

Blunting the phisher's spear: A risk-based approach for defining user training and awarding administrative privileges

Arun Vishwanath, Ph.D., MBA

Associate Professor

<http://arunvishwanath.us>



**I study how hackers, cyber terrorists,
hactivists enter networks...**

I study...

- ➊ I study how hackers, cyber terrorists, hactivists enter and compromise networks
- ➋ The proverbial “people problem” of cyber security

Unintentional Insiders

Brute Force
Hacking



DEFENDED

UNINTENTIONAL INSIDER

PERCEPTIONS

HABITS

PERSONALITY

COGNITIVE
PROCESSING

PSYCHOGRAPHICS

EMPLOYEE

Organizational
Email Provider



Spear phishing

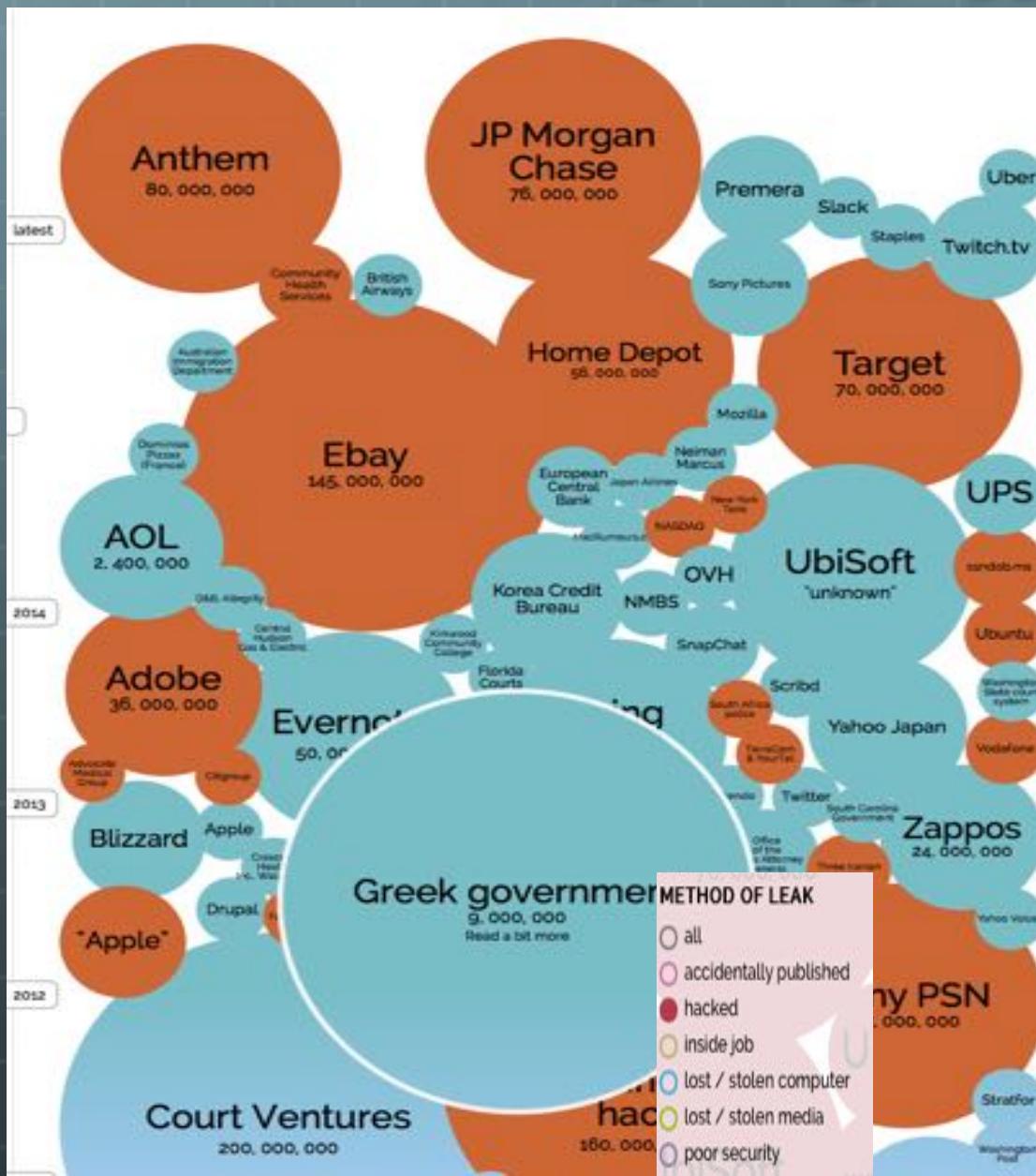


External
Email Provider

UNSECURED INTERACTION

VULNERABLE

Data breaches keep getting bigger...



Source: <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

Spear phishing is the attack vector of choice

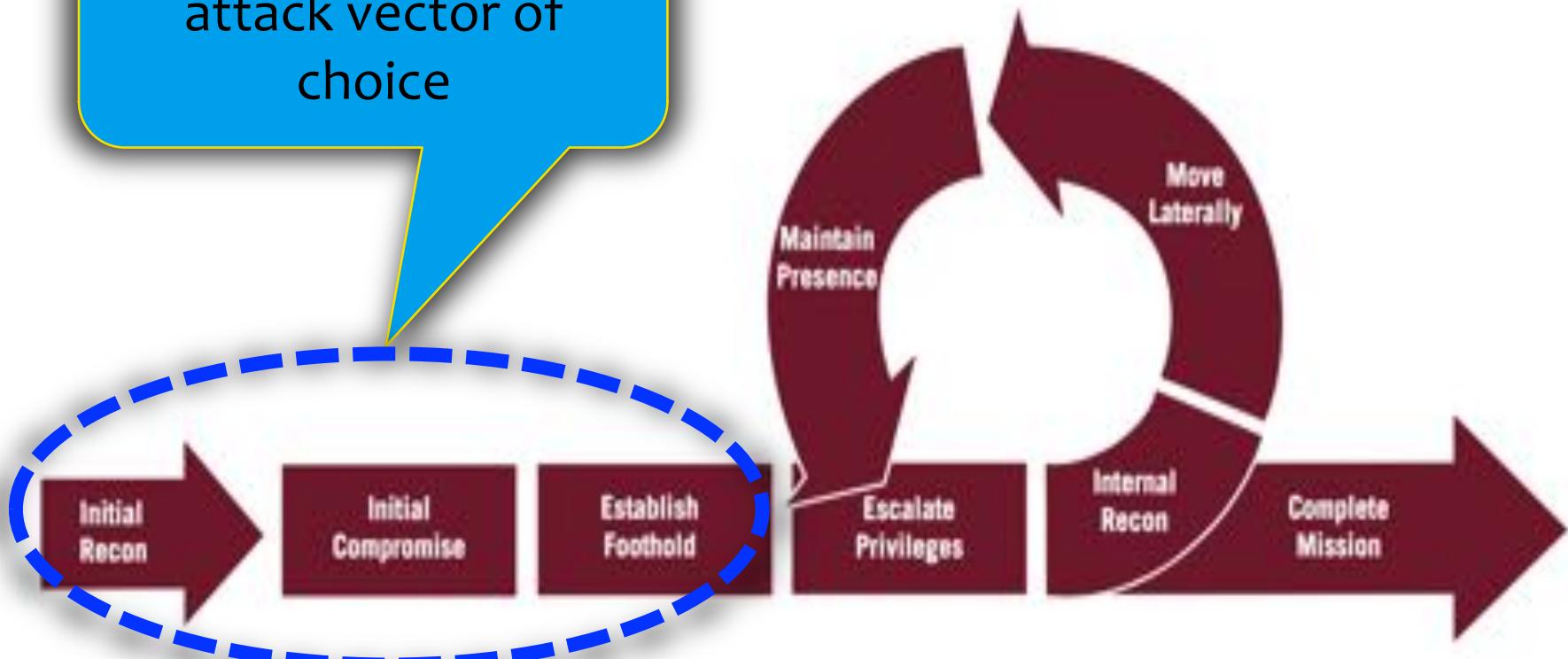
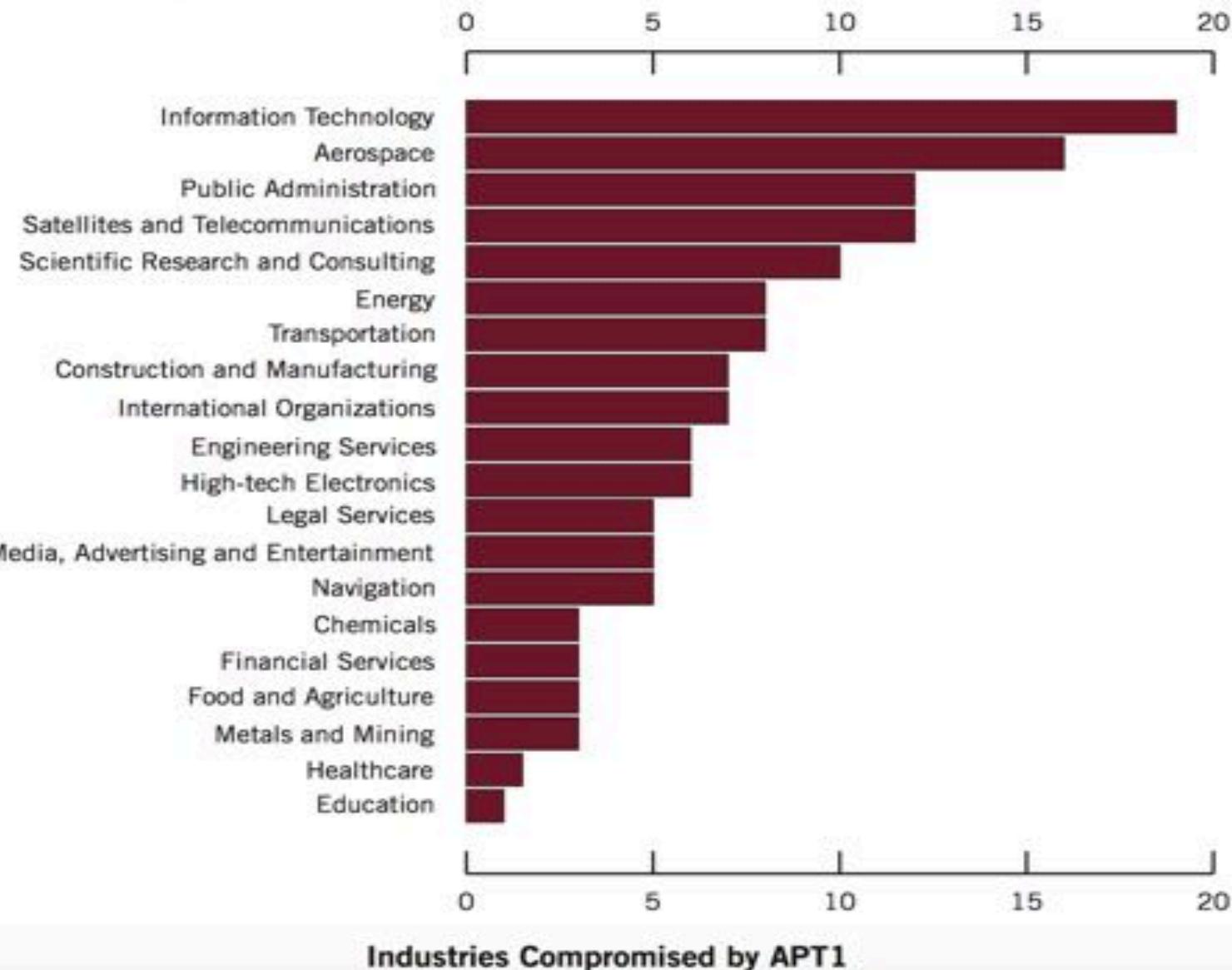
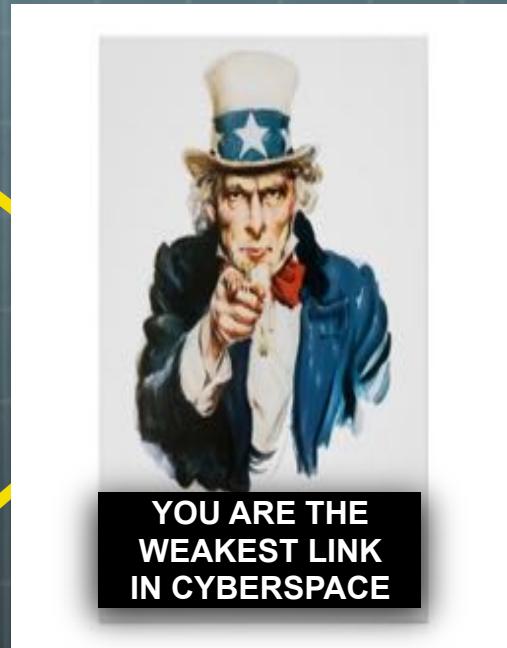


FIGURE 14: Mandiant's Attack Lifecycle Model

Impacted every industry



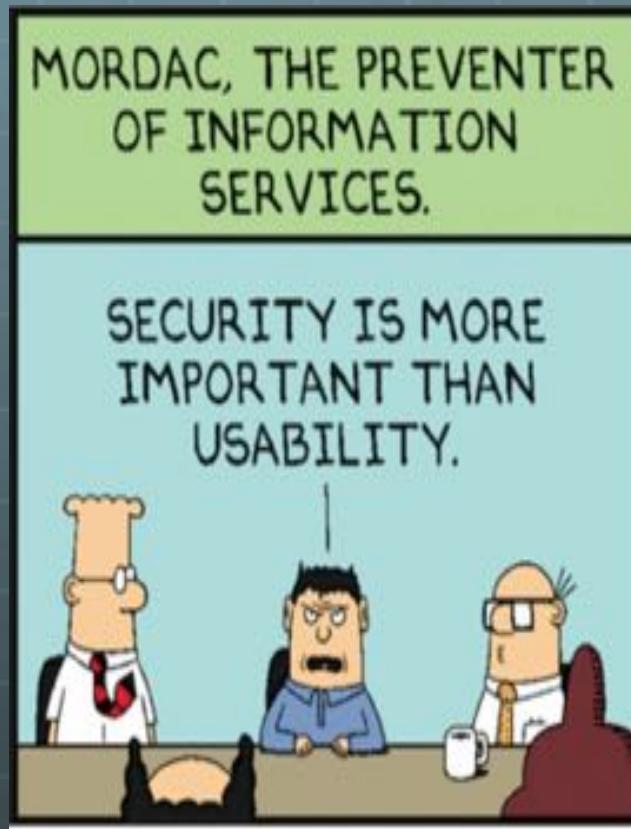
Perpetrated by State and Non-state Sponsors



Approaches to dealing with the “people problem”

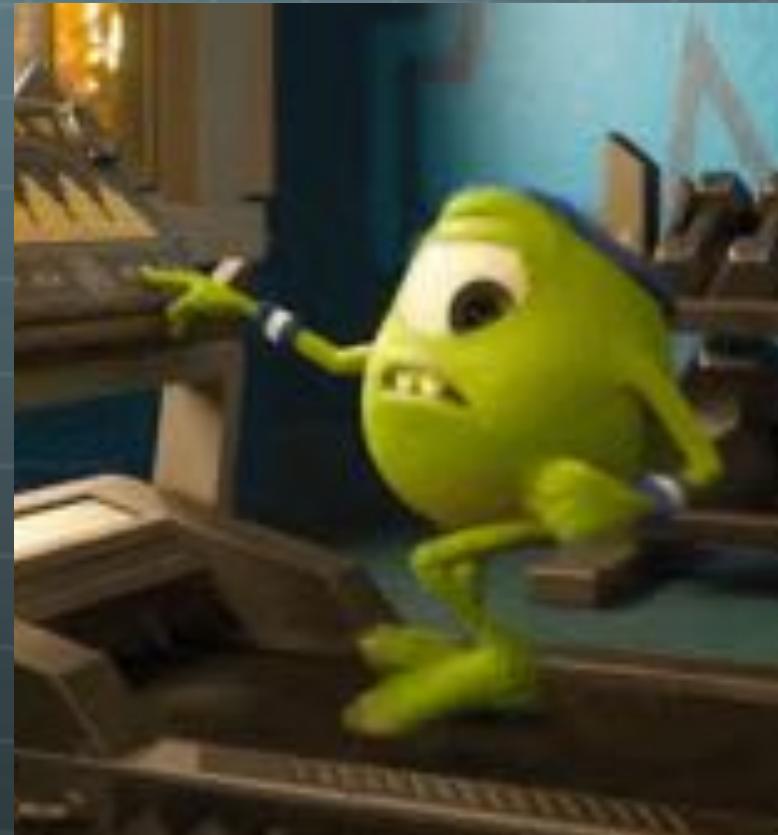
-  Firewalls, antivirus; Whitelisting approaches
-  EMET; Constrain access/admin privileges

How realistic is this...



Human factors approach: Cyber security training

1. “Phish” people simulations
2. Show them why they fell for it
3. Keep telling them to shape-up
4. Admiral Mike Rogers: “We should court-martial them!”



The PEOPLE PROBLEM

- The Problem is NOT the People
- It is in our UNDERSTANDING of PEOPLE
- We Have developed a human factors model that explains how people think, act, behave online, and why.

Suspicion, Cognition, Automaticity Model (SCAM)

(Vishwanath, Harrison, & Ng, 2016)

**SCAM explains how users
think:**



Scrooge: I
am a
cognitive
miser

I use cognitive
shortcuts a.k.a
Heuristics

Heuristics



The Starbucks logo, featuring the green mermaid Siren with three stars above her head, set against a circular background of green and white.

Free WiFi

From our friends at Google

Accept & Connect

I agree to the [Terms of Service](#) and have reviewed the [Google Privacy Policy](#)

Need help? [855-446-2374](#)



The Starbucks logo, featuring the green mermaid Siren with three stars above her head, set against a circular background of green and white.

Free WiFi

From our friends at Google

One account. All of Google.

**Sign in with your
Google Account**

Username: ex. pat@example.com

Password:

Stay signed in

Accept & Connect

[Can't access your account?](#)

I agree to the [Terms of Service](#) and have reviewed the [Google Privacy Policy](#)

Need help? [855-446-2374](#)

Gmail



Cyber Attack Against Anthem

Dear Anthem Client,

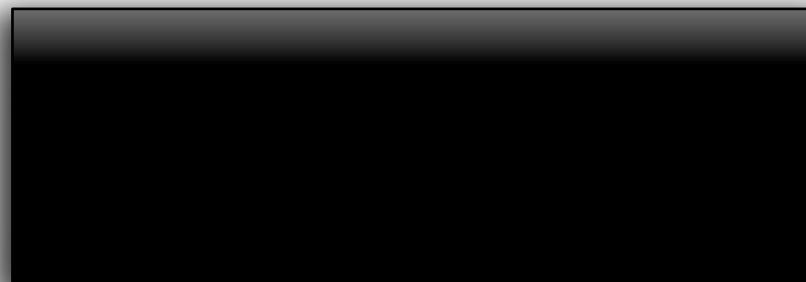
We wanted to make you aware of a data breach that may have affected your personal health information and credit card data. The data which was accessed may impact clients who made credit or debit card payments for healthcare or who got treatment during the year 2014.

Your trust is a top priority for Anthem, and we deeply regret the inconvenience this may cause. The privacy and protection of our client's health care information is a matter we take very seriously and we are working diligently to resolve the incident.

To subscribe to a free year of credit card account protection please click on the link below and follow the instructions that will be required:

[Click Here To Get Your Free Year Of Credit Card Protection](#)

Anthem



November 4, 2015

Dear [REDACTED]

As you may have heard in media reports, Excellus BlueCross BlueShield (Excellus) publicly disclosed that it was the victim of a cyber attack. Excellus notified Anthem about this incident on September 9, 2015, the same day Excellus notified the media. You are receiving the attached letter from Excellus because Excellus has determined that your information may have been impacted by the cyber attack.

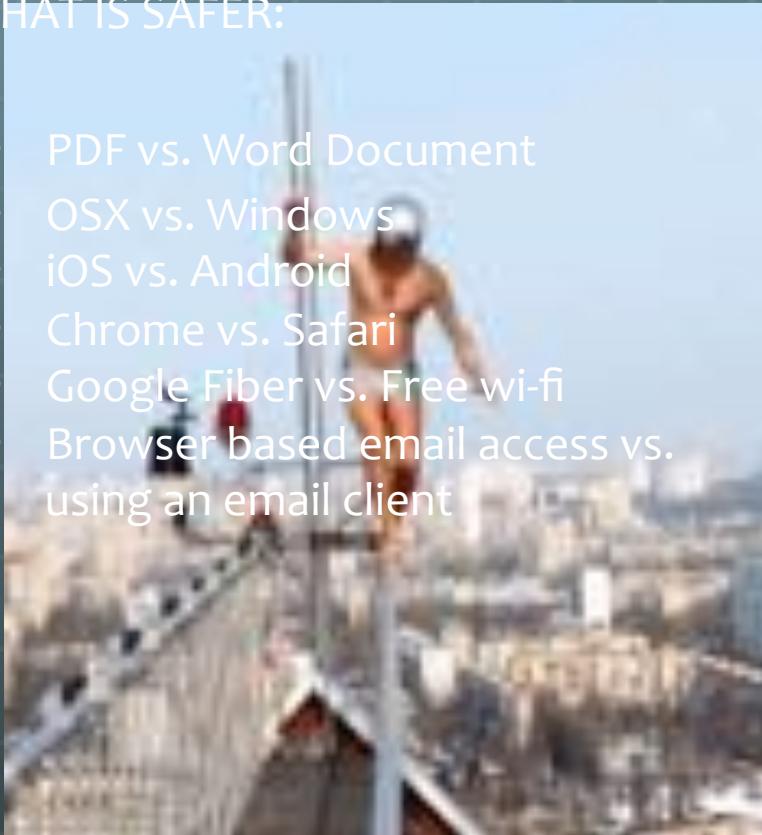
We would like to help explain Anthem's relationship with Excellus and why your data may have been in Excellus's systems. First, Anthem is neither owned nor operated by Excellus. Excellus is a separate company with which Anthem works to administer certain programs.

**SCAM explains what users
believe:**

Cyber Risk Beliefs

WHAT IS SAFER:

- PDF vs. Word Document
- OSX vs. Windows
- iOS vs. Android
- Chrome vs. Safari
- Google Fiber vs. Free wi-fi
- Browser based email access vs. using an email client



**SCAM explains the role of
habits and devices**

Habits

- ➊ Ritualistically checking email
- ➋ Texting while talking, walking, driving
- ➌ Entering login, password, authentication credentials



Smartphones, smart watches... not so smart people

- Thanks Apple and Google!

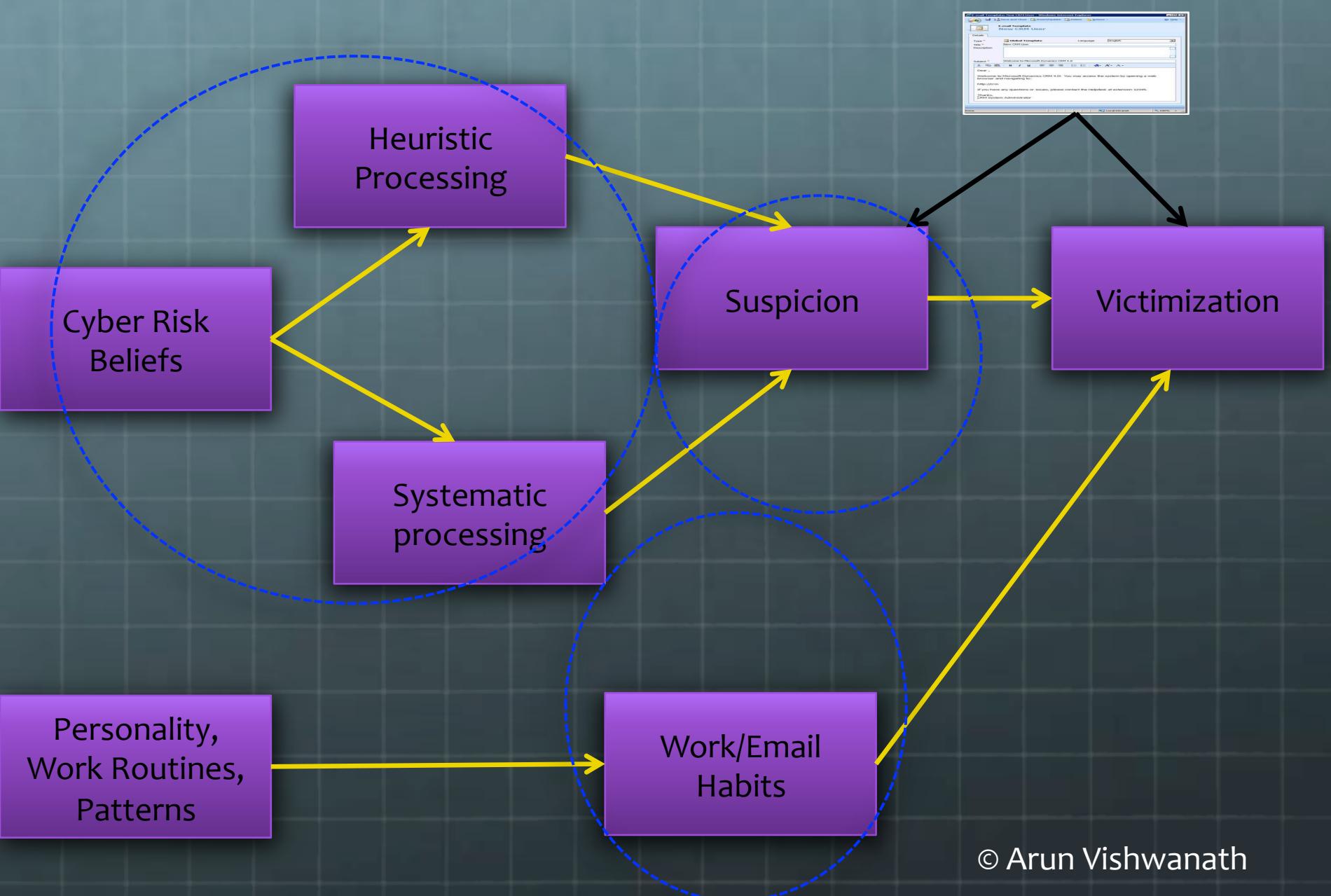


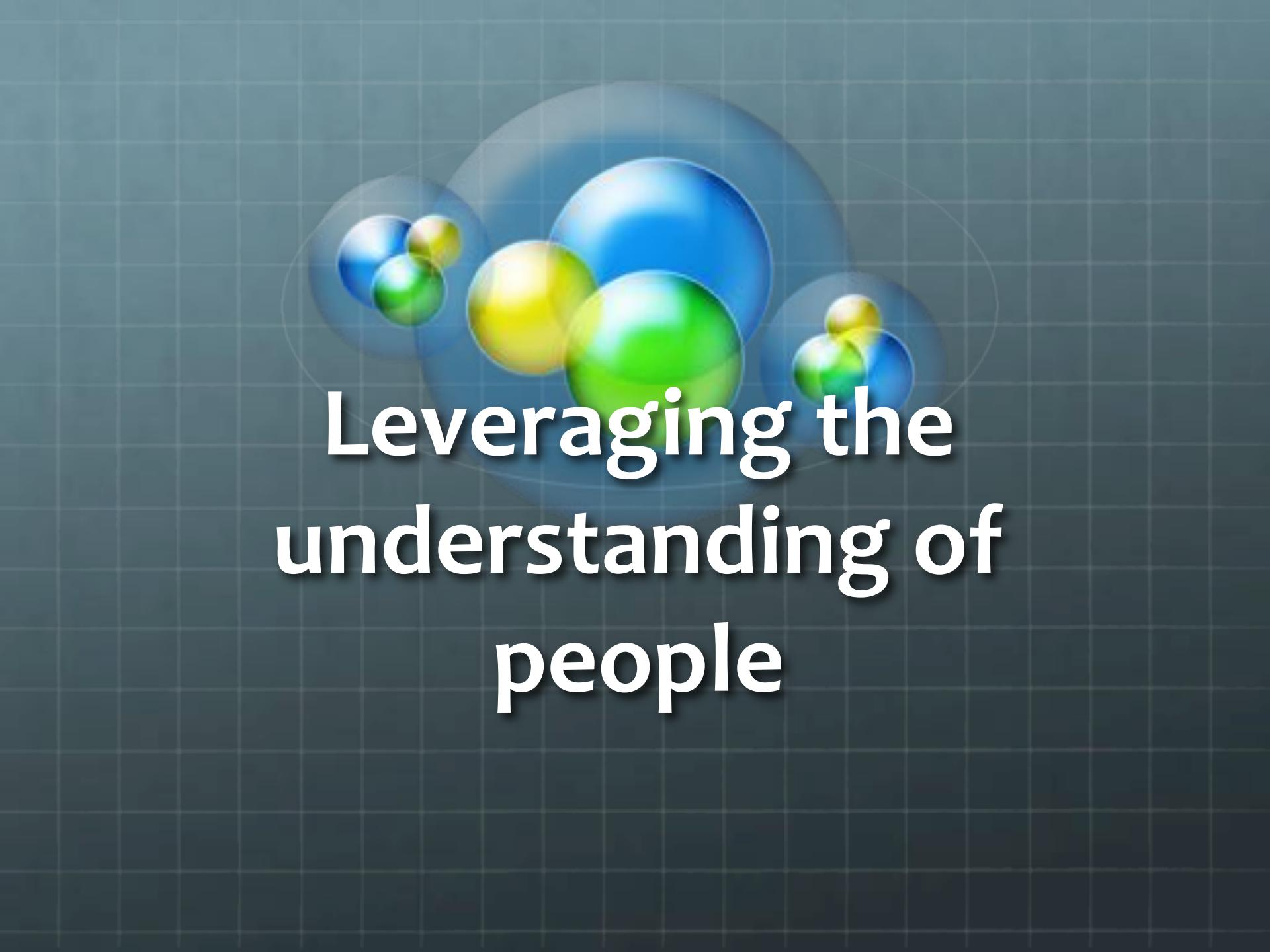
A woman in a grey business suit is crouching on a city sidewalk, interacting with several small ducklings. A white duck is standing nearby, and a small container holding pens or pencils is on the ground next to her. The background shows a glass door and some people walking by.

Beware of

Cute Duckling Scam

Suspicion, Cognition, Automaticity Model (SCAM) (Vishwanath, Harrison, & Ng, 2014)



The background features a light blue grid pattern. Overlaid on this are several semi-transparent, rounded shapes: a large central sphere with a gradient from blue at the top to green at the bottom, surrounded by smaller spheres in shades of blue, green, and yellow. There are also faint, larger circular outlines.

Leveraging the understanding of people

Develop a Cyber Risk Index (CRI)

- An empirical data driven approach
- Uses a short, 40 question self-report survey
- Can be done within existing “red-team” simulations
- Like credit rating, it can we aggregated across division, organizations, sectors

Deciding who gets trained and how:



Deciding who gets access:

- Current system of providing access is based on organizational role and status
- Use CRI to identify individual risk levels and changes in risk behavior overtime
- This becomes a quantitative score of INDIVIDUAL CYBER HYGIENE

References to published research and writings:

Selected Academic Research

- Vishwanath, A., Harrison, B., & Ng, Y.J. (2016). Suspicion, Cognition, Automaticity Model (SCAM) of Phishing Susceptibility. *Communication Research*.
- Vishwanath, A. 2016). Mobile Device Affordance: Explicating How Smartphones Influence The Outcome Of Phishing Attacks. *Computers in Human Behavior*.
- Vishwanath, A. (2015). Habitual Facebook Use and its Impact on Getting Deceived on Social Media. *Journal of Computer-Mediated Communication*, 20(1), 83-98.

Selected pieces in CNN

- Why the cyberattacks keep coming:
<http://www.cnn.com/2015/06/08/opinions/vishwanath-stopping-hacking/>
- Why we need a cyber wall:
<http://www.cnn.com/2016/05/02/opinions/build-cyber-wall-vishwanath/index.html>
- When hackers turn your lights off:
<http://www.cnn.com/2016/02/11/opinions/cyber-infrastructure-attacks-vishwanath/>

Contact Information

- Arun Vishwanath, Ph.D., MBA
- Email: avishyoo1@gmail.com
- Web: <http://arunvishwanath.us>
- Mobile: 716.508.0192

