



Karen McDowell, Ph.D., University of Virginia
Commonwealth of Virginia IT Security Conference
April 3, 2014

Social Networking: Information Security Paradox



Virtual Goldmine

- Hacker's Dream
- Easy to identify prime victims within organizations, & send spear phish with malicious attachments



Spear Phishing

- Most prevalent and effective threat to information security
- Phishing, QRishing, Smishing, USBishing, and Vishing



Spear Phishing is Very Tricky

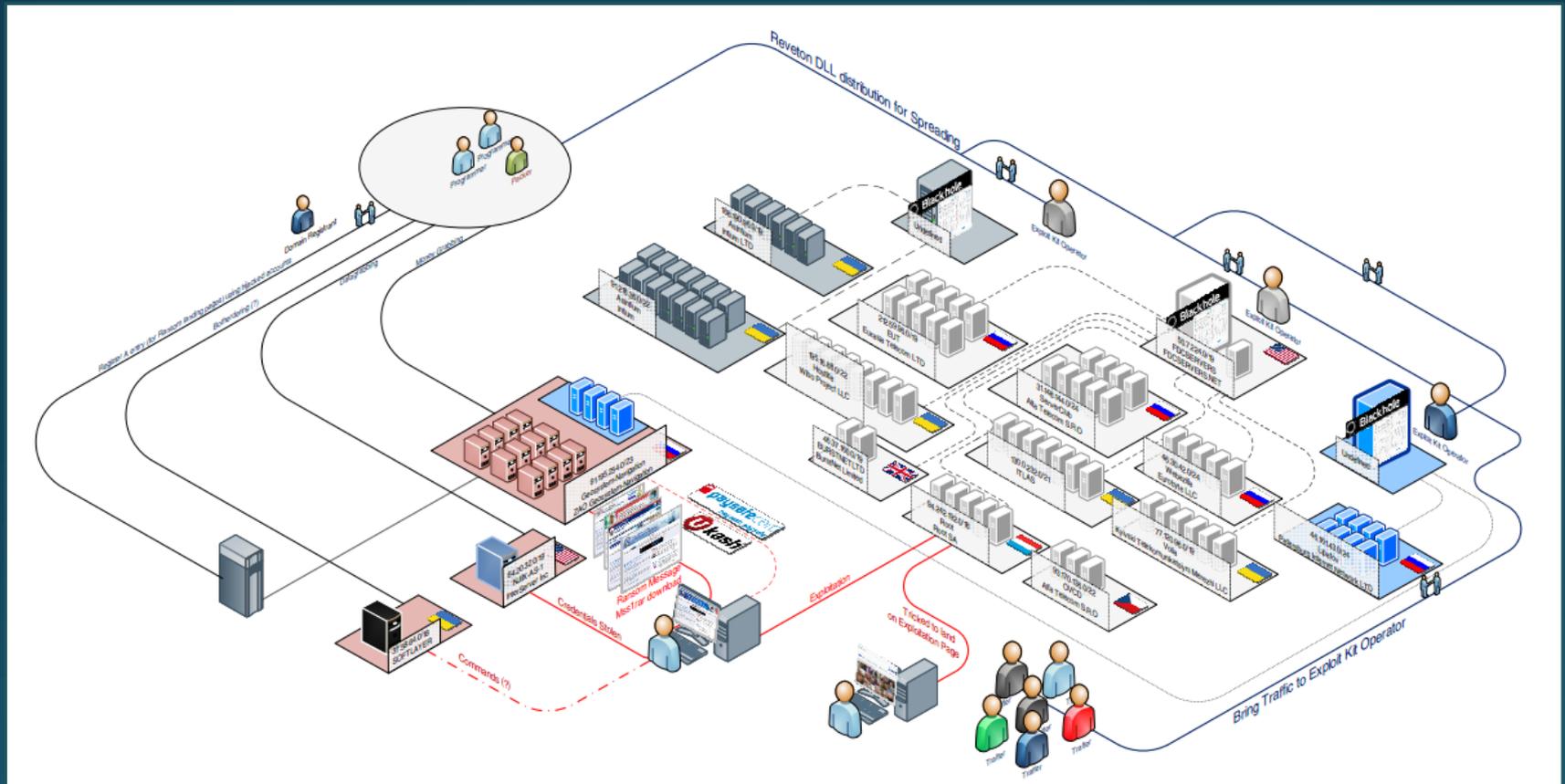
Employee Benefit and...

A screenshot of a document viewer showing a file named "employee benefit and overhead adjustment keys.pdf". The file icon is a red square with a white document symbol. The text is displayed in a light gray font on a white background.

employee benefit and overhead adjustment keys.pdf ... Application

2011 Recruitment Plan.xlsx

Hacking is an Industry Crime is a Service



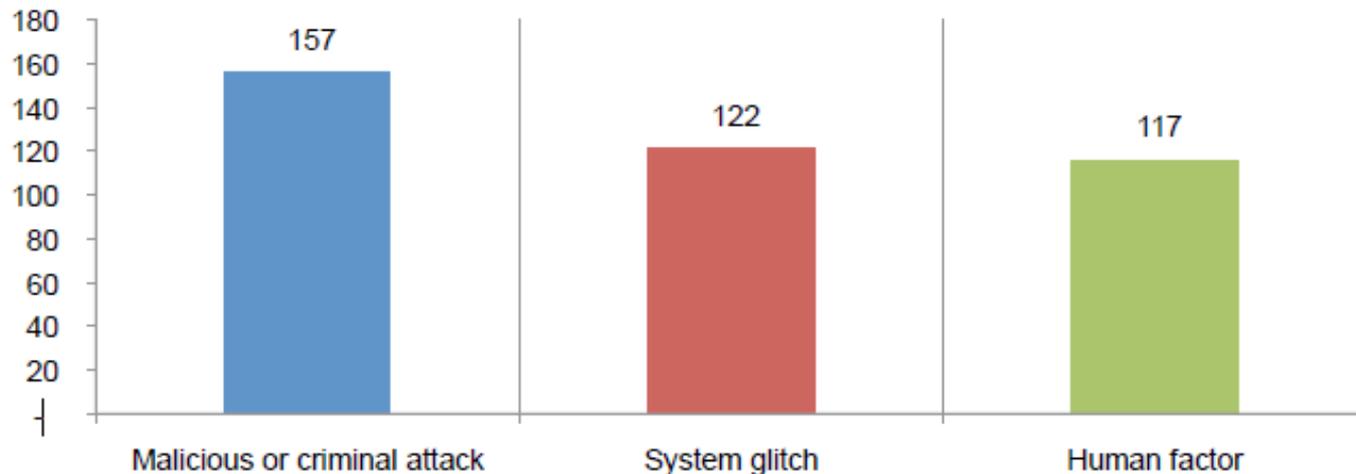
...an emerging trend with traditional organized crime syndicates and criminally minded technology professionals working together and pooling their resources and expertise...

\$650K per Cyberattack Incident

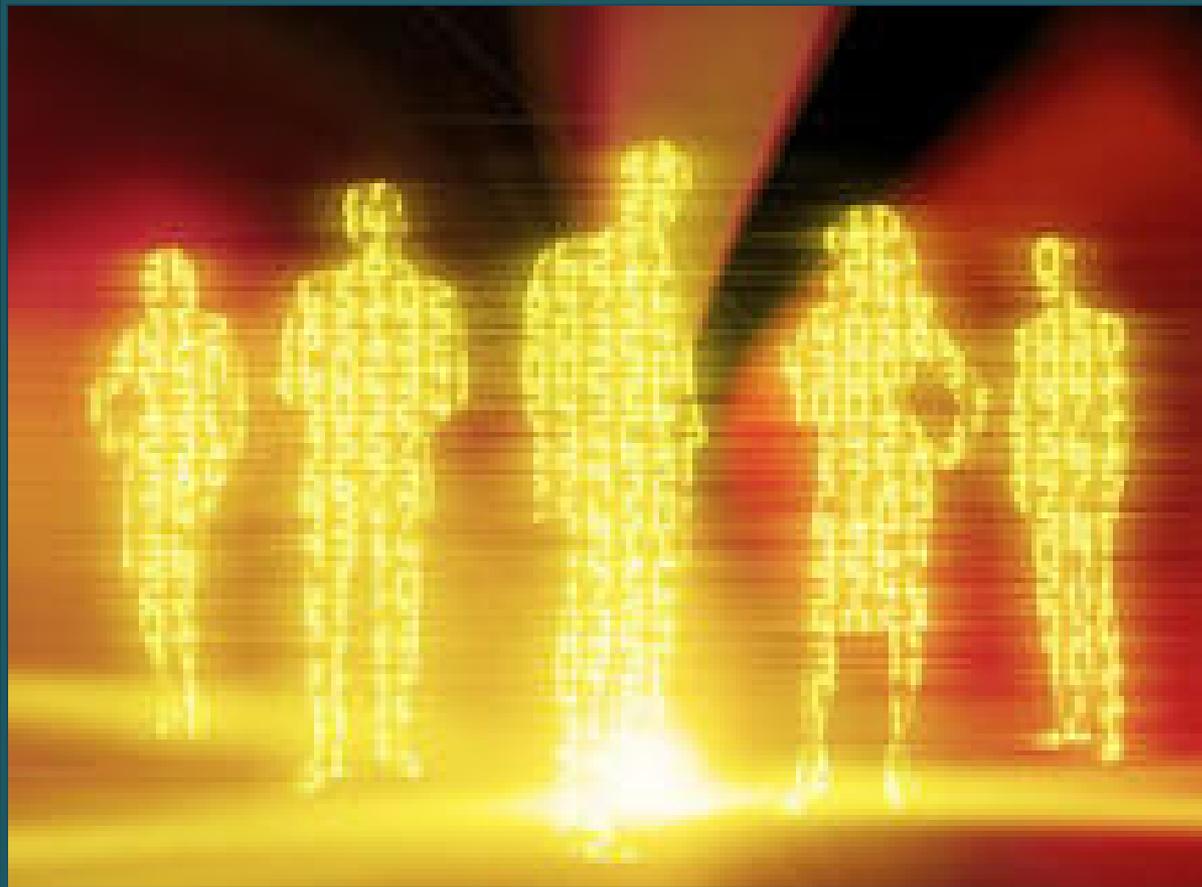
- If you think you haven't been hacked, it may be lurking on your network
- Eat, drink, and be merry, for tomorrow you will be hacked

Figure 7. Per capita cost for three root causes of the data breach

Consolidated view (n=277). Measured in US\$



The Human is the Weakest Link



Curiosity, Distraction, Ignorance

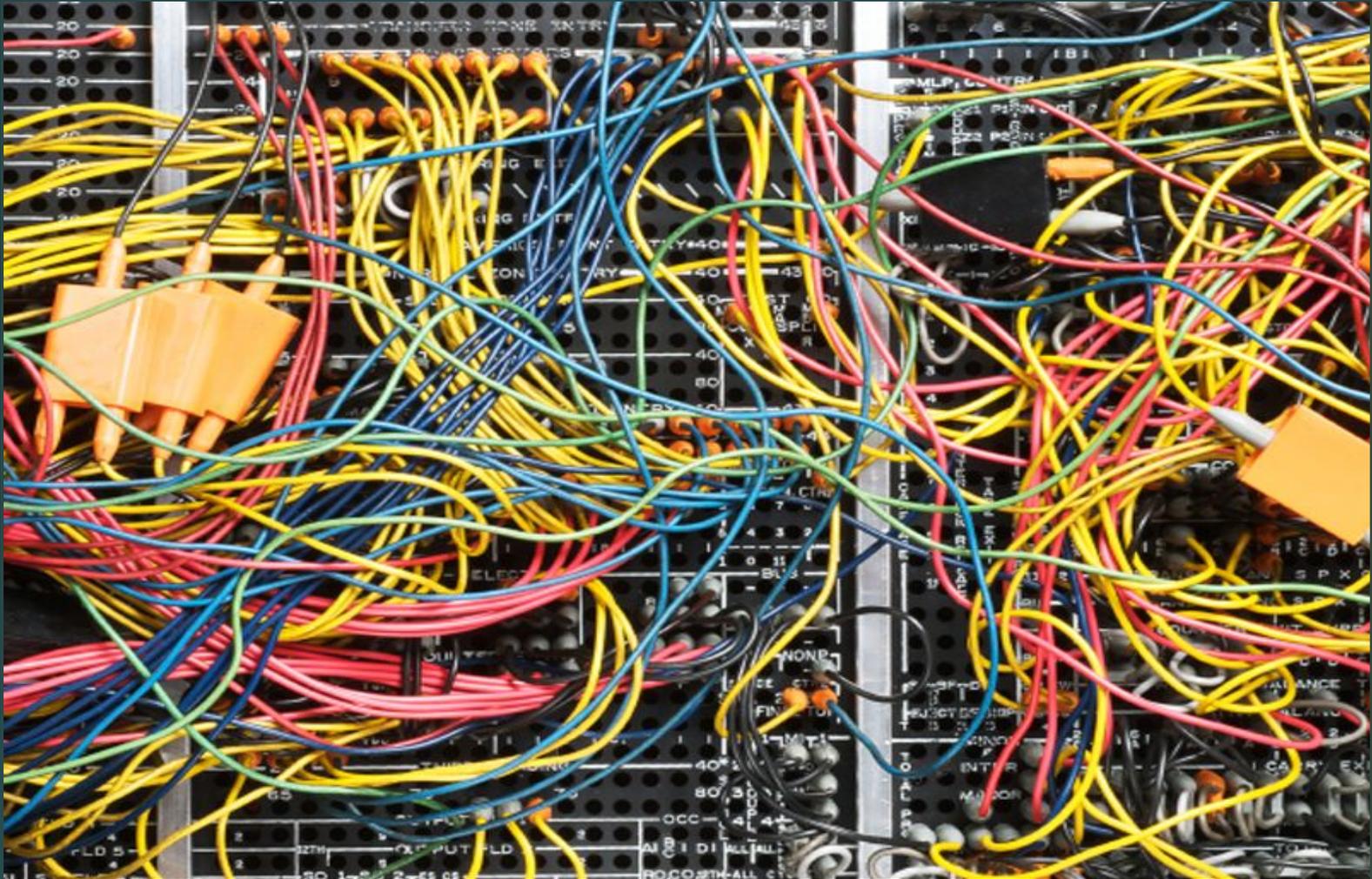
Other Variables



What's an Employer to Do?



Governance, Security, Compliance



Social Media “What Ifs”

- Employee tweets “something big is going to happen tomorrow”
- Manager sends message to employee’s Facebook -- hurtful and demeaning
- After work, employee posts in LinkedIn about a frustrating interaction with a client
- Manager notices employee is posting negative comments about her style

Policy: 1.75 – Use of Electronic Communications And Social Media

Effective Date: 8/1/01

Revision Date: 3/17/11

USE OF ELECTRONIC COMMUNICATIONS AND SOCIAL MEDIA

Application: All state employees, including employees of agencies exempt from coverage of the Virginia Personnel Act.

Social Media & Code of Virginia

- Policy: 1.75 – Use of Electronic Communications And Social Media
- Agencies are responsible for ensuring employees have access to, read, understand, and acknowledge this policy... and
- Communicate this policy...

“Incidental and Occasional Personal Use” of Social Media at work *is* permitted



Protect the Enterprise

- Consider both a no-employment disclosure and social media policy
- Teach, train all employees, especially IT personnel
- Limit access to certain social networks
- Teach employees to lock down settings
- Don't completely eliminate it.
 - Employees who want access will get it

Build Awareness, Teach





- “Tell me and I forget. Teach me and I remember. Involve me and I learn.”
- One of 20 Critical Security Controls:
“Security Skills Assessment and Appropriate Training to Fill Gaps: Security awareness training, security policies, and awareness testing”

Social Media Basic Protection

- Limit amount of personal information (PI) you share on any social media account
- Don't respond to email requests to do anything on social media.
- Instead, login to your account and see what's going on ...

General Best Practices

- Use strong, unique passwords & different ones for each account!
- Ensure you are actually logging into your social media account. Type in URL
- Log out when you leave.
- Keep your computer patched, up to date, and secured.

Hackers Exploit Our Trust



Worst Case Scenario?

Using the same password for different accounts has potentially devastating consequences

Hackers spear phish using stolen credentials, & so widen their net



Password Managers

- Stand-alone
 - 1Password (~\$50/yr)
 - Dashlane (free & premium 19.95/yr)
 - KeyPass (open source & free)
 - LastPass (free & premium ~\$12/yr)
 - PasswordSafe (open source & free)
- Built into the browser
 - I don't trust them, though they claim to encrypt passwords

facebook

Email or Phone

Password

Log In

Keep me logged in

[Forgot your password?](#)

- Biggest kid on the block
- If FB users constituted a country, it would be the world's third largest, behind China and India
- Powerful tool for businesses, yet FB takes note of every look or like

2005

Click the chart to advance, or click on a year

2005

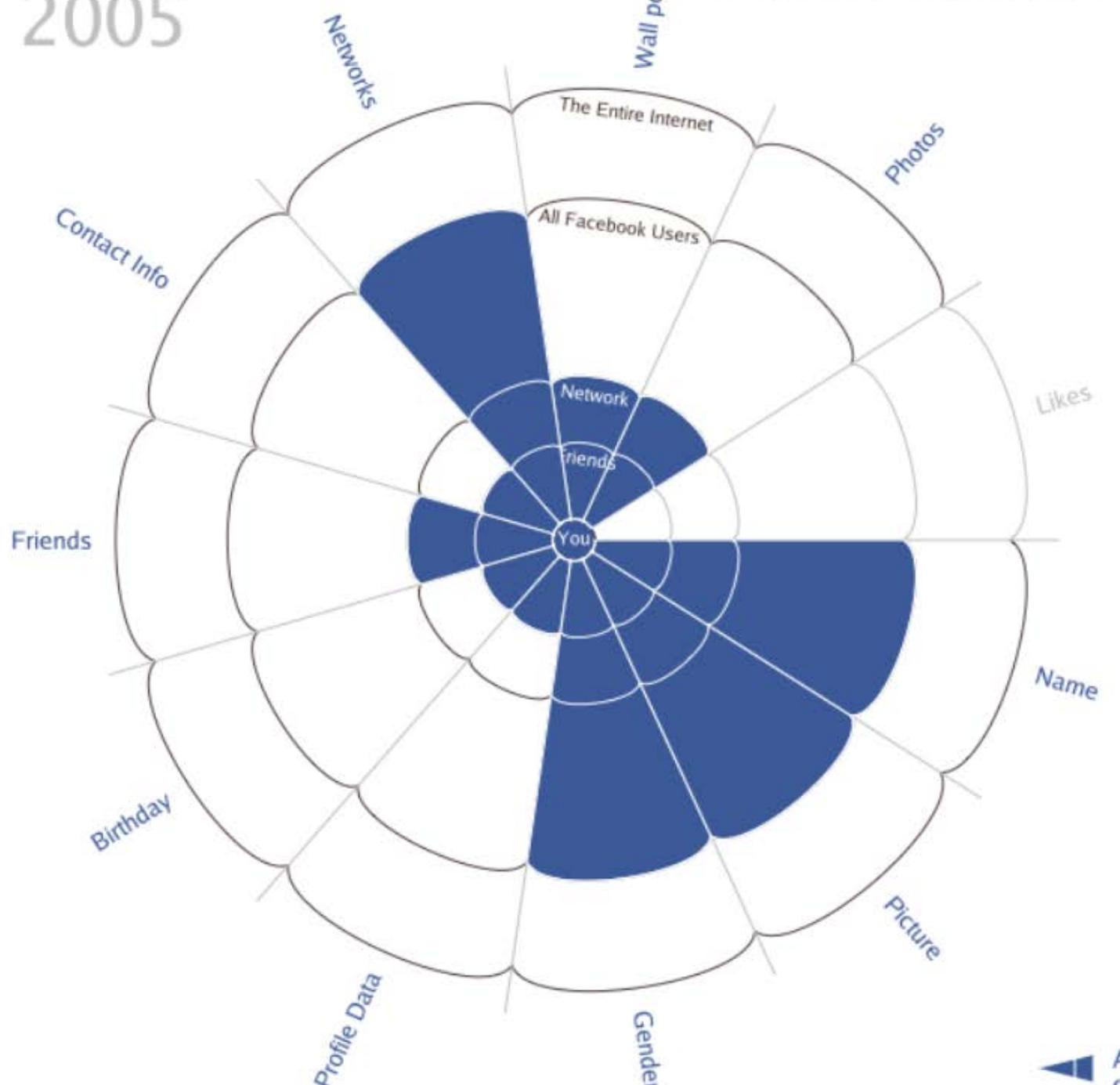
2006

2007

2009 (Nov)

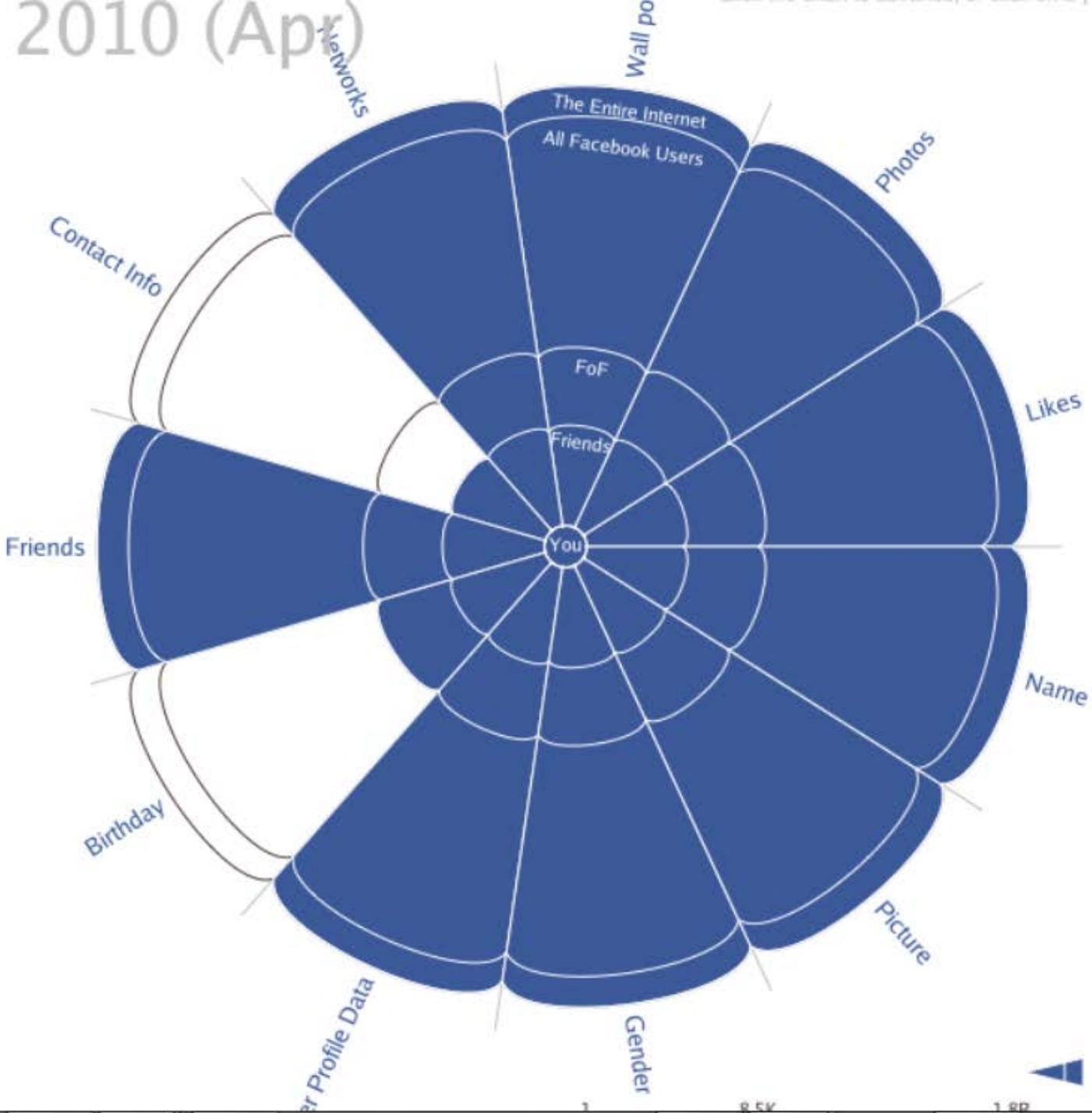
2009 (Dec)

2010 (Apr)



Availability of your personal data on Facebook (default settings)

2010 (Apr)



2006
2007
2009 (Nov)
2009 (Dec)
2010 (Apr)

Availability of your personal data on Facebook (default settings)

- Who can forget the LinkedIn hack of 2012? 6.5M user accounts/passwords.
- LinkedIn did not follow best practices with user info. May be losing momentum, “spammy”



Email address

Password [Forgot your password?](#)

Sign In

Aims to become “virtual town square”

Head hunters troll it. “Jobs you might be interested in” feature. VITA presence.

We list current employers, past employers, certifications and skill sets, making company & ourselves prime targets.

Google+ (httpS: enabled)

- Over 1 billion Google+ enabled accounts
- Reached 359 million, monthly active users 5/2013
- Growing at 33% per annum
- Security risk: Learn how to restrict profile visibility from “circles of connections”



Twitter: Special Vulnerability

- Short URL Services, usually free
 - Bit.ly
 - TinyURL.com
 - Goo.gl
 - Is.gd



Other Social Media Threats

- Dissemination of commercially sensitive information
- Spreading false information, like shouting “Fire” in a crowded cinema



The screenshot shows a Twitter post from The Associated Press (@AP). The profile name is "The Associated Press" with a verified account icon and a "Following" button. The tweet text reads: "Breaking: Two Explosions in the White House and Barack Obama is injured". Below the text are interaction options: Reply, Retweet, Favorite, and More. The tweet has 876 retweets and 32 favorites. A row of ten profile pictures of users who interacted with the tweet is visible. The timestamp is "1:07 PM - 23 Apr 13". The Twitter logo and handle "@AP" are in the bottom right corner.

AP The Associated Press  

@AP

Breaking: Two Explosions in the White House and Barack Obama is injured

 Reply  Retweet  Favorite  More

876 RETWEETS **32** FAVORITES

1:07 PM - 23 Apr 13

Twitter/@AP

Recon-ng

- <http://www.youtube.com/watch?v=R5xMe41i95E>
- Open source reconnaissance framework
- Not illegal
- Easy, automated way to recon any Twitter account

QRishing

- QR Codes
- Link Shorteners: bitly.com, tinyURL



A Cautionary Tale



Robin Sage

- 25-year old female
- Naval Network Warfare Command
- Cyber threat analyst
- Internship at the NSA
- Educated at MIT
- New Hampshire prep school
- Ten years work experience

Moral of the Robin Sage Story

- Just because it's on social media doesn't mean it's true.
- Limit the amount of personal information you post online.
- What goes on the Internet, stays on the Internet.
- Nobody loves you on the Internet.



Search ▾ find friends

Applications edit

 Photos

 Groups

 Events

 Marketplace

▾ more



[Edit My Profile](#)

▾ London Friends

6 friends in London. [See All](#)

Freddi Staur

Update your status...

Networks: London
Sex: Male
Interested In: Women
Relationship Status: Single
Birthday: June 4, 1980

▾ Mini-Feed

Displaying 10 stories. [See All](#)

Yesterday

-  Freddi and [\[Name\]](#) are now friends. [X](#)
-  Freddi and [\[Name\]](#) are now friends. [X](#)

August 7

-  Freddi and [\[Name\]](#) are now friends. [X](#)
-  Freddi and [\[Name\]](#) are now friends. [X](#)

Trust, but Verify!



Login to social media accounts *only* by typing in the URL yourself.

Anatomy of a Hack (APT)

- Step 1: Do Reconnaissance
- Step 2: Attract the Victim
- Step 3: Gain Control
- Step 4: Exfiltrate Data and conscript computers



Reconnaissance

1. Hacked accounts yield email addresses
2. What we post on social media & how we respond
3. Public websites, public addresses



Attract the Victim

Send spear phishing message!



The New York Times



Store

Mac

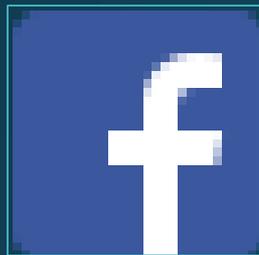
iPod

iPhone

iPad

iTunes

Support



REUTERS

EDITION: U.S.



Adobe



Microsoft

Google

THE WALL STREET JOURNAL.

epsilon

Office Productivity Tool?

- Social media technologies create a data overload.
- NASA-style mission control centers for social media are taking off, enabling companies to visualize instantly key metrics.
- Social media technologies replacing email?

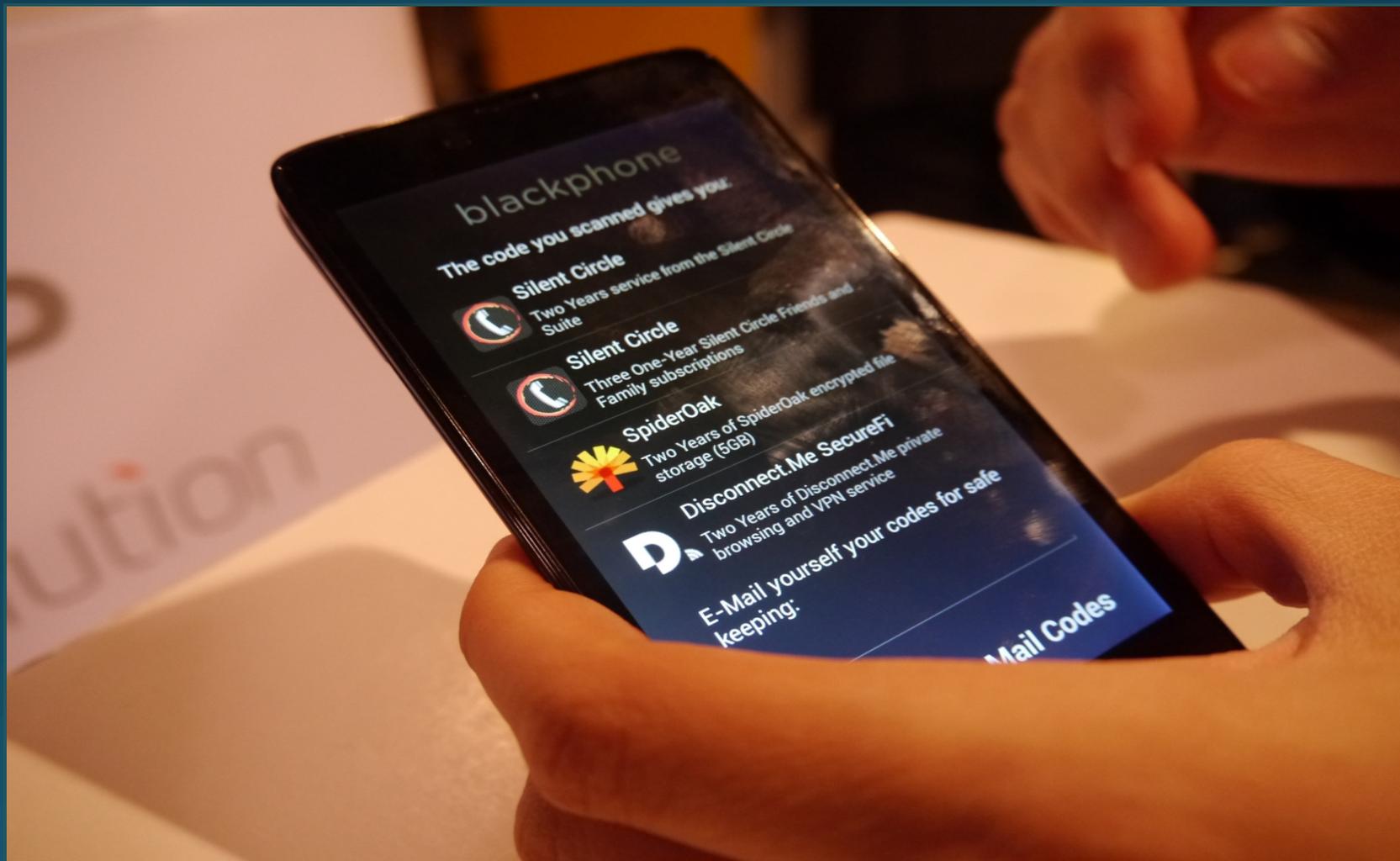
Facebook & Oculus VR



Internet Access by Drone



Blackphone - \$629



Questions?

