as Strategic Influencers, Focus on Values Compatibilitiy
<b>Persuasion Theory</b>	<b>Innoculate the User Communtiy</b> 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!”*

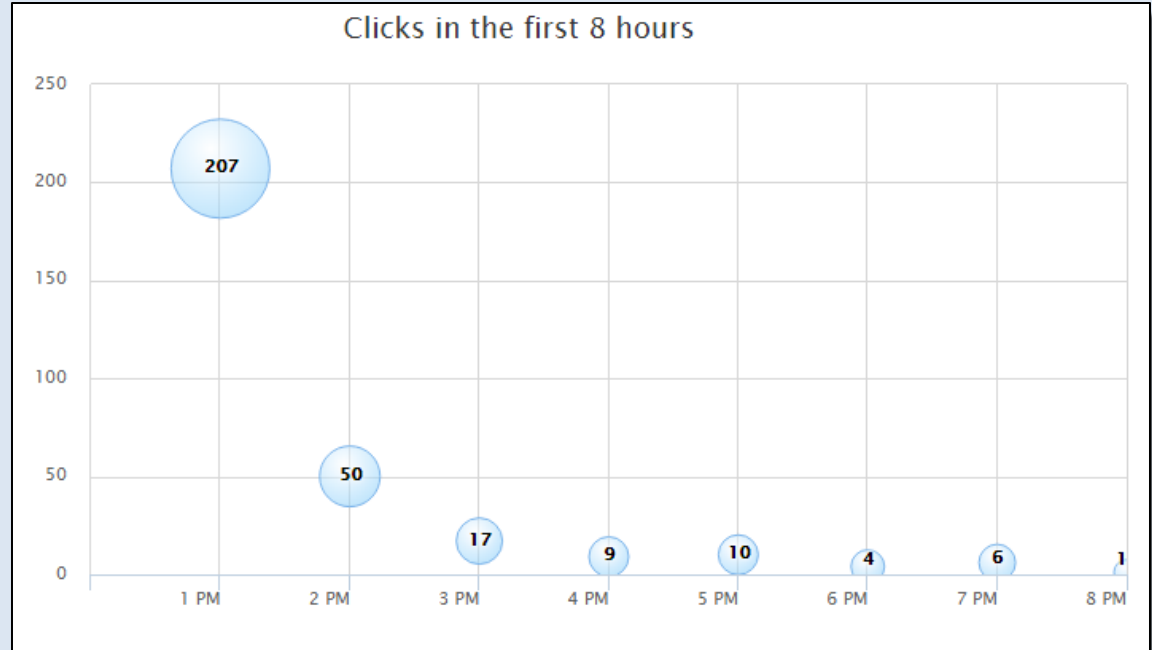
# Audience Benchmarking Phishing Behavior

## Lesson Learned:

Cyber-mindfulness matters!

Most ***“click-first and think-later”*** behaviors happen within the first hour 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



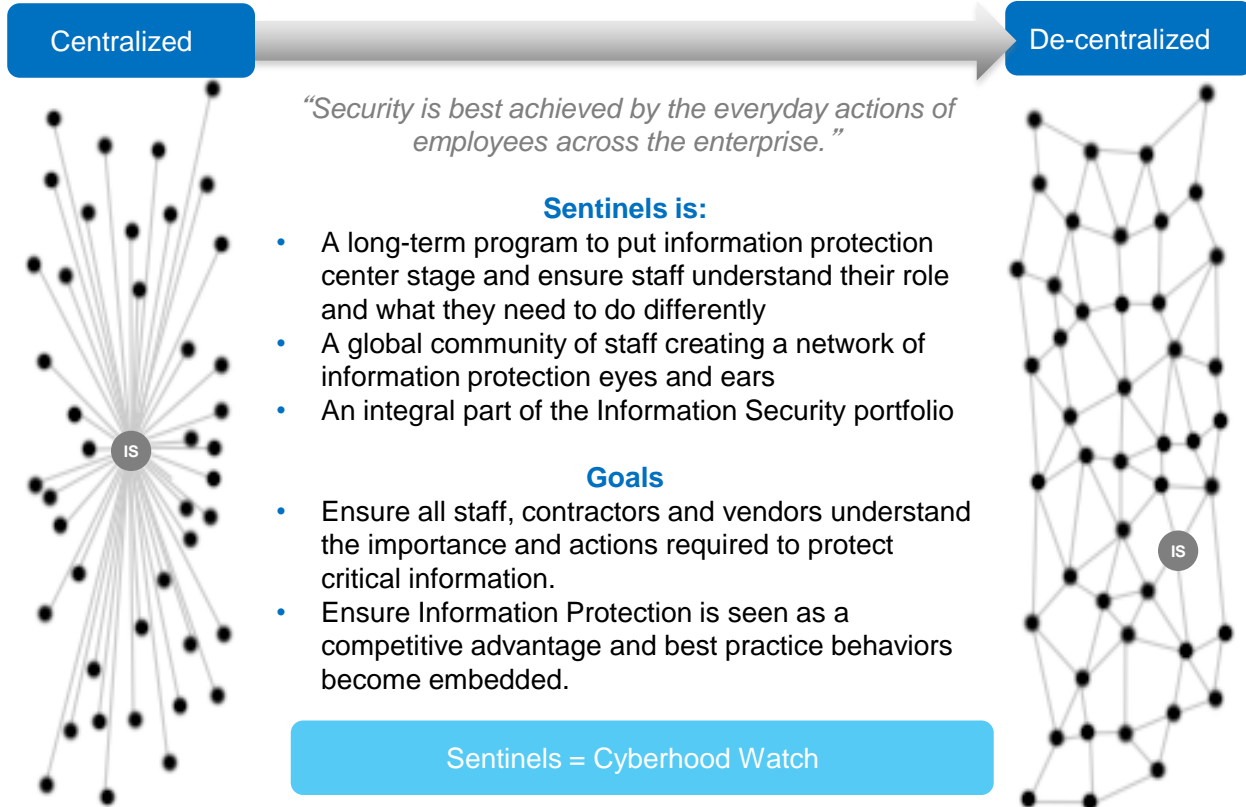
## Staff Sentinels

- 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

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



## Information Security

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

= Protected

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



**Information Protection**

**Pass it On**

Are you the key to Information Protection?

Ask me about SENTINELS

**Click for Bonus Tips**

Don't be a **TURKEY** this holiday season.

You are the key to Information Protection.

**Information Protection 101**

AMGEN Sentinels

**Strong and Secure Passwords**

How to create strong and secure passwords

How NOT to do with passwords

AMGEN Sentinels

**Why do we need Sentinels?**

How do they help?

AMGEN's Culture of Excellence

Don't forget

Need more information?

AMGEN Sentinels

**Why should I join Sentinels?**

Information Protection 101

AMGEN Sentinels

**Information Protection**

**@Home FOR YOUNGER USERS**

1. Don't give away personal information to strangers.
2. Don't give your name, address, phone number, or other personal information to anyone online.
3. Don't give your password to anyone.
4. Don't give your credit card number to anyone.
5. Don't give your Social Security number to anyone.
6. Don't give your date of birth to anyone.
7. Don't give your home address to anyone.
8. Don't give your phone number to anyone.
9. Don't give your email address to anyone.
10. Don't give your school name to anyone.
11. Don't give your favorite team to anyone.
12. Don't give your favorite food to anyone.
13. Don't give your favorite color to anyone.
14. Don't give your favorite animal to anyone.
15. Don't give your favorite book to anyone.
16. Don't give your favorite movie to anyone.
17. Don't give your favorite TV show to anyone.
18. Don't give your favorite song to anyone.
19. Don't give your favorite game to anyone.
20. Don't give your favorite sport to anyone.

**Pass it On**

**THINK Before Sharing ONLINE**

**Play IT Safe**

**Cyber Pro: My Profile's Private**

**THINK before you CLICK.**

**Connect with Respect**

**Only Post Positives**

**Always Aware**

**Play IT Safe**

**Report Cyber Bullies**

**Spread Heart not Hurt**

**PASSWORD PERFECT**

**PASSWORD PERFECT**

**THINK Before Sharing ONLINE**

**Why do we need Sentinels?**

- 54% of users have had their accounts hacked
- 70% of users have had their passwords stolen
- 60% of users have had their personal information stolen
- 75% of users have had their credit card information stolen
- 85% of users have had their identity stolen

**How do they help?**

- Provide real-time alerts for suspicious activity
- Monitor for phishing attempts
- Detect and block malware
- Provide secure communication channels
- Offer secure file sharing
- Provide secure web browsing
- Offer secure email
- Provide secure mobile app usage
- Offer secure social media usage
- Provide secure cloud storage
- Offer secure remote access
- Provide secure VPN usage
- Offer secure mobile device management
- Provide secure mobile app development
- Offer secure mobile app testing
- Provide secure mobile app deployment
- Offer secure mobile app maintenance
- Provide secure mobile app updates
- Offer secure mobile app security
- Provide secure mobile app performance
- Offer secure mobile app analytics
- Provide secure mobile app reporting
- Offer secure mobile app support
- Provide secure mobile app training
- Offer secure mobile app documentation
- Provide secure mobile app compliance
- Offer secure mobile app governance
- Provide secure mobile app risk management
- Offer secure mobile app incident response
- Provide secure mobile app disaster recovery
- Offer secure mobile app business continuity
- Provide secure mobile app resilience
- Offer secure mobile app sustainability
- Provide secure mobile app innovation
- Offer secure mobile app growth
- Provide secure mobile app scalability
- Offer secure mobile app flexibility
- Provide secure mobile app interoperability
- Offer secure mobile app compatibility
- Provide secure mobile app accessibility
- Offer secure mobile app usability
- Provide secure mobile app user experience
- Offer secure mobile app customer satisfaction
- Provide secure mobile app loyalty
- Offer secure mobile app retention
- Provide secure mobile app engagement
- Offer secure mobile app conversion
- Provide secure mobile app revenue
- Offer secure mobile app profitability
- Provide secure mobile app ROI
- Offer secure mobile app value
- Provide secure mobile app impact
- Offer secure mobile app legacy
- Provide secure mobile app reputation
- Offer secure mobile app brand
- Provide secure mobile app identity
- Offer secure mobile app culture
- Provide secure mobile app spirit
- Offer secure mobile app soul
- Provide secure mobile app heart
- Offer secure mobile app mind
- Provide secure mobile app body
- Offer secure mobile app spirit
- Provide secure mobile app soul
- Offer secure mobile app heart
- Provide secure mobile app mind
- Offer secure mobile app body

**Why should I join Sentinels?**

- Receive real-time alerts for suspicious activity
- Monitor for phishing attempts
- Detect and block malware
- Provide secure communication channels
- Offer secure file sharing
- Provide secure web browsing
- Offer secure email
- Provide secure mobile app usage
- Offer secure social media usage
- Provide secure cloud storage
- Offer secure remote access
- Provide secure VPN usage
- Offer secure mobile device management
- Provide secure mobile app development
- Offer secure mobile app testing
- Provide secure mobile app deployment
- Offer secure mobile app maintenance
- Provide secure mobile app updates
- Offer secure mobile app security
- Provide secure mobile app performance
- Offer secure mobile app analytics
- Provide secure mobile app reporting
- Offer secure mobile app support
- Provide secure mobile app training
- Offer secure mobile app documentation
- Provide secure mobile app compliance
- Offer secure mobile app governance
- Provide secure mobile app risk management
- Offer secure mobile app incident response
- Provide secure mobile app disaster recovery
- Offer secure mobile app business continuity
- Provide secure mobile app resilience
- Offer secure mobile app sustainability
- Provide secure mobile app innovation
- Offer secure mobile app growth
- Provide secure mobile app scalability
- Offer secure mobile app flexibility
- Provide secure mobile app interoperability
- Offer secure mobile app compatibility
- Provide secure mobile app accessibility
- Offer secure mobile app usability
- Provide secure mobile app user experience
- Offer secure mobile app customer satisfaction
- Provide secure mobile app loyalty
- Offer secure mobile app retention
- Provide secure mobile app engagement
- Offer secure mobile app conversion
- Provide secure mobile app revenue
- Offer secure mobile app profitability
- Provide secure mobile app ROI
- Offer secure mobile app value
- Provide secure mobile app impact
- Offer secure mobile app legacy
- Provide secure mobile app reputation
- Offer secure mobile app brand
- Provide secure mobile app identity
- Offer secure mobile app culture
- Provide secure mobile app spirit
- Offer secure mobile app soul
- Provide secure mobile app heart
- Offer secure mobile app mind
- Provide secure mobile app body
- Offer secure mobile app spirit
- Provide secure mobile app soul
- Offer secure mobile app heart
- Provide secure mobile app mind
- Offer secure mobile app body

**Did You Know?**

- 70% of users have had their accounts hacked
- 60% of users have had their personal information stolen
- 75% of users have had their credit card information stolen
- 85% of users have had their identity stolen



# 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

