RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Making The Security Super Human: How To Effectively Train Anyone/Anything.

SESSION ID: STU-T08B

Katrina Rodzon

Security Awareness and Behavior Modification
@krodzon

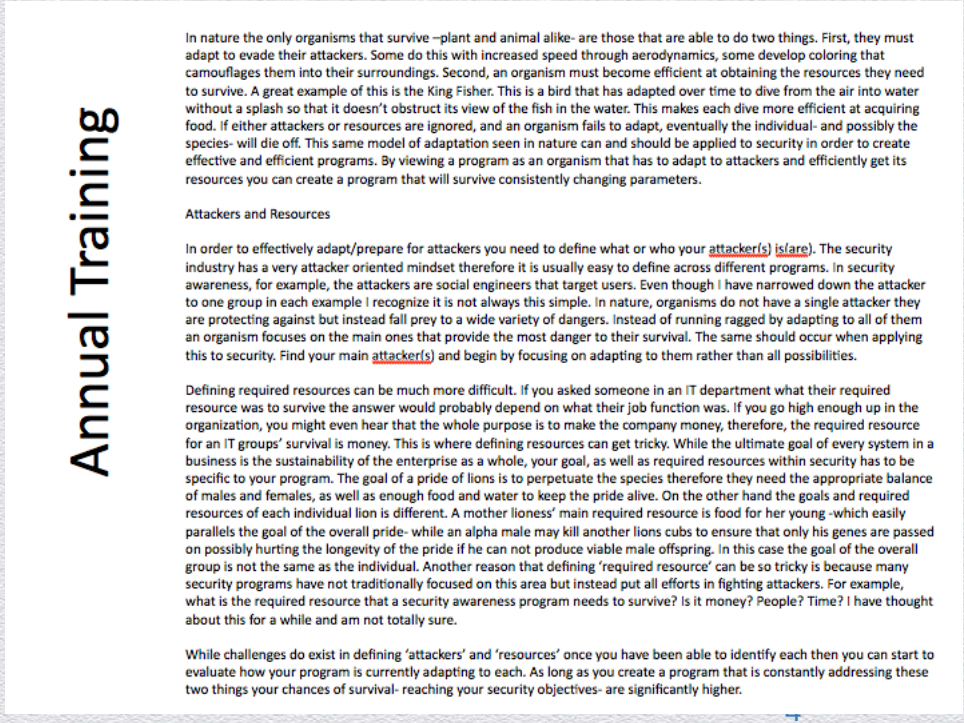
Behavior Modification & Cognition

Instinct and Training

aff + Tra g

Behavior and Punishment

- What is punishment?



Annual Training

In nature the only organisms that survive –plant and animal alike- are those that are able to do two things. First, they must adapt to evade their attackers. Some do this with increased speed through aerodynamics, some develop coloring that camouflages them into their surroundings. Second, an organism must become efficient at obtaining the resources they need to survive. A great example of this is the King Fisher. This is a bird that has adapted over time to dive from the air into water without a splash so that it doesn't obstruct its view of the fish in the water. This makes each dive more efficient at acquiring food. If either attackers or resources are ignored, and an organism fails to adapt, eventually the individual- and possibly the species- will die off. This same model of adaptation seen in nature can and should be applied to security in order to create effective and efficient programs. By viewing a program as an organism that has to adapt to attackers and efficiently get its resources you can create a program that will survive consistently changing parameters.

Attackers and Resources

In order to effectively adapt/prepare for attackers you need to define what or who your attacker(s) is(are). The security industry has a very attacker oriented mindset therefore it is usually easy to define across different programs. In security awareness, for example, the attackers are social engineers that target users. Even though I have narrowed down the attacker to one group in each example I recognize it is not always this simple. In nature, organisms do not have a single attacker they are protecting against but instead fall prey to a wide variety of dangers. Instead of running ragged by adapting to all of them an organism focuses on the main ones that provide the most danger to their survival. The same should occur when applying this to security. Find your main attacker(s) and begin by focusing on adapting to them rather than all possibilities.

Defining required resources can be much more difficult. If you asked someone in an IT department what their required resource was to survive the answer would probably depend on what their job function was. If you go high enough up in the organization, you might even hear that the whole purpose is to make the company money, therefore, the required resource for an IT groups' survival is money. This is where defining resources can get tricky. While the ultimate goal of every system in a business is the sustainability of the enterprise as a whole, your goal, as well as required resources within security has to be specific to your program. The goal of a pride of lions is to perpetuate the species therefore they need the appropriate balance of males and females, as well as enough food and water to keep the pride alive. On the other hand the goals and required resources of each individual lion is different. A mother lioness' main required resource is food for her young -which easily parallels the goal of the overall pride- while an alpha male may kill another lions cubs to ensure that only his genes are passed on possibly hurting the longevity of the pride if he can not produce viable male offspring. In this case the goal of the overall group is not the same as the individual. Another reason that defining 'required resource' can be so tricky is because many security programs have not traditionally focused on this area but instead put all efforts in fighting attackers. For example, what is the required resource that a security awareness program needs to survive? Is it money? People? Time? I have thought about this for a while and am not totally sure.

While challenges do exist in defining 'attackers' and 'resources' once you have been able to identify each then you can start to evaluate how your program is currently adapting to each. As long as you create a program that is constantly addressing these two things your chances of survival- reaching your security objectives- are significantly higher.

Time Out!

Behavior and Reward

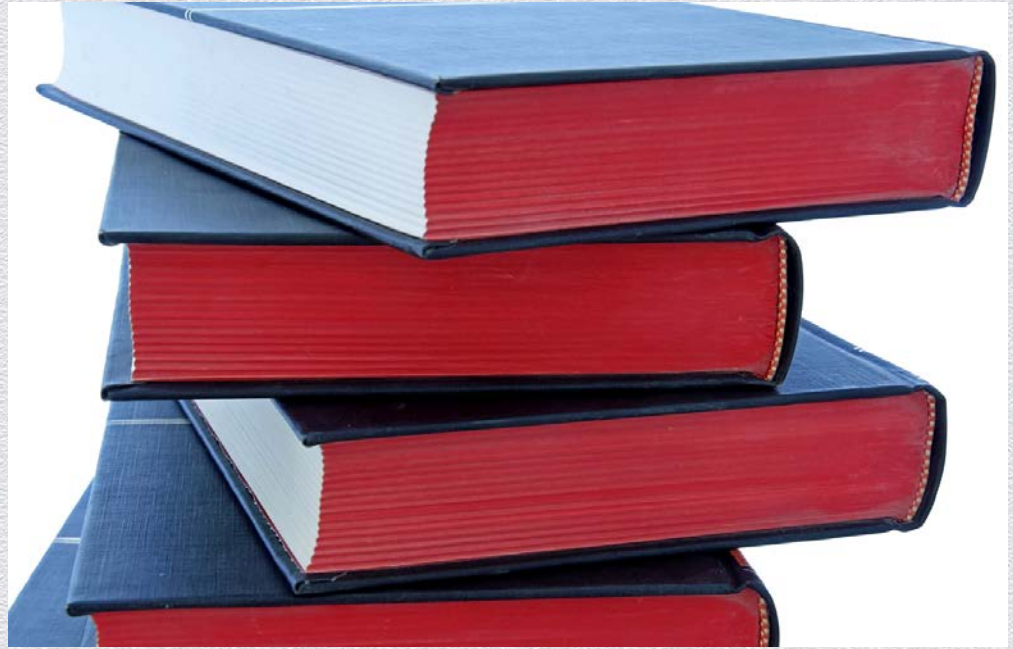
- What is reward?
  - What is the desired behavior in training?
- Reward with good content

What Makes Good Content?

- Cognition
  - Motivation
  - Attention
  - Memory

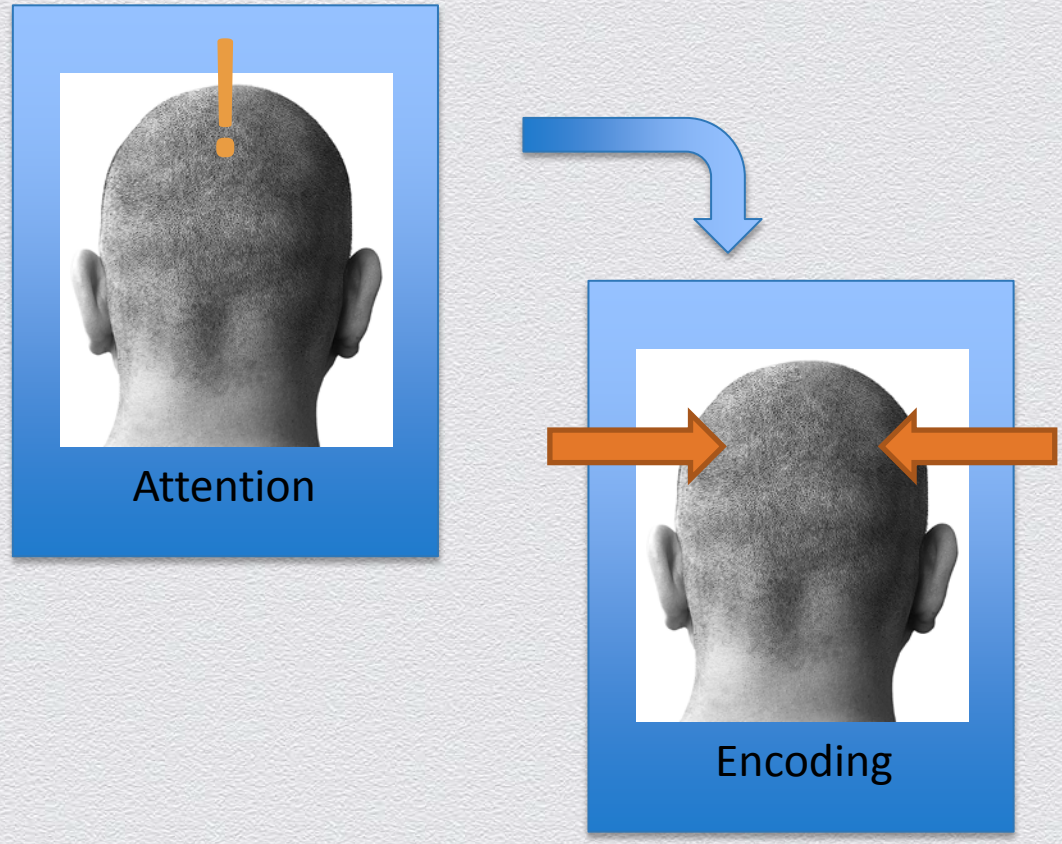
Motivation

- Know your audience



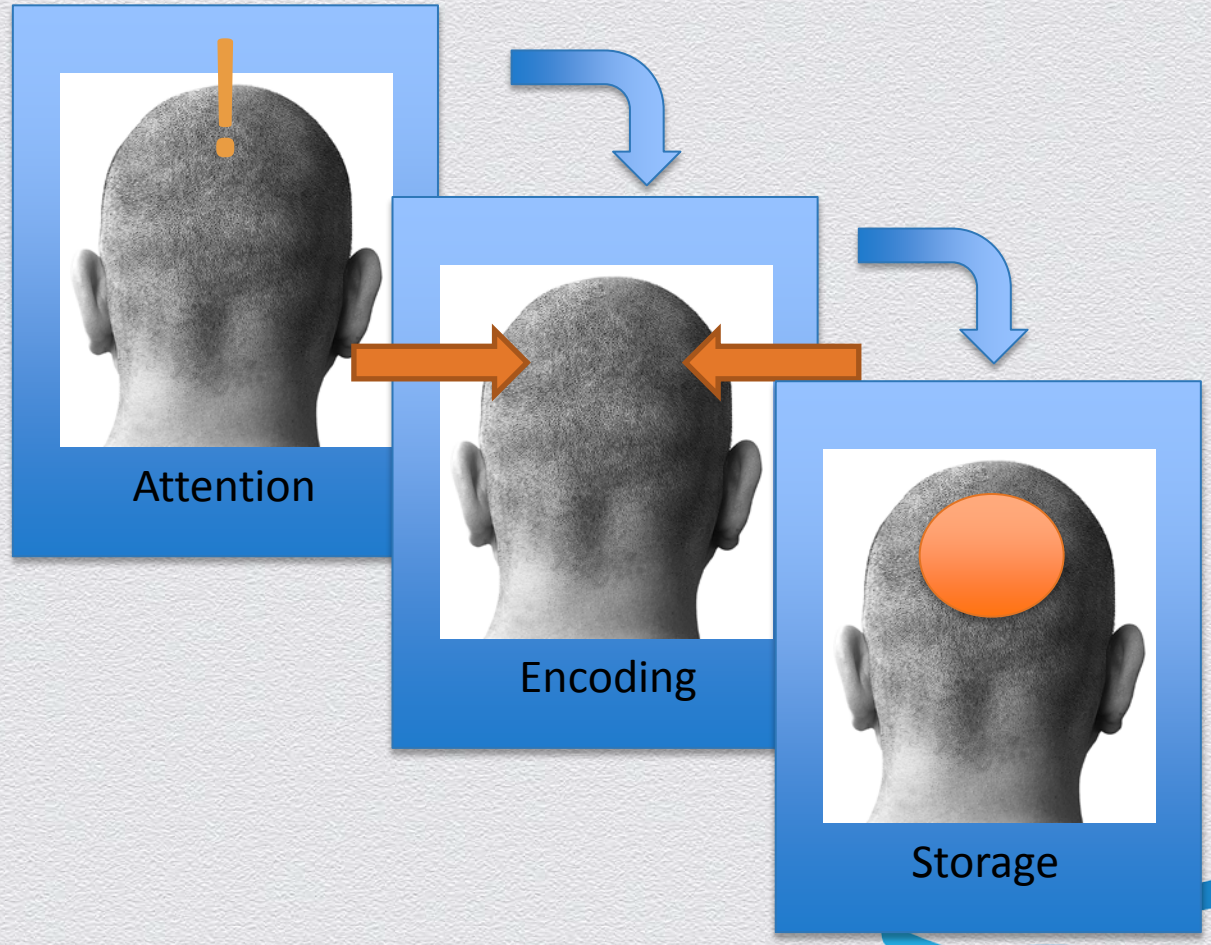
Attention

- Limited
  - 5-10 minutes
  - Easily taxed
- Chunk Information



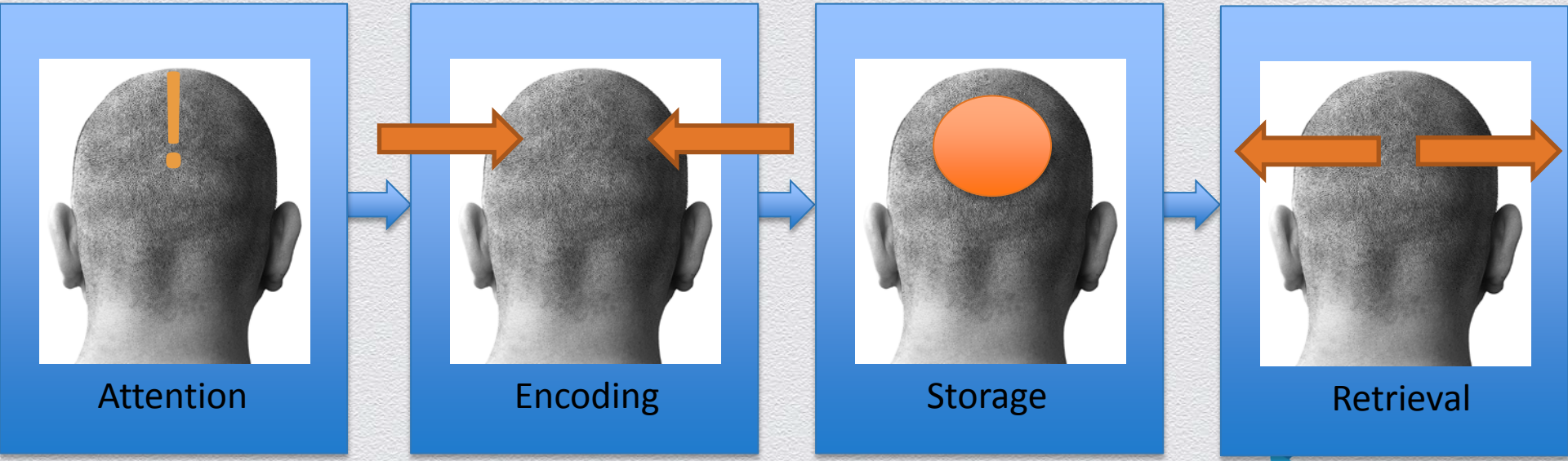
Memory

- Don’t overload
- Make users apply



Using An LMS

- Creating a foundation
- Make your LMS a resource not an annual destination



How To Train Anyone/Anything.

Thank you.

SESSION ID: STU-T08B

Katrina Rodzon

krodzon@gmail.com
@krodzon