Security Awareness Has Failed: A Suggested New Approach

François van Heerden
Senior Security Education Specialist
Cyber Security Branch,
Treasury Board Secretariat

SecTor 2014
How Far Would You Go ...
For a cup of tea?
It’s all about risk!
Some questions to ask:

- How successful is your organization’s security awareness program?
  - Have incidents increased, decreased or do you really know?

- What is the focus of your organization’s security awareness program?
  - Is it just to meet legislated requirements?

- What is your organization’s risk tolerance?
Security Awareness VS. Risk Management

- Security Awareness
  - End user reaction?
    - Eyes glaze over
    - Mind shuts off

  VS

- Risk Management
  - End user reaction?
    - How does this apply to me?
    - Pays attention
3 Pillars of Risk Management
3 Pillars of Risk Management

- **Technology**
  - Determine physical risks and mitigations
  - Tool – TRA / Architecture Review

- **Processes**
  - Determine if gaps exist in processes
  - Tool – Process audit review

- **People**
  - Awareness and behavior / culture change
  - According to statistics – greatest risk lies here!
Security Awareness Has Failed!

- 30 years of security awareness
- 30 years of minimal or no impact
- 30 years has become “check box” mentality

**PROOF:**

- We still see exactly the same behaviors and lack of application of corrective measures!
Security Awareness Has Failed!

- Approach across industry and business has been:
  - A single solution for all awareness activities
  - Standardized “awareness” program
    - Generic
    - Not necessarily applicable to every audience
“One Size Fits All”

When we said "one size fits all," we didn't mean all at the same time.

Used with permission of Jon Carter
“One Size Doesn’t Fit All”
“One Size Doesn’t Fit All”

Because:

- Adults learn differently
- Work circumstances vary dramatically
- Business drivers vary dramatically
- Risk issues vary dramatically
Change Drivers

- Workforce mobility
- Portable devices (BYOD)
- Tele-work and alternate work locations
- Public demands for services / access
- Speed of technological change
What’s to be done?

- A new approach that is:
  - More personal to the audience (end user)
  - Provides context that is applicable to personal and business environments
  - Risk-based
  - Starts with the user at home!
Understand the audience

- What motivates people?
  - W I I FM – people’s favorite radio station
Personal Self Interest

- What’s
- In
- It
- For
- Me?
Apply elements of marketing

- 6 Principles of Persuasion
  - Reciprocity
  - Commitment and Consistency
  - Social Proof
  - Liking
  - Authority
  - Scarcity
Reciprocity

- We generally aim to return favors, pay back debts, and treat others as they treat us.

- According to the idea of reciprocity, this can lead us to feel obliged to offer concessions or discounts to others if they have offered them to us. This is because we're uncomfortable with feeling indebted to them.
Commitment and Consistency

- Once we've committed to something, we're then more inclined to go through with it.

- For instance, you'd probably be more likely to support a colleague's project proposal if you had shown interest when he first talked to you about his / her ideas.
Social Proof

- This principle relies on people's sense of "safety in numbers."

- We're more likely to work late if others in our team are doing the same, put a tip in a jar if it already contains money, or eat in a restaurant if it's busy. Here, we're assuming that if lots of other people are doing something, then it must be OK.

- We're particularly susceptible to this principle when we're feeling uncertain, and we're even more likely to be influenced if the people we see seem to be similar to us. That's why commercials often use moms, not celebrities, to advertise household products.
Friendship /Liking

- We're more likely to be influenced by people we like. Likability comes in many forms – people might be similar or familiar to us, they might give us compliments, or we may just simply trust them.

- Companies that use sales agents from within the community employ this principle with huge success.

- People are more likely to buy from people like themselves, from friends, and from people they know and respect.
Authority

- We feel a sense of duty or obligation to people in positions of authority. This is why advertisers of pharmaceutical products employ doctors to front their campaigns, and why most of us will do most things that our manager requests.

- Job titles, uniforms, and even accessories like cars or gadgets can lend an air of authority, and can persuade us to accept what these people say.
Scarcity

- Things are more attractive when their availability is limited, or when we stand to lose the opportunity to acquire them on favorable terms.

- For instance, we might buy something immediately if we're told that it's the last one, or that a special offer will soon expire.
Cyber Security Branch

Applying those principles to Risk Management

By applying marketing principles to Awareness and Risk Management:

- Greater likelihood of adoption by the end user
- Buy-in because we are making it personal
Some examples

- The same message BUT
  - Different context
  - More relevant and timely
- It’s all about marketing ...
“Outdated approach”

- “Big Stick” – threaten corrective action

- MESSAGE - Don’t use free Wi-Fi

- No explanation or reasons given
“Future approach”

- Ever wonder what can happen when you use free “WiFi?"
“Future approach”

- Explain risks in:
  - Simple terms
  - How it applies to the user
  - What can be done to prevent compromise?
“Outdated approach”

- Acceptable Use of I & IT Resources Policy

- List examples of what isn’t allowed and infer that there are other things as well

- Threaten action but rarely carried it out because there is little “follow-up” or enforcement
“Future approach”

- Give the user a personal reason to want to implement security measures:
  - Do you want your personal information to appear in an FOI response?
  - Do you want your personal information / activities known to all of your colleagues?
  - Do you want your personal health and financial information to become public knowledge?
“Outdated approach”

- Clean desk policy
- Just DO it!
“Future approach”

- Risks of data loss

- Multiple versions of documents – which is the real / newest document?

- Do you want to be the person who is responsible for giving incorrect information that may impact life, limb and health of a member of the public?
Current awareness approach

- Single, generic awareness package
- Everyone gets the same material – whether it is applicable or not
- Most people can “click through” entire package and get credit even if they weren’t paying real attention
Future awareness programs

- Request comes in – consult with client management team
- Research client – contact CSOC (Cyber Security Operations Center) and find out what they are seeing
- Using modular format, pull those parts needed for awareness
- Use actual incidents from the recipient’s business area to reinforce messages for managing risk
Will this approach work?

- Everyone talks about metrics – so how do we measure success?
  - Reduction in incidents
  - Changes in personal behavior
Suggested Approach Metrics

- After delivering cyber security awareness:
  - Follow up questionnaires – immediately after sessions
  - By e-mail – 30 days after
  - 6 months afterwards (test retention)
  - Follow up with Cyber Security Operations Center to see if incidents are decreasing
Anecdotal Evidence To Date

- Recent presentations to Ontario Works and Ontario Disability Support Program service providers
- Responses back from staff that they spoke to friends and family
- Installation of anti-virus, anti-SPAM, anti-malware on personal devices – iPhones, iPads and Android phones / tablets – right at presentation!
Anecdotal Evidence To Date

- Significant increase in requests for:
  - Risk management presentations at branch, unit meetings, CBTs
  - Links to applicable information for end users
Conclusion:

- A “risk management” approach to Cyber Security Awareness:
  - Should have a better “uptake” of the security messages
  - Should be more effective because it uses “a marketing/social engineering approach”
  - Should assist in creating a “security culture” because it starts with the end user at home
  - Should provide better metrics based on better identification of success factors
Information Security Forum

- ISF released a report February 2014 detailing a new approach to Cyber Security Awareness

- Provides insight into appropriate metrics and how to gather the necessary information
References on learning

- Graphic novels in schools to enhance learning
  - [http://ivn.us/2013/05/21/study-shows-graphic-novels-add-value-to-k-12-student-learning/](http://ivn.us/2013/05/21/study-shows-graphic-novels-add-value-to-k-12-student-learning/)

- Graphic novels for teaching science
  - [http://libguides.aurora.edu/content.php?pid=112928&sid=850840](http://libguides.aurora.edu/content.php?pid=112928&sid=850840)
Harnessing the Science of Persuasion
by Robert B. Cialdini

- **Liking**: “People like those who like them.”
  - Uncover real similarities and offer genuine praise.
- **Consistency**: “People align with their clear commitments.”
- **Reciprocity**: “People repay in kind.”
  - Give what you want to receive.
- **Authority**: “People defer to experts.”
- **Social Proof**: “People follow the lead of similar others.”
- **Scarcity**: “People want more of what they can have less of.”
  - Use peer power whenever it’s available.

- **Make their commitments active, public, and voluntary.**
- **Expose your expertise; don’t assume it’s self-evident.**
- **Highlight unique benefits and exclusive information.**
Questions?

- francois.vanheerden@ontario.ca