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

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

50 Shades of Security: Whipping Users Into Submission

SESSION ID: EXP-R02

Ira Winkler, CISSP

President
Secure Mentem
@irawinkler
ira@securementem.com

Full Disclaimer

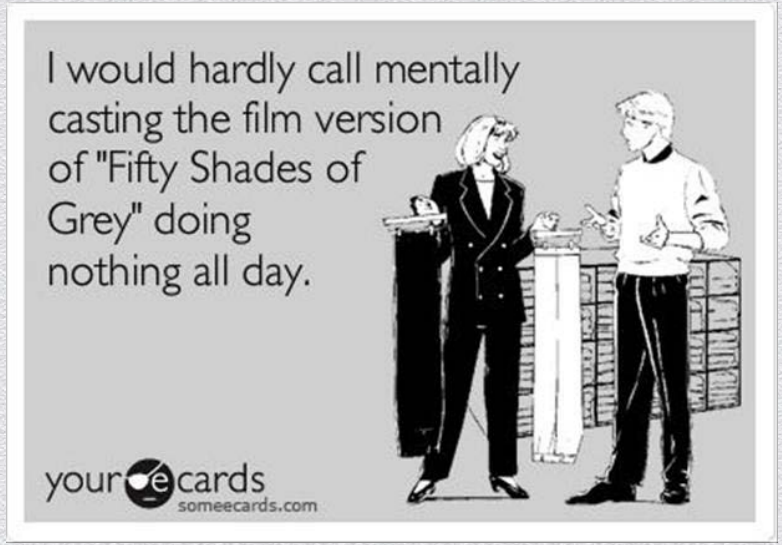
- If you are easily offended, leave now
- I offend people talking about *The Wizard of Oz*
- While I won't go into graphic detail, if you are offended by the content and subject matter of *50 Shades of Grey*, you will be offended by the presentation
- If you haven't heard of *50 Shades of Grey*, you should probably leave

Seriously…

- Some of you are here just because of the title
- But if you wonder how bad this can get, assume you will be offended and leave now
- RSAC says probably won't listen to this warning, but I tried
- This is a toned down version of what was initially submitted

50 Shades of Grey as a Phenomenon

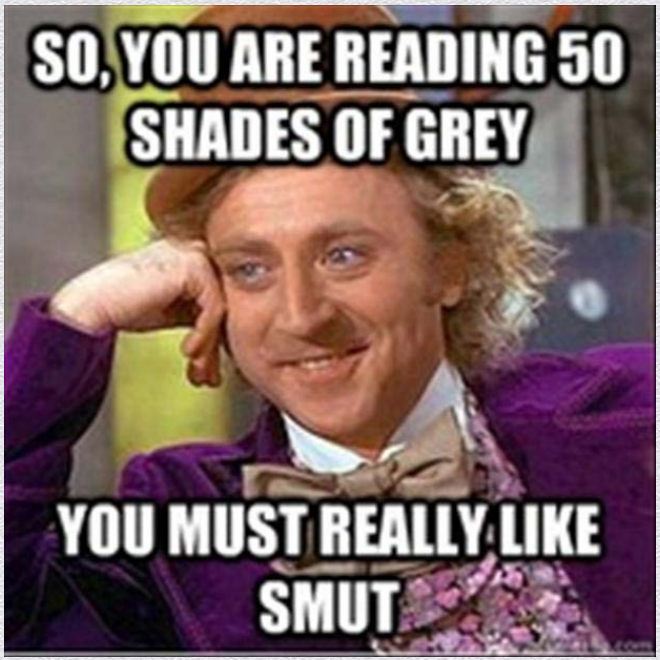
- I don’t know why, but it is a bestseller
- The trilogy topped the bestseller lists for extended periods of time
- Subject of pop culture
- Became a question in a political debate
- Made Mommy Porn mainstream
- More than 70,000,000 copies sold



50 Shades of Grey Summary – Edited

- Essentially *Twilight* fan fiction
- Writer meets reclusive billionaire
- Billionaire seduces writer
- Wants her to sign contract about behaviors she agrees to engage in
- Engages is some activity without a contract, but knowledge of what she is involved in
- Struck a chord with many people

The Reality - Edited



- It is a bad book, but it demonstrates a counterintuitive relationship
- Behaviors that are apparently against personal interests are agreed to
- Terms of agreement are made clear

Not Just Mommy Porn – Edited

- Accidentally depicts a complex psychological relationship
- Defines agreements to behaviors that are potentially against the better interest
- Demonstrates that a feeling of security can overcome hesitations of not being in control

Psychology of People Engaged in 50 Shades-like Activity

- Technically considered a disorder by the American Psychiatric Association until 2013
- Studies indicate that practitioners are more conscientious
- Tend to be better adjusted as well
- Submissives tend to be more agreeable
- Dominants are less agreeable
- 92% of women and 52% of men can be submissive

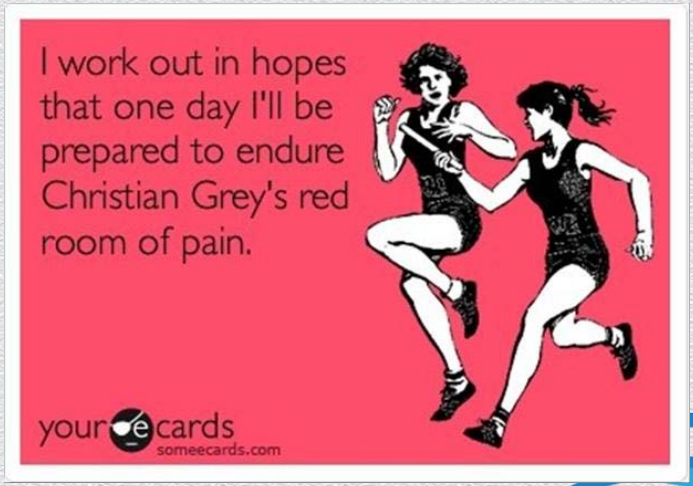
The Irony of *50 Shades of Grey*-like Activities

- The submissives have ultimate control
- They can use the “Safe Word” and say, “No” at anytime
- In order for a submissive to feel comfortable submitting, they have to feel ultimately safe
- It creates the concept that while they supposedly have no control, submissives must approve what they submit to
- The contract in *50 Shades of Grey* is actually for the benefit of the woman, more than the billionaire

Negotiations From 50 Shades – Edited

- Types of activities engaged in
- Timing of activities
- Limitations of activities
- Availability of participants
- Communications methods
- Non-Disclosure Agreements

- Health of participants
  - Regular physicals
  - Exercise regiments
  - Medications



Fundamental Human Needs

- Certainty
- Variety
- Security
- Connection
- Growth
- Contribution

- Several different models, but the concepts all the same
- This activity satisfies all of those needs for participants

Should Security Programs Adopt Similar Models?

- It is counterintuitive for people to want to submit to burdensome regulations
- Security creates limitations
- Security can create certainty, connection, contribution
- While there might not be a sexual element to security, it satisfies other psychological needs

Security Requires Users to Follow Rules

- Submissives are agreeable and roughly 75% of people are prone to be agreeable
- Actions may be limited by rules
- They must behave a certain way online and offline
- They must not do things that they want to do
- They must do things that they don’t want to do

Typical Security Program Methodology

- Employees sometimes exposed to an NDA before they are hired
- Pre-employment screening frequently includes drug test, background check, and sometimes psychological evaluation
- Might be told some rules as part of new hire program
- Information pushed out periodically
- Sometimes security policies are built into operational procedures
- Penalties for violations are ambiguous
- Generally passive efforts

NSA Security Program

- Made aware of operational security concerns during recruitment process
- Meet with security staff during interviews
- Hiring materials stress “Secret” nature of affiliation
- Documents clearly lay out security responsibilities
- 2-3 days of security awareness upon hiring
- Penalties are clear
- Environment supports security behaviors and awareness

NSA Security Satisfying Human Needs

- Certainty
  - There is an expectation of process
- Variety
  - Cloak and dagger nature
- Contribution
  - Contributing to national security
- Connection
  - Camaraderie in sharing secrets
- Growth
  - Seems to allow people to learn more about security
- Security
  - It is a very safe environment

Overbearing, But It Works

- Despite Snowden, there are very limited losses
- There are likely incidents that are not public, but they are limited
- Few people quit because of security limitations
- There are possibly more than 1,000,000 people with clearances
- They report to work on a regular basis and adhere to security requirements

Whipping Users Into Submission…And They Like It

Incorporate Security Into The Interview Process

- Demonstrate security processes in the interview process
  - Instill a sense of certainty and security
- Define security expectations in interviews
- Prior to hiring a person, ensure that they have copies of security policies in advance
- Provides the company with additional legal protection as well
- Knowing they were aware of the security requirements prior to accepting employment makes it voluntary

Incorporate Security Into the Hiring and Indoctrination Process

- Paperwork and expectations should be clearly defined, before the person accepts employment offer
- Ensures security expectations are clearly defined
- Kind of like a Dominant and submissive negotiating a contract
- They have ultimate control as they can always quit, but they accepted employment knowing their requirements

SECURE MENTEM

Throughout Employment

- Ensure that security practices are consistently enforced
- Have a security routine
- Don’t show weakness in enforcement of security practices
- Demonstrate consistency in process
- This is not just about awareness
- Technology and process implements security, as well as the people

SECURE MENTEM

Upon Separation

- You need to ensure that the contract is reviewed
- Refresh security requirements
- Ensure that they know that you will protect their interests as well
- Security responsibilities are mutual

Consider Establishing a Security Focus Group

- Solicit broad employee participation
- Define security requirements
- Get group input and implementation recommendations
- Let the group negotiate security procedures
- Provide methods for continued feedback and updating of procedures as feasible

It Is a Management Process

- While this may seem like a major shift in security, it really isn't
- Companies put requirements on employees in other forms
  - Adding security as an expectation in advance is not a major change
- Defining expectations can provide other benefits to the organization as well
- Employees should understand information security is a major concern
- It should be an evolutionary process to implement this
- Admittedly more realistic for some organizations than others

Conclusions

- This started as a joke, but there are important lessons
- Most people actually don’t mind security when it is a clearly laid out expectation
- It should be a two way contract
- You expect to get from employees what you want
- You give them what they want, need and expect
- Unfortunately security is not typically defined as an expectation and contract, and maybe even a negotiation, but it should be done

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Ira Winkler, CISSP

ira@securementem.com

@irawinkler

www.facebook.com/ira.winkler

www.linkedin.com/in/irawinkler

@SecureMentem