RSAConference2016

Singapore | 20-22 July | Marina Bay Sands

Connect to Protect

Security Awareness Is Not Enough: Build Security Culture Using Science of Habits

Bikash Barai

Co-founder (Cigital India)

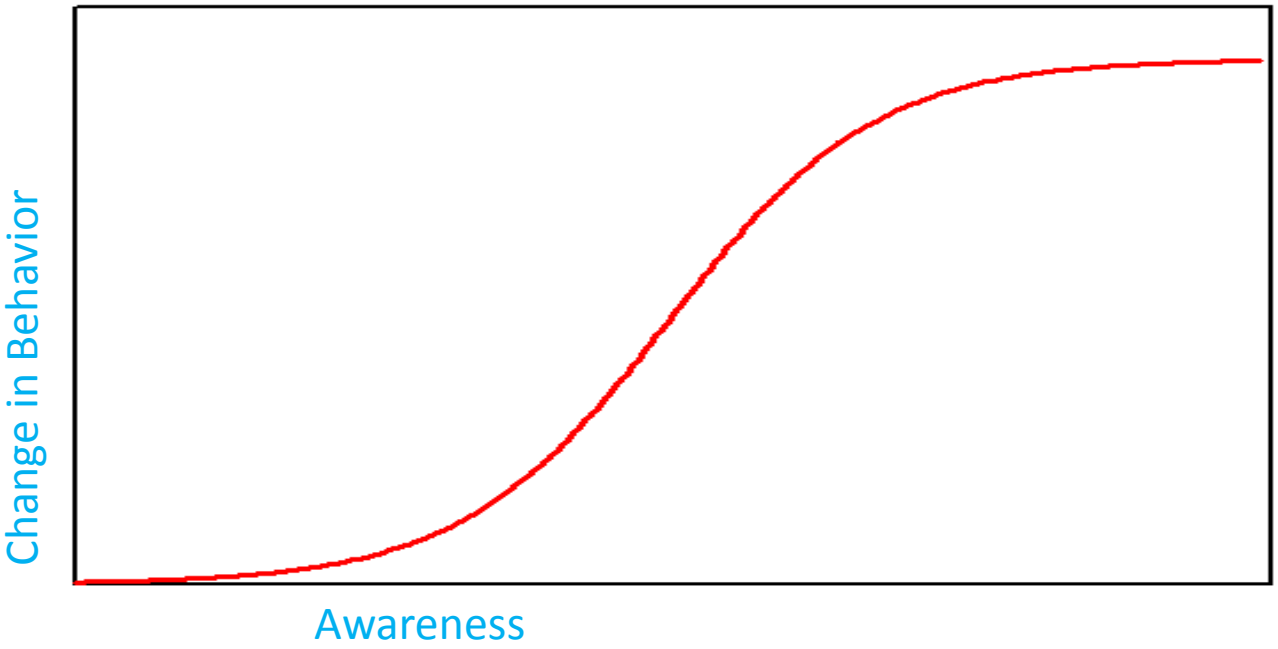
@bikashbarai1

#RSAC

Is Awareness Enough To Change Human Behavior?

Credit: Abd Allah Foteih

Awareness vs Change Of Behavior



Example: Continued security training beyond the baseline are unlikely to be effective - "Modifying Smartphone User Locking Behavior" – by Dirk et al (ACM – 2013)

What Else Do We Need?

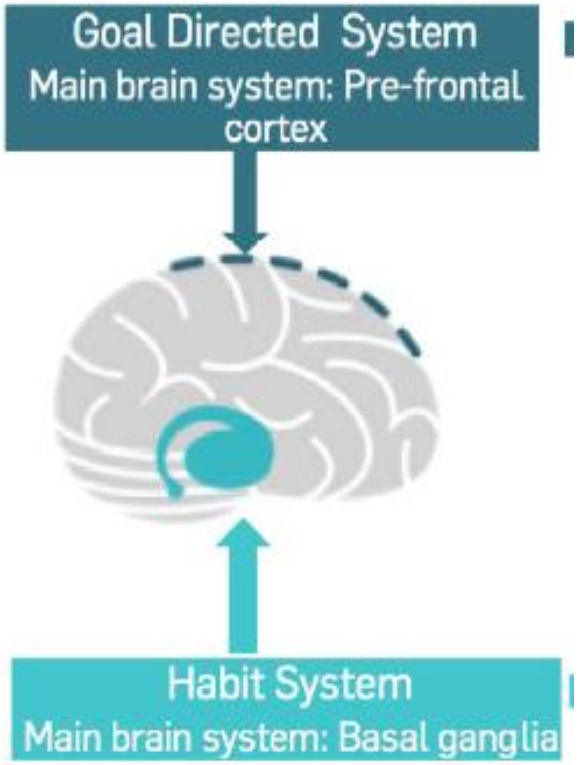
The Mystery of Eugene Pauly's Brain ..

Dr. Lary R. Squire
University of California, San Diego

Image Source: http://whoville.ucsd.edu/about.html

Goal Directed and Habit System

- **Goal Directed System (Pre-Frontal Cortex)**
  - Responsible for new or infrequent behaviors
  - Guided by attitudes, goals, values, knowledge
  - Conscious and deliberate
  - Slow
- **Habit System (Basal Ganglia)**
  - Very fast. Does not require thought or attention
  - Less conscious. More automatic



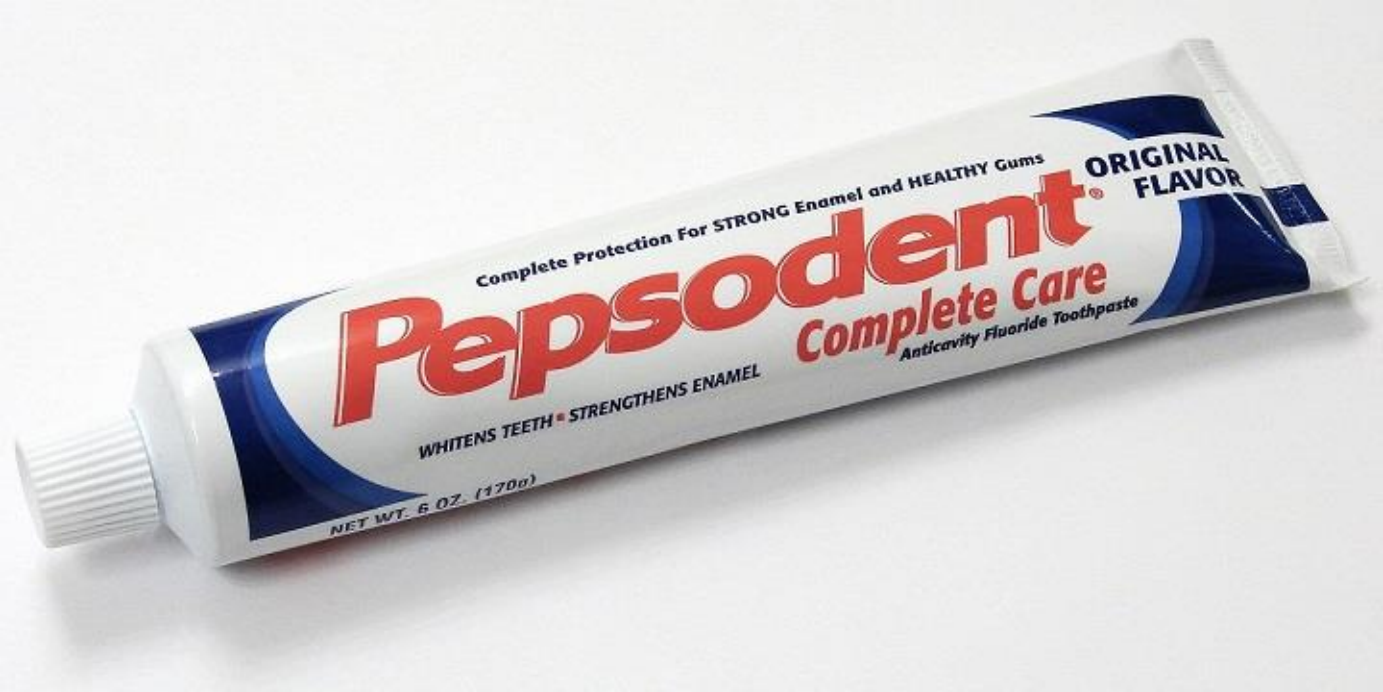
Credit: Neal et al – The Science of Habit…

Habits in Action..

- **40% of our daily actions are driven without thinking**
- Examples of Habits in action
  - Changing gears
  - Getting out of elevator in wrong floor
  - Tying Shoe knots
- Bad habits in action
  - Checking phone/blackberry during the middle of sleep
  - Clicking phishing links
  - Writing down passwords in open

How To Build A New Habit?

Story of Pepsodent ..



https://upload.wikimedia.org/wikipedia/en/8/88/Pepsodent-0179c.jpg

Trigger – Routine – Reward (& Craving)

Trigger:

Feel Tooth Film with tongue

Routine:

Brushing Teeth

Reward:

Great Smile

https://i.ytimg.com/vi/rf1Bs2XpwFI/maxresdefault.jpg

Image Credit: Wikipedia

Image Credit: Seth Lemmons

Steps for Building New Habits

- Step 1: Find a Predictable and Recurring Trigger
- Step 2: Devise the new Routine/Habit
- Step 3: Find the Reward

- Practice, Practice, Practice without exceptions

How To Change A Habit?

Old Habits Never Die

Example – Changing A Habit

Trigger: Boredom

Routine: Have a Whisky

Reward: Feel Happy

Cigital

Image Credit: Wiki

Example – Changing A Habit

Trigger:
Boredom

New Routine:
Talk to a friend

Reward:
Feel Happy

Image Credit: Wiki

3 Steps for Changing Old Habits

- Identify and Deconstruct the Habit
  - Find the Trigger
  - Find the “real hidden reward” – Experiment to discover
  - Find the Trigger-Routine-Reward-Craving model
- Find an alternative routine to satisfy the “real hidden reward”
- Practice. Practice. Practice.

“Hard Thing” about “Easy Things”..

Understanding Buffer Overflow - Easy

Finding A vulnerability - Hard

Writing A "Reliable" Exploit- Very Hard

Hard or Easy?

- Several “toothpaste” companies went bankrupt
- Coke, McDonalds campaigns..

- **What is hard about it?**
  - Finding a “Reliable” trigger and reward
  - Creating craving and making it stick

Applying The Science Of Habit
In Information Security & Life..

Example 1: Create Habit of Locking Computer Screen..

- Goal: Locking system while leaving desk
  - Trigger – Getting up from chair/Leaving the system
  - Routine – Lock your computer
  - Reward – Feeling of security
- Rehearse or Repeat at least 20 times
- If you forget then go back to seat and repeat the routine

Example 2 – Change the Habit of Writing Down Password in Open Areas

- Goal: Stop the habit of writing down password areas
  - Trigger – New password setting request
  - Old Routine – write down the password
  - New Routine – “write down the clue” or “Use a Scheme to generate new passwords”
  - Reward – Feeling of security
- Rehearse or Repeat

Example 3: Preventing Phishing

- Old Habit
  - Trigger: Legitimate entity asks for personal details
  - Routine: Share the details
- New Desired Habit
  - Trigger: Legitimate entity asks for personal details
  - New Routine: Validate the legitimacy of the entity
- Practice. Practice. Practice

Example 4- Create Secure Coding Behavior

- Goal – Ensuring coders use secure coding functions
  - Trigger – Typing a function
  - Old Routine – Type insecure function
  - New Routine – Use intervention method to prompt secure function
  - Enough practice
  - Automatic use of secure function

Habits in Day to Day Life..

- Playing/Exercise everyday
- Controlling anger outbursts..

Story of Alcoa… And Keystone Habit

Playbook for Changing Security Culture

Using Habits for Cultural Change

- Augment Awareness with a Habit Strategy
- Reduce friction or Create friction based on goals
- Utilize “Keystone Habit”

Other Learning for Cultural Change

- Certainty of negative incentive and not Severity has high impact
- Group sharing has positive impact
- Start at the Top
- Leverage a disaster
- Start with a why

Current State of Industry

Current State of Industry

- There is very little research or adoption of directly using science of habits in organizational security awareness programs
- A few technologies for awareness are using habit forming principles (e.g. Automated Social Engineering Drill Tools, Secure Coding Tools that prompt insecure coding while being written)
- There is tremendous need and wide gap for the industry to use techniques of forming/changing habits beyond traditional awareness programs

Apply What You Learned..

Apply What You Learned

- **Next Week**
  - Choose 1 habit that you want to change or build
  - Identify a small group for experiment
  - Experiment
- **First 3 months**
  - Find the most important habits to change in your organization
  - Create an organization wide plan for habit change drills
  - Make people practice at least 20 to 30 times in a short time frame. (Group activities, Simulation exercise, Wargames etc)
  - Measure the success of the program

- **After 6 months**
  - Assess the success of the program based on the metrics defined
  - Reassess the risky and secure behavior and create a new program

Awareness Is Not Enough
Invest In Forming Lasting Habits

Practice Does Not Make Perfect
"Perfect Practice" Makes Perfect

Want To Engineer A Habit?
Let's Meet At The Bar ..

Questions please..

Bikash Barai

bbarai@cigital.com

@bikashbarai1

References and Other Studies ..

- Balleine et al – Goal directed instrumental action: contingency and incentive learning and their cortical substrates
- Kahneman – Thinking fast and slow
- Duhigg- The power of habit
- Neal et al – The pull of the past when do habits persist despite conflict with motives?
- Rothman et al- Reflective and automotive processes in the initiation and maintenance of dietary change
- Sheeran et al – Implementation intentions and repeated behavior..
- Wood et al – A new look at habits and habit- goal interface
- Wood et al- The habitual consumer
- Wood et al- Habits in everyday life: thought emotion and action