Message	Answer
How do you quantify sensitivity to social engineering?	This gets back to understanding what you are defining as social engineering (that first box in the sequence on my slides). Does social engineering mean shoulder surfing? Giving up information on the phone? People leaving doors unlocked? Or something more specific to your organization? Once you have defined this then you can start to quantify it.
If your systems are restricted to a particular password length then how does this work with your measurements?	All metrics are set up around the parameters of the organization. Password length would just be one of the things that you tested for/measured.
What are your thoughts on actually demonstrating awareness, i.e. showing people how quickly a weak password is cracked compared to a strong password or what SQL injection actually looks like?	Video demonstrations are the best. Their is something very powerful about a video showing a password getting cracked. It demonstrates that it doesn't take a huge amount of skill or technology and that is can happen at any moment. It's the same premise as actions speak louder than words. Always make sure it's anonymous and that you aren't attacking any one person/department in particular.
Is there a "standard" list of things that should be monitored? I'm sure it will vary from company to company - just looking for a general list or starting point.	I hestitate to give a list because it really does depend on what you are doing within your company. You can start with metrics around passwords and phishing - since these are things that impact every organization - and then go from there. Do you have security risk around physical security? Email use? Information on social media? Unapproved thumb drives? Ask yourself "what are my top 5 issues within my organization that I would change with the snap of my fingers if I could?"

How do you measure something softer like Social Media usage?	Social media 'usage' I don't think you can unless they do it on a work computer that you own but i'm not sure that's what you want to track anyway.
What are your thoughts around building a security culture rather simply running topic based awareness	I think building a security culture is tantamount to security in general. If you don't know and understand your users/co-workers any efforts you are doing to influence/change their behavior is pretty much just a shot in the dark- similar to buying someone that you have never met a christmas present.
I am not entirely sure how you can use password cracking metrics with before and after results.	This example was to demonstrate the concept of A/B testing. A/B testing is very powerful to demonstrate that you specific manipuation/content/program/message had an impact. You test the behavior before -to get a baseline- and then see what happens after.
Can you tell us what and how they measure metrics for BYOD? I imagine other than an anonymous survey it could be tricky to measure.	You are completely right that it is tricky and at this point a lot of organizations have had to get creative. In the best case scenario I worked with an organization that was able to identify BYOD from activity- but not WHO they were- because of a program that the IT group had actually set up that was totally different. In some cases, it really is a matter of asking which presents issues within itself.

Do you have any recommendations on getting uppoer management onboard with 'experiments', to ensure associates are not desensitized by them or feel 'big brother' but still achieve results?	Great question. First, when you are doing content/message/event/product testing with a small group of individuals you should always keep upper management in the loop. This does prevent the 'big brother' feel while allowing you to test. Second, do not go crazy with these. If you are testing small groups of people monthly then it will come across as scatter brained to upper management and as an inconvenience to users/associates.
Why not use metrics to stop depending on passwords but fixing the issue all together by approaching this from a defense in depth approach with adding of two-factor security controls?	Metrics are not implemented as a means of stopping/increasing/changing any behavior. They are simply the measurement to see if your control/message was actually effective or if the user ignored or bypassed it somehow.
What is the hardest metric you have implemented?	Key sharing as an aspect of physical security.
What are the "best" ways to present metrics to management?	Easy to understand graphs with lots of 'why this matters.' Simply presenting lots of data might be appealing to you but they just want the big picture with the 'how this matters to what i find important'
In my group we are talking about creating a risk aware culture. Is that "correct" in one way?	This will depend on if that is why they aren't changing their behavior. If it's a matter of awareness then you are on the right track but it could be motivation, difficulty, or forgetting.