Trust, Mental Models, Semantic attacks, Social Engineering, and User Education

Jie Chen

Outline

- Concepts Review
- Why user education is important?
- Different views in user education
  - Traditional perspective
  - Economic perspective
  - Usability perspective
- Exercise
- A Vision: People Centric Security

Concepts Review

- Semantic attack:
  - A computer-based attack that exploits human vulnerabilities rather than system vulnerabilities
- Social engineering
  - the exploitation of the natural human tendency to trust
- Mental models
  - existence of human risk heuristics (perceptions)

Why user education is important?

- “Only amateurs attack machines; professionals target people.”

  ---Bruce Schneier

- Users are the weakest link

- Social Engineering
  - Low cost, not very sophisticated, widely-reached, and effective

Why user education is important?

- A Clinical Study of Risk Factors Related to Malware Infections

User characteristics

- ☒ Gender
- ☒ Age
- ☒ Status
- ☒ Field
- ☒ Computer Expertise

User behaviors

- ☒ Browser used
- ✚ Applications installed
- ✚ Websites visited
- ✚ Types of websites visited

Different Views in User Education

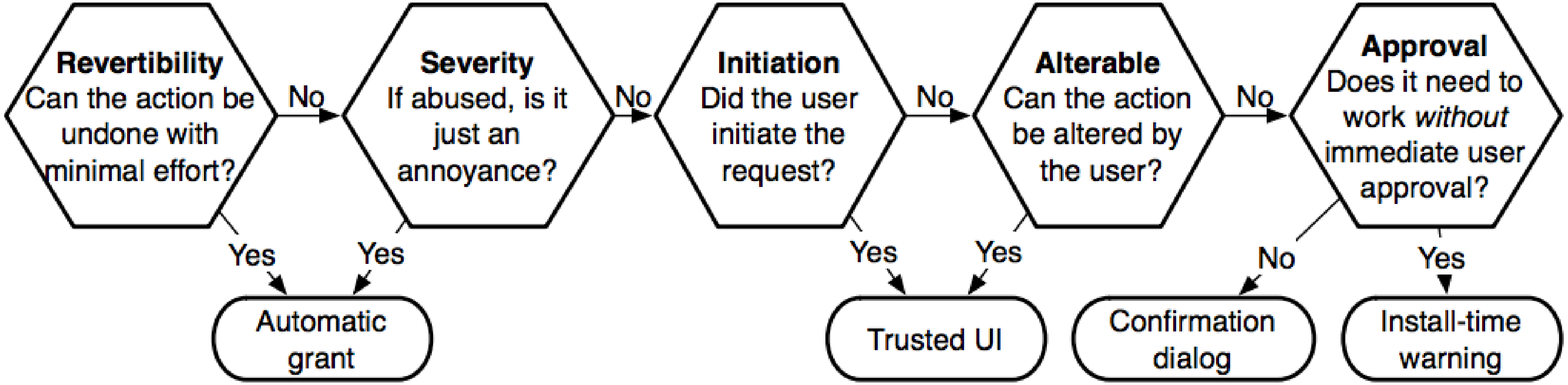
- Users are hopelessly lazy
- Security tasks should be more usable
- It is rational to ignore security warnings from economic perspectives

Economic Perspectives

- So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users
  - Password Rules
  - Phishing URL Education
  - Certificate Errors
- Poor cost-benefit trade-offs
- Worst case harm ≠actual harm

When to warn users?

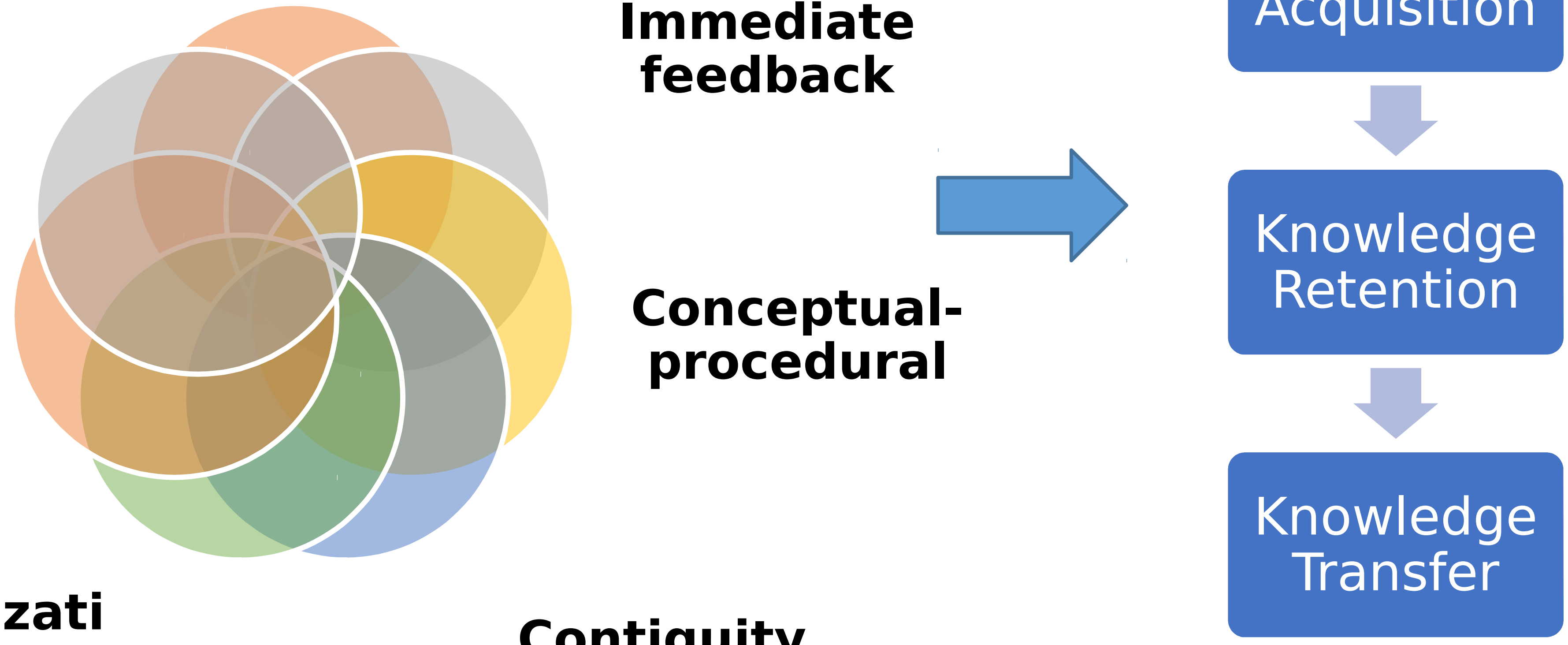
- Users’ effort is not free
- When to warn users?


Revertibility
Can the action be undone with minimal effort?
No
Severity
If abused, is it just an annoyance?
No
Initiation
Did the user initiate the request?
No
Alterable
Can the action be altered by the user?
No
Approval
Does it need to work *without* immediate user approval?
Yes
Yes
Yes
Yes
No
Yes
Automatic grant
Trusted UI
Confirmation dialog
Install-time warning

- Surveyed 3115 smart phone users
- 55% automatic grant, 23% trusted UI, **16%** confirmation dialog, **6%** install-time warnings.

Picture From How to Ask For Permission

How to help users learn effectively?



Learning-by-doing

Reflection

Immediate feedback

Story-based agent environment

Conceptual-procedural

Personalization

Contiguity

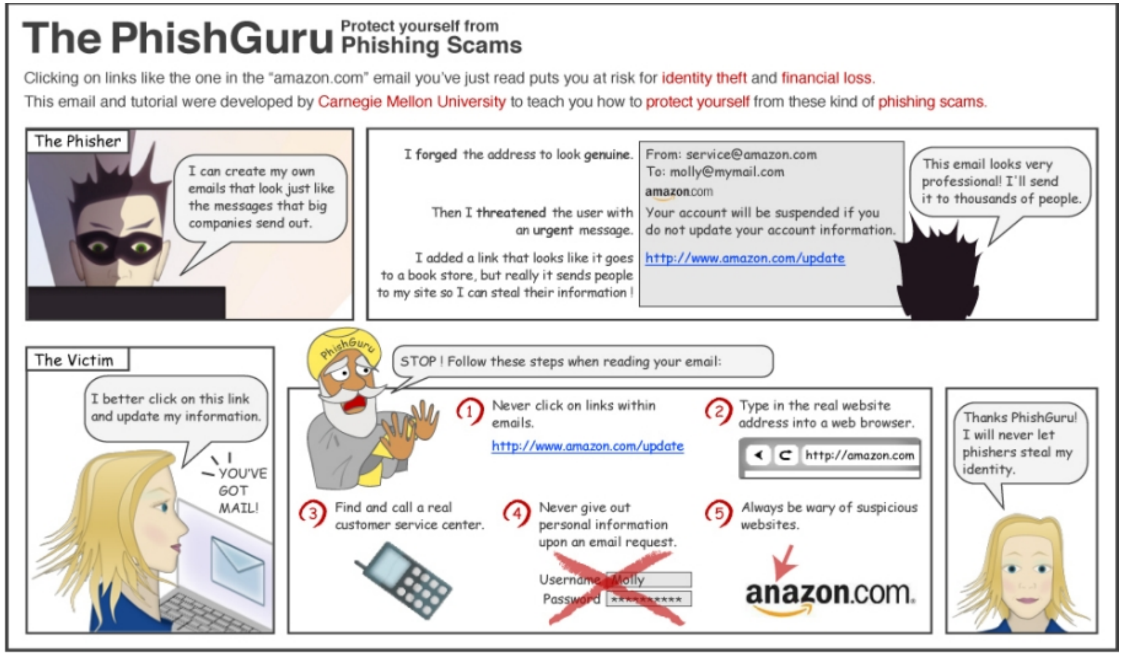
Knowledge Acquisition

Knowledge Retention

Knowledge Transfer

Effective Learning Tools

- Phish Guru



The PhishGuru Protect yourself from Phishing Scams

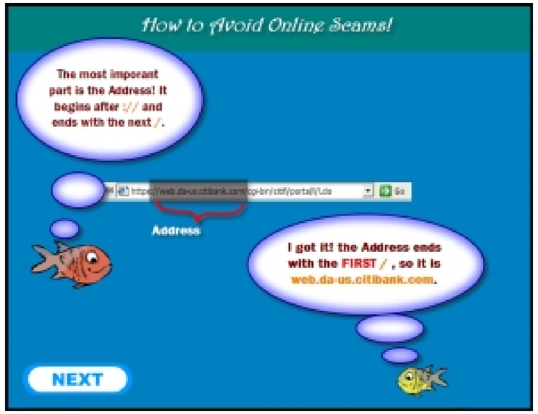
Clicking on links like the one in the "amazon.com" email you've just read puts you at risk for identity theft and financial loss.
This email and tutorial were developed by Carnegie Mellon University to teach you how to protect yourself from these kind of phishing scams.

The Phisher
I can create my own emails that look just like the messages that big companies send out.
I forged the address to look genuine.
Then I threatened the user with an urgent message.
I added a link that looks like it goes to a book store, but really it sends people to my site so I can steal their information !
From: service@amazon.com
To: molly@mymail.com
amazon.com
Your account will be suspended if you do not update your account information.
http://www.amazon.com/update
This email looks very professional! I'll send it to thousands of people.
The Victim
I better click on this link and update my information.
YOU'VE GOT MAIL!
PhishGuru
STOP ! Follow these steps when reading your email:

1. Never click on links within emails. http://www.amazon.com/update
2. Type in the real website address into a web browser. http://amazon.com
3. Find and call a real customer service center.
4. Never give out personal information upon an email request. Username Molly Password **********
5. Always be wary of suspicious websites. anazon.com

Thanks PhishGuru! I will never let phishers steal my identity.

- Anti-Phish Phil



How to Avoid Online Scams!

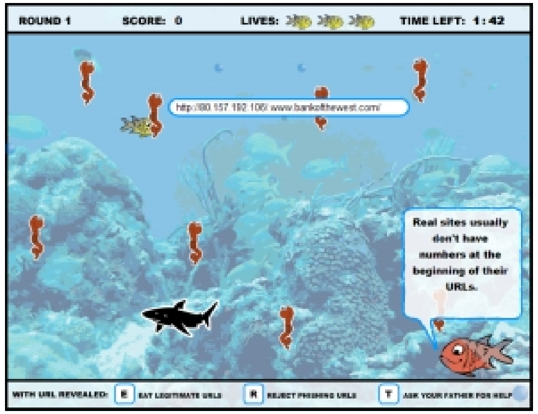
The most imporant part is the Address! It begins after :// and ends with the next /.

https://web.da-us.citibank.com/cgi-bin/citif/portal/l/.do

Address

I got it! the Address ends with the FIRST / , so it is web.da-us.citibank.com.

NEXT

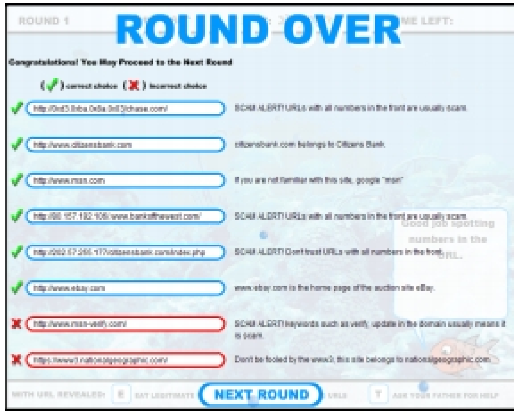


ROUND 1 SCORE: 0 LIVES: TIME LEFT: 1:42

http://80.157.192.106/ www.bankofthewest.com/

Real sites usually don't have numbers at the beginning of their URLs.

WITH URL REVEALED: E EAT LEGITIMATE URLS R REJECT PHISHING URLS T ASK YOUR FATHER FOR HELP



ROUND OVER

Congratulations! You May Proceed to the Next Round

(✓) correct choice (✗) incorrect choice

✓	http://0xd3.0xba.0x9a.0x83/chase.com/	SCAM ALERT! URLs with all numbers in the front are usually scam.
✓	http://www.citizensbank.com	citizensbank.com belongs to Citizens Bank.
✓	http://www.msn.com	If you are not familiar with this site, google "msn"
✓	http://80.157.192.106/www.bankofthewest.com/	SCAM ALERT! URLs with all numbers in the front are usually scam.
✓	http://202.67.255.177/citizensbank.com/index.php	SCAM ALERT! Don't trust URLs with all numbers in the front.
✓	http://www.ebay.com	www.ebay.com is the home page of the auction site eBay.
✗	http://www.msn-verify.com/	SCAM ALERT! keywords such as verify, update in the domain usually means it is scam.
✗	https://www3.nationalgeographic.com/	Don't be fooled by the www3, this site belongs to nationalgeographic.com.

Good job spotting numbers in the URL.

NEXT ROUND

Mental Models

- Medical
- Warfare
- Market
- Crime
- Physical

Exercise

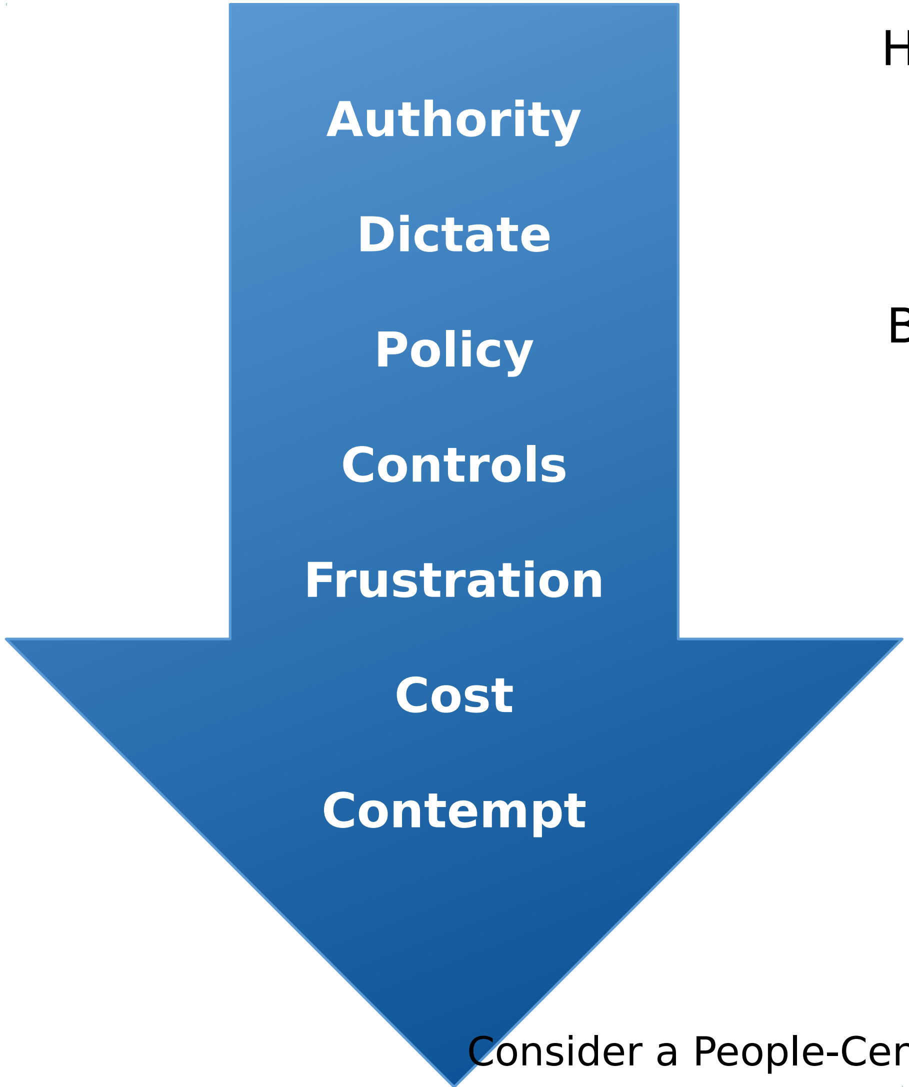
- Imagine you are the CEO of a company, how much time should invest in security training?
- what should it focus on?
- How do you make your training sessions interesting and effective?

A Vision: People Centric Security

- Hype or Trend?
- Gartner’s recent research

Traditional Security Approach

Status Quo



Authority

Dictate

Policy

Controls

Frustration

Cost

Contempt

Hierarchy

Bureaucracy

Enforcement

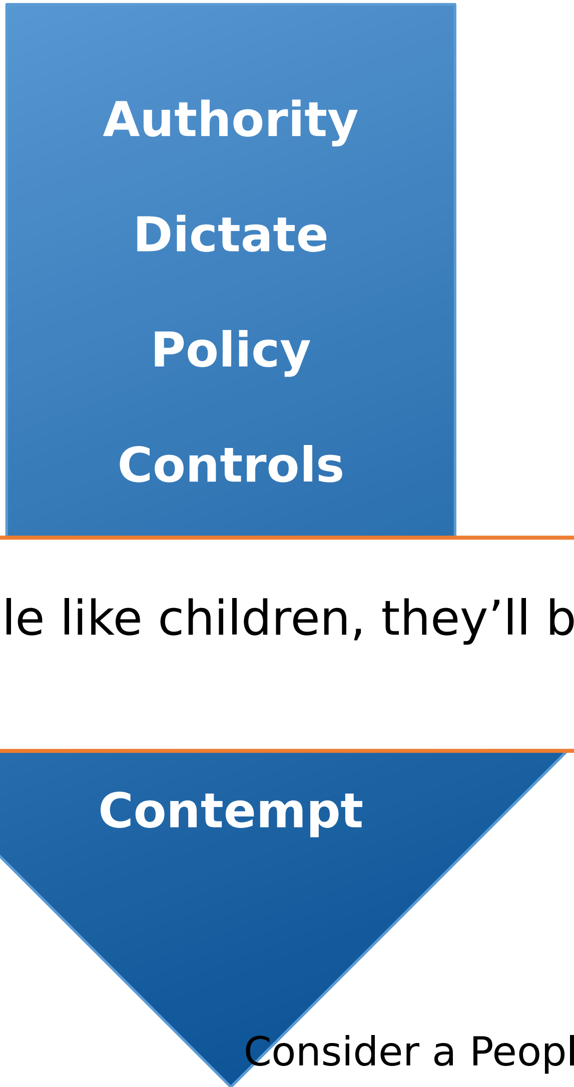
Consider a People-Centric Security Strategy Tom Scholtz (G0024935

Traditional Security Approach

Hierarchy

Status Quo

Bureaucracy



Authority

Dictate

Policy

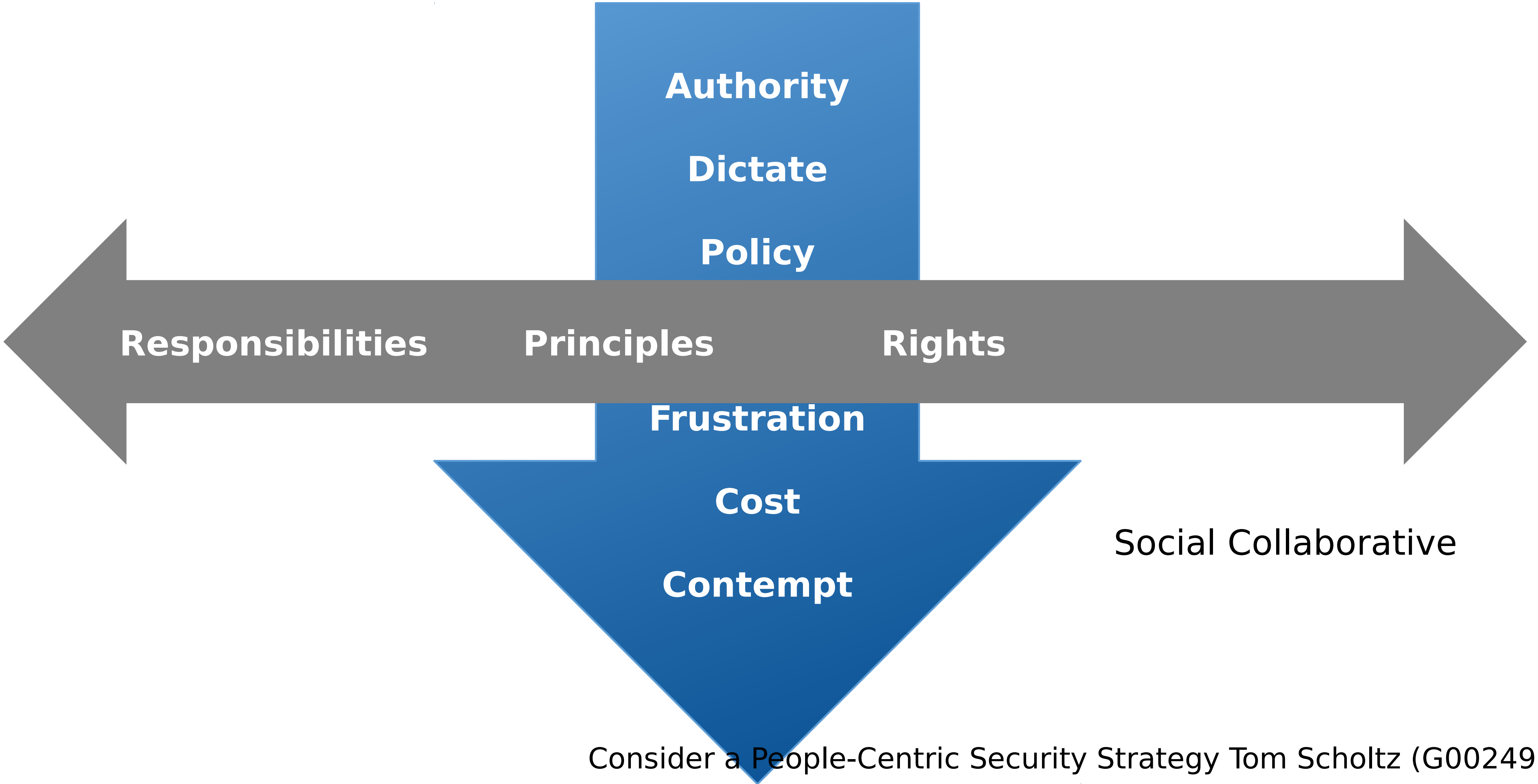
Controls

Contempt

> “ If you treat people like children, they’ll behave like children.”
> --Peter Cochrane

Consider a People-Centric Security Strategy Tom Scholtz (G0024935

People Centric Security



Authority

Dictate

Policy

Responsibilities

Principles

Rights

Frustration

Cost

Contempt

Social Collaborative

Consider a People-Centric Security Strategy Tom Scholtz (G00249357)

The Nexus of Forces Drives the Change

Mobile

Social

Cloud
&Virtualization

Consider a People-Centric Security Strategy Tom Scholtz (G00249357)

What if we reduce security controls?

- Less bureaucracy
- Cost reduction
- Improved staff morale
- A truly agile IT environment that offers feasibility

- Better security
  - Less “underground activity”
  - Focus on monitoring the reactive processes

Consider a People-Centric Security Strategy Tom Scholtz (G00249357)

Less Controls, Fewer Accidents

- Hans Monderman Experiment "Shared Space" Concept:
  - Removes curbs, lines, signs, and signals
  - Forces personal responsibility for road safety
  - Has shown positive results in the Netherlands, Sweden, the U.K., and the U.S.

From Control Centric to People Centric Security

- Conventional Security
- People Centric Security

Policies and control based	Principles, rights, and responsibilities-based
Suspicion based	Trust based
Preventative	Corrective
Impedes the good people in order to control the bad people	Controls the bad people; liberates the good people
Based on the behaviors of bad guys	Based on the behavior of the good guys
Standard oriented	Service-oriented
IT and security makes risk decisions	Owners and users make risk decisions
Impedes progress	Enables progress
Bureaucratic	Democratic
Dr. No	Business enabler

Maximize human potential by increasing trust and independent decision-making

Consider a People-Centric Security Strategy Tom Scholtz (G00249357)

Discussion

- Challenges?

- Any thoughts?

Citations

- Fanny Lalonde Lévesque, Jude Nsiempba, José M. Fernandez, Sonia Chiasson, Anil Somayaji. A Clinical Study of Risk Factors Related to Malware Infections. In Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security, 2013. (CCS '13)

- Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. Teaching Johnny Not to Fall for Phish. In ACM Transactions on Internet Technology (TOIT), Volume 10, Issue 2, May 2010.

- Adrienne Porter Felt, Serge Egelman, Matthew Finifter, Devdatta Akhawe, David Wagner. How to Ask For Permission. In Proceedings of the 7th USENIX conference on Hot Topics in Security, 2012. (HotSec '12)

- L. Jean Camp. Mental Models of Privacy and Security. In IEEE Technology and Society magazine, Volume 28, Number 3, pp. 37--46, 2009.

- Cormac Herley. So Long, and No Thanks for the Externalities: the Rational Rejection of Security Advice by Users. In Proceedings of the 2009 New Security Paradigms Workshop, 2009. (NSPW '09)

- Consider a People-Centric Security Strategy Tom Scholtz (G00249357)
  - http://my.gartner.com/portal/server.pt?open=512&objID=202&mode=2&PageID=5553&ref=webinar-rss&resId=2546716&srcId=1-2920760825