



**Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation...A graphic representation of data abstracted from the banks of every computer in the human system.**

- Gibson, William (1984). *Neuromancer*

# GOALS & CONSTRAINTS

—

Cyber security in mobile context

—

Definitions, velocity and opportunities

—

Define three mobile types of attacks

—

Live Demonstration

—

Techniques to mitigate mobile risks

## PRESENTER

Andrew Hoog is the CEO/Co-founder of viaForensics.

Andrew is a published author, computer scientist, and mobile forensic/security researcher. He has several patents pending and does frequent presentations/briefings.

*Additionally*

Pursuing Executive MBA, University of Chicago



# VIAFORENSICS OVERVIEW

viaForensics is a Mobile Security company founded in 2009.

Bootstrapped with ~40 employees and a 10 person dedicated mobile security R&D team

*Customer Breakdown*

50% US Government, 50% commercial

# CYBERSPACE

A global domain within the information environment consisting of the *interdependent network of information systems* infrastructures including the *Internet, telecommunications networks, computer systems* and *embedded processors and controllers*

[http://www.cnss.gov/Assets/pdf/cnssi\\_4009.pdf](http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf)

# CYBERATTACK

An attack, via cyberspace, for the purpose of *disrupting, disabling, destroying, or maliciously controlling* a computing environment/infrastructure;  
or *destroying the integrity of the data*  
or *stealing controlled information*

[http://www.cnss.gov/Assets/pdf/cnssi\\_4009.pdf](http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf)

# CYBERSECURITY

The ability to *protect or defend*  
the use of **cyberspace** from  
**cyber attacks**

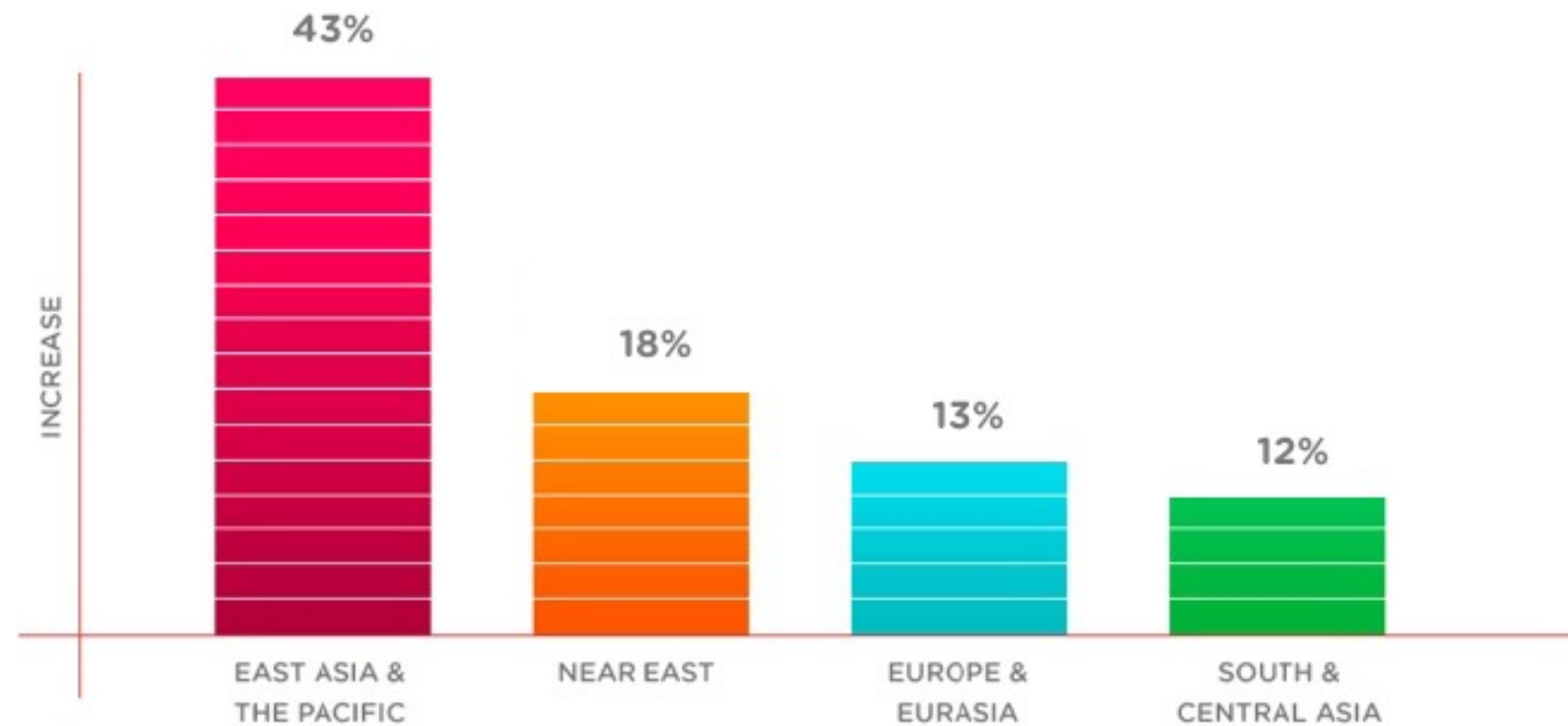
[http://www.cnss.gov/Assets/pdf/cnssi\\_4009.pdf](http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf)



# DSS ON TARGETING OF U.S.

Targeting of U.S. technologies is constant and unwavering.

There has been a 75% increase overall from FY10.



# FBI COUNTERINTELLIGENCE

“...economic espionage losses to the American economy total more than \$13 billion...”



# ASSUME COMPROMISE

*Operate as if*

—

Hostile environment

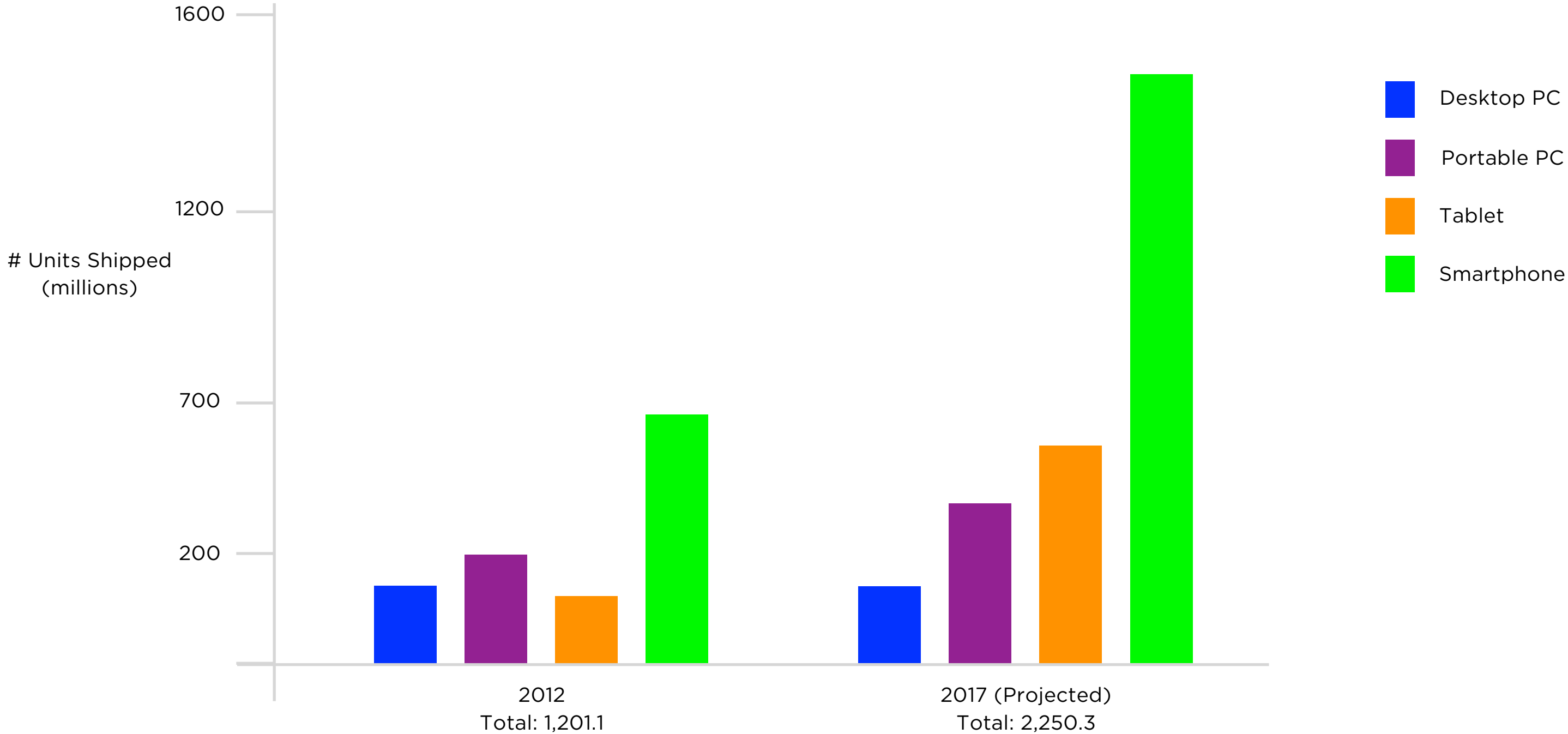
—

Compromised networks

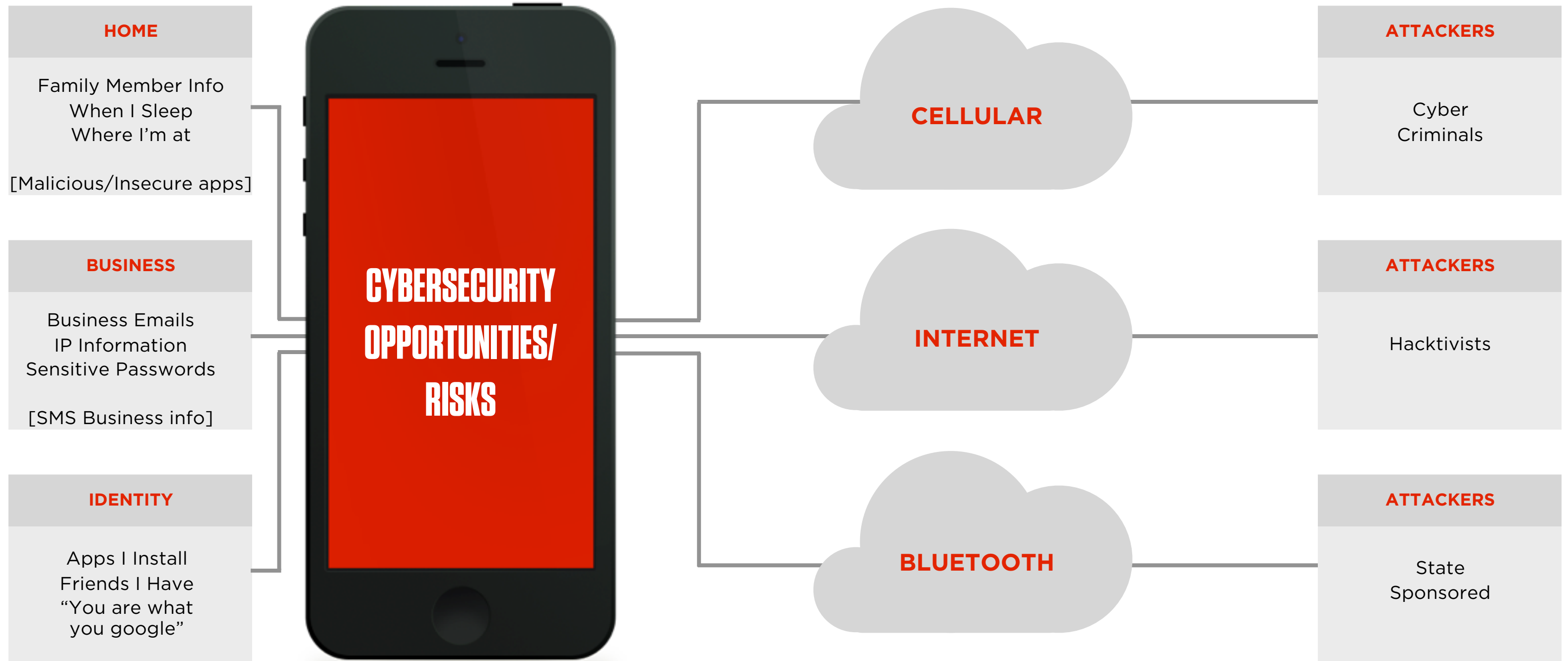
—

Vulnerable apps and devices

# MOBILE DEVICE VELOCITY



# HOW PEOPLE (MIS)USE MOBILE DEVICES



# BILLIONS OF DEVICES



**NEST THERMOSTAT**



**ALARM.COM**



**LG SMART TV**

# MOBILE OPPORTUNITIES (CONSUMERS)

—  
Loyalty, Cross-selling

—  
Rewards/offers

—  
Drive mobile payments

—  
Capture underbanked / unbanked

The image shows two mobile phone screens side-by-side. The left screen is labeled 'android phones' and displays the Cricket 4G LTE website. It features a green header with the Cricket logo and '4GLTE' text, followed by the slogan 'Get ready for fast everything.' and a 'shop now' button. Below this is a 'navigate' section with links for 'Overview', 'Android', and 'BlackBerry'. A second section titled 'already have cricket?' contains a login form with fields for 'Phone #' and 'Password', and buttons for 'register', 'forgot password?', and 'sign in'.

The right screen is labeled 'android smartphone' and displays an advertisement for the Huawei Mercury. The headline reads 'SAVE TIME & MONEY WITH THE SMARTPHONE THAT DOES IT ALL' and 'Get the Huawei Mercury with plans starting at just \$50/month'. The ad features a central image of the Huawei Mercury smartphone displaying the 'muve MUSIC' app. To the right of the phone are several feature icons: 'Entertain' (Find restaurants, movie times, recipes), 'Navigate' (Find where you need to go), 'Shop' (Searching millions of products), 'Socialize' (Stay connected with your friends), 'Chat' (Check in with friends), and 'Surf the Web' (Hold the Internet in your hand). A testimonial box on the right says 'The Best No Contract Smartphone' and includes a photo of a man and a 'PC EDITORS' CHOICE' award logo. At the bottom of the ad, it says 'ALL THE FEATURES. NO MORE FEES.' and has a 'shop now' button.

# MOBILE RISKS

—

Mobile attack

—

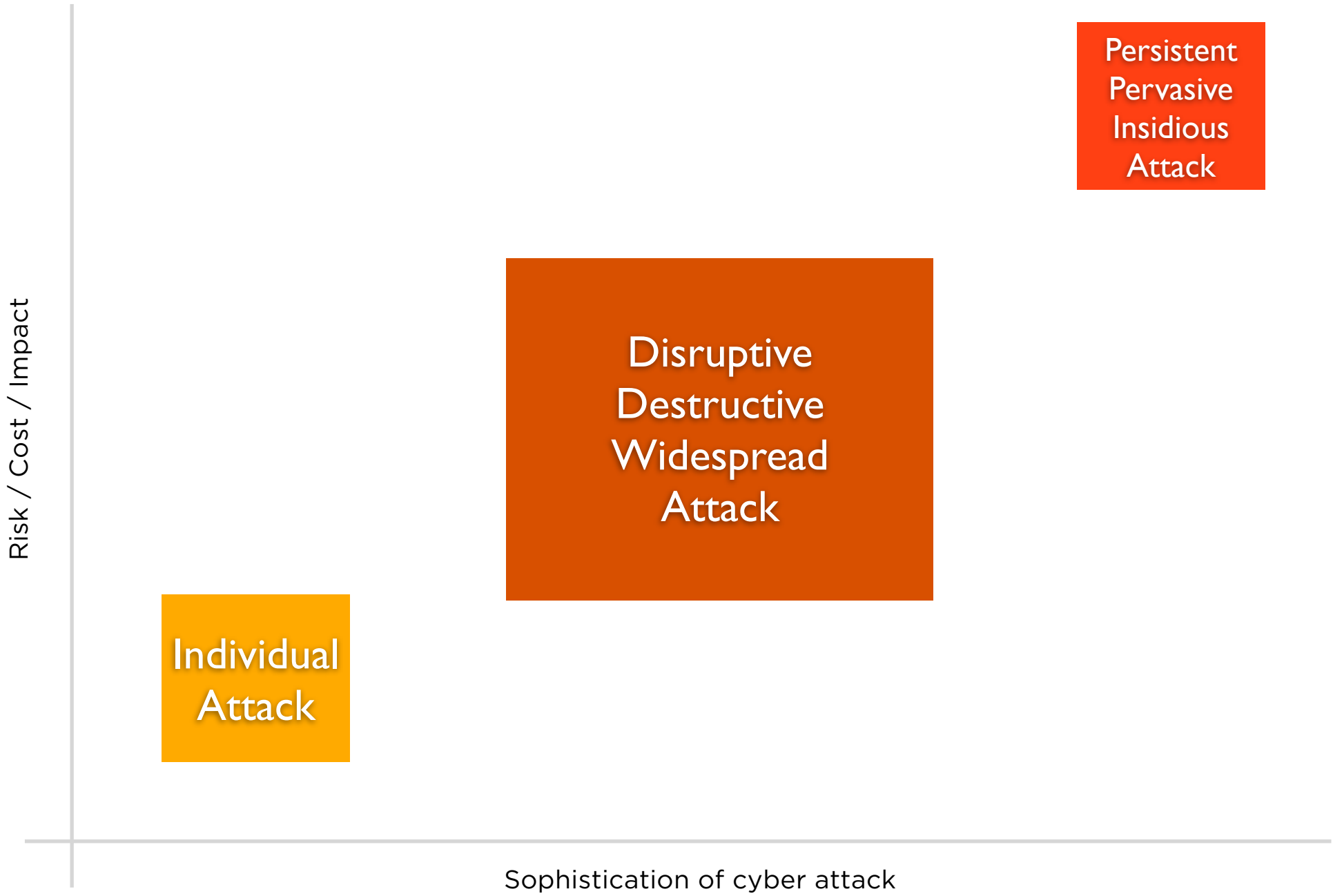
Compliance / Regulation

—

Legal / E-Discovery



# Mobile Attacks



# MOBILE BANKING/PAYMENT ATTACKS

INDIVIDUAL	DISRUPTIVE / DESTRUCTIVE / WIDESPREAD	PERSISTENT / PERVASIVE / INSIDIOUS
<p><i>Goals:</i> Identity theft Financial theft (small)</p> <p><i>Attackers:</i> Individual criminal Cyber criminal</p> <p><i>Methods:</i> Mobile app vulnerabilities Recover sensitive data Intercept username/password Physical access</p>	<p><i>Goals:</i> Impact profits Make a statement</p> <p><i>Attacker profiles:</i> Hacktivist Cyber criminal groups State sponsored</p> <p><i>Methods:</i> DDoS SQL Injection</p>	<p><i>Goals:</i> Intellectual property theft Financial theft (large) Espionage</p> <p><i>Attacker profiles:</i> Cyber criminal groups State sponsored</p> <p><i>Methods:</i> 0-day Targeted attacks Malware implants</p>

# MOBILE APP VETTING

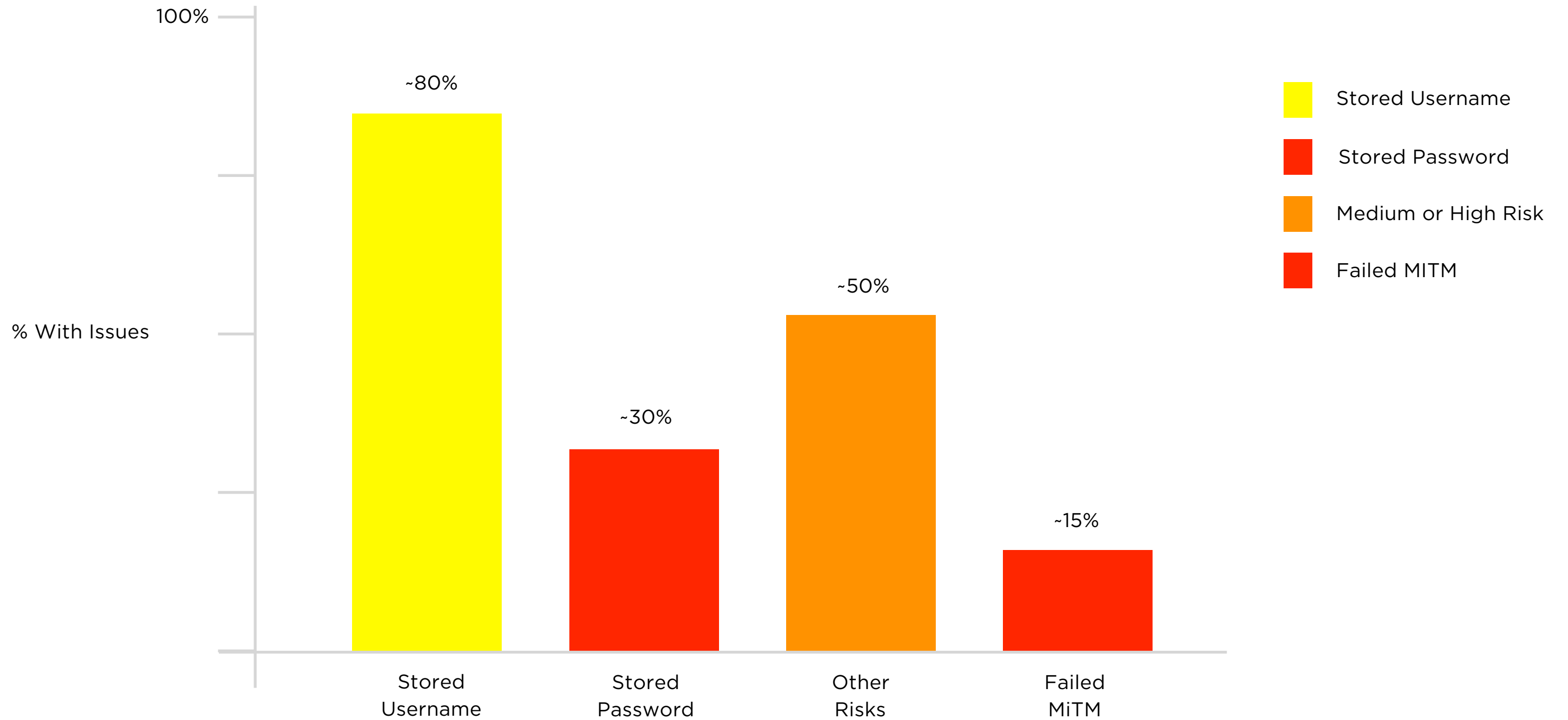
# APP SELECTION

Apps were selected based on popularity, number of downloads, or potential sensitivity of data

Approximately 50 apps have been reviewed and organized into categories

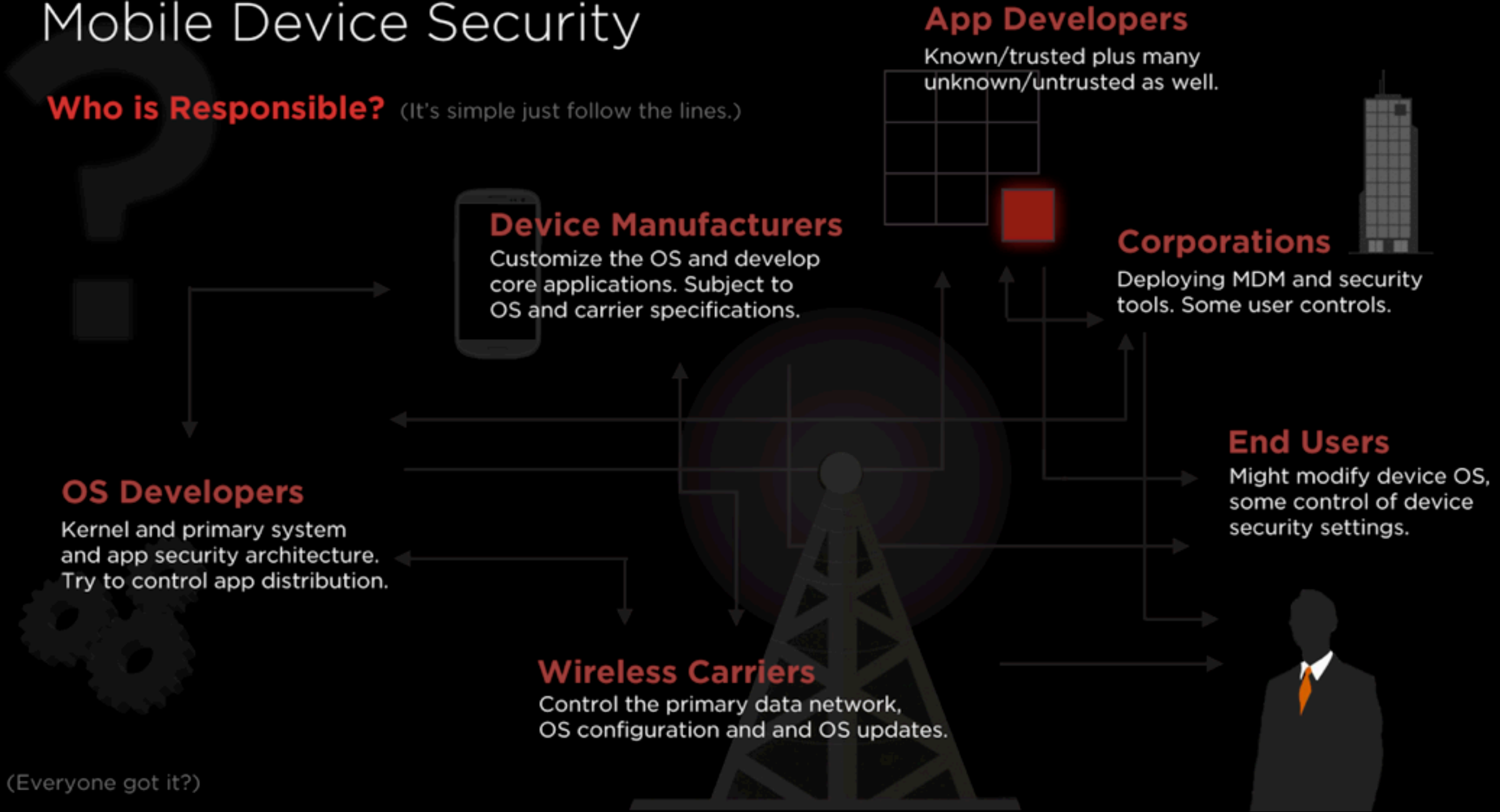
Category	# apps reviewed
Finance	10
Lifestyle	11
Productivity	6
Travel	5
Social Networking	6
Security	6
Other	6

# APP TESTING RESULTS



# Mobile Device Security

**Who is Responsible?** (It's simple just follow the lines.)



(Everyone got it?)

**IN 1955, THE KGB DESIGNED  
THE ULTIMATE ESPIONAGE  
DEVICE, THOUGH  
IMPOSSIBLE TO BUILD WITH  
TECHNOLOGY OF THE ERA...**

## ... IT IS NOW PERVASIVE

- Flexible means to gather intelligence
- Remotely accessible and updateable
- Possesses sophisticated sensors
- Goes anywhere, does not attract attention
- And targets readily carry it with them





# CORPORATE ESPIONAGE

- Theft of sensitive data, processes, relationships to influence competitive advantage
- Increasingly perpetrated via cyber



# ENTER MOBILE

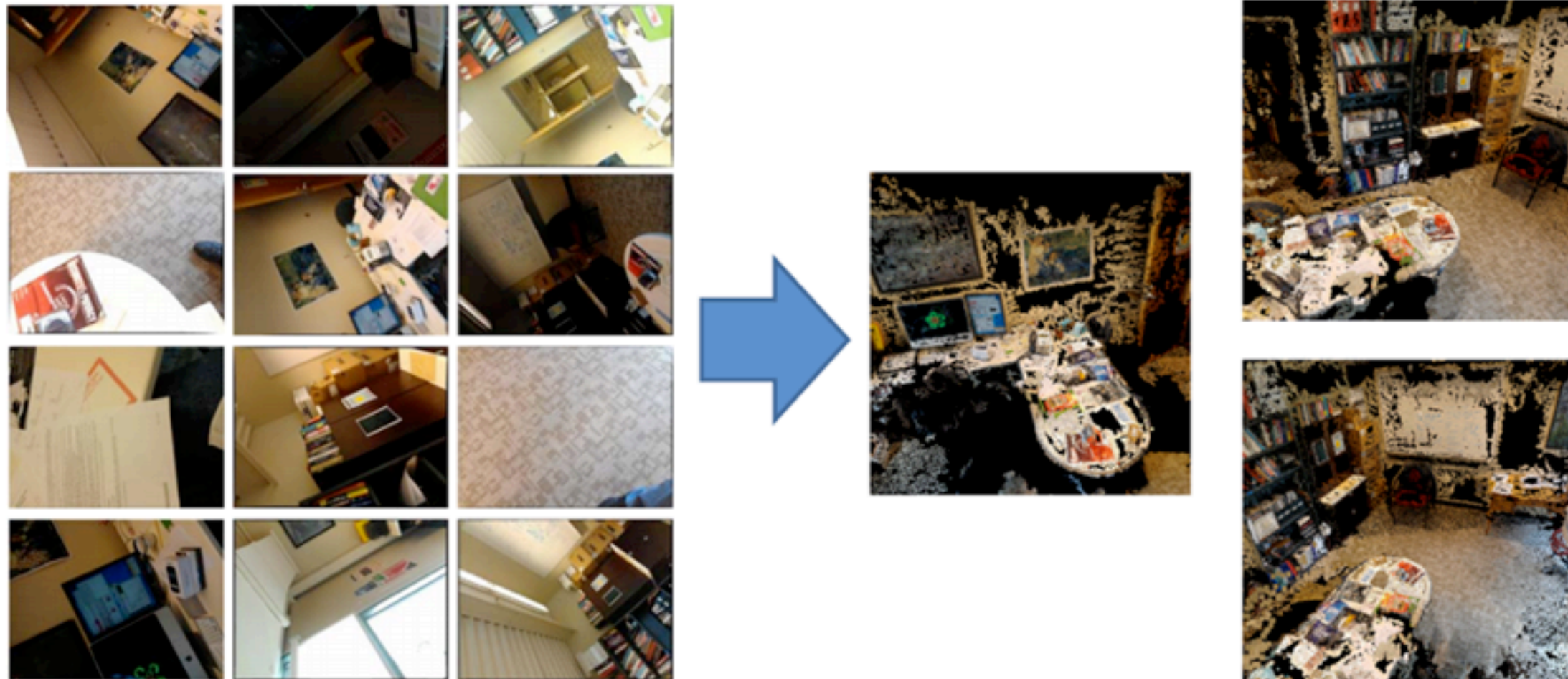
- Operates on both sides of the firewall
- Stores sensitive corporate and personal data
- Mostly outside the control of IT/ Security (BYOD)
- Runs loads of untested code, of unknown origin



# **BYPASSING TRADITIONAL DEFENSES**

# CIRCUMVENT TRADITIONAL CORPORATE SECURITY CONTROLS...

# HIJACK THE CAMERA



*PlaceRaider “visual malware”  
Robert Templeman, et al*

# MOBILE ATTACK DEMO

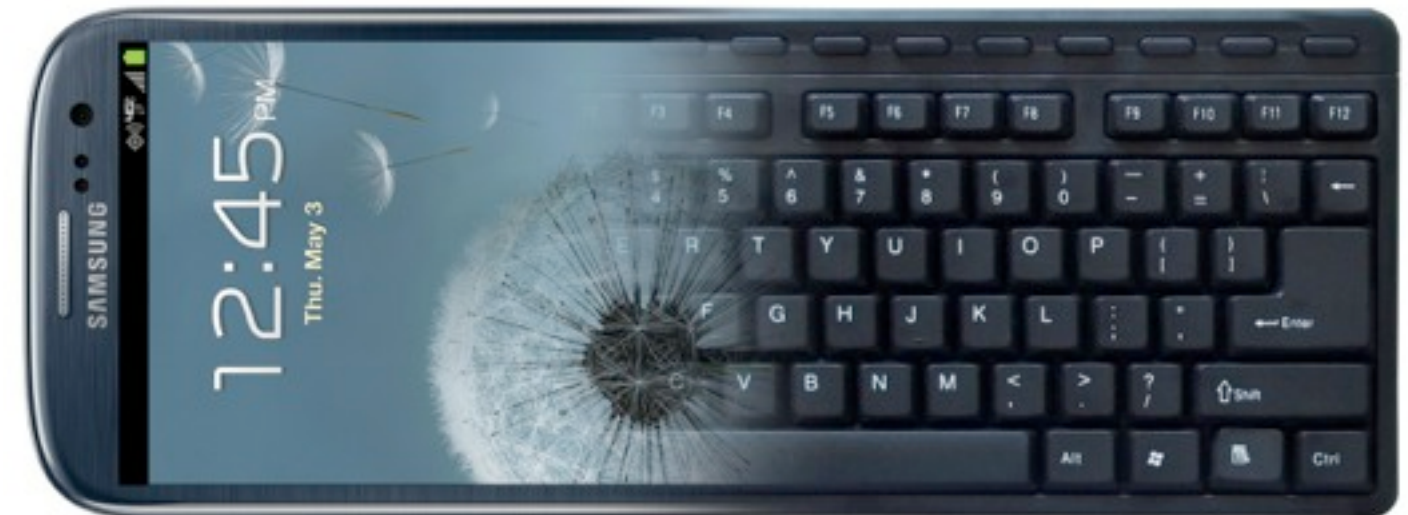
## CORPORATE ESPIONAGE VIA MOBILE COMPROMISE

—  
Remote compromise mobile device

—  
Morph mobile device into keyboard

—  
Circumvents all traditional defenses

—  
Gives attacker hands on keyboard/network



# IN THE NEWS



**USB AUTORUN**



**CARBERP WENT MOBILE**





**SPEAR PHISHING**

# IN THE NEWS

Detection ratio: 1/46

SHA256:	e275b06aa61cc9be5a5805200c33f357a7b6952fe379055305d73315a8f94e7c
File name:	Document.apk
Detection ratio:	1 / 46
Analysis date:	2013-03-26 12:58:41 UTC ( 1 week, 2 days ago ) <a href="#">View latest</a>

  
More details





# IMPACTS TO BUSINESS

—

Loss of intellectual property/sensitive data

—

Loss of market confidence

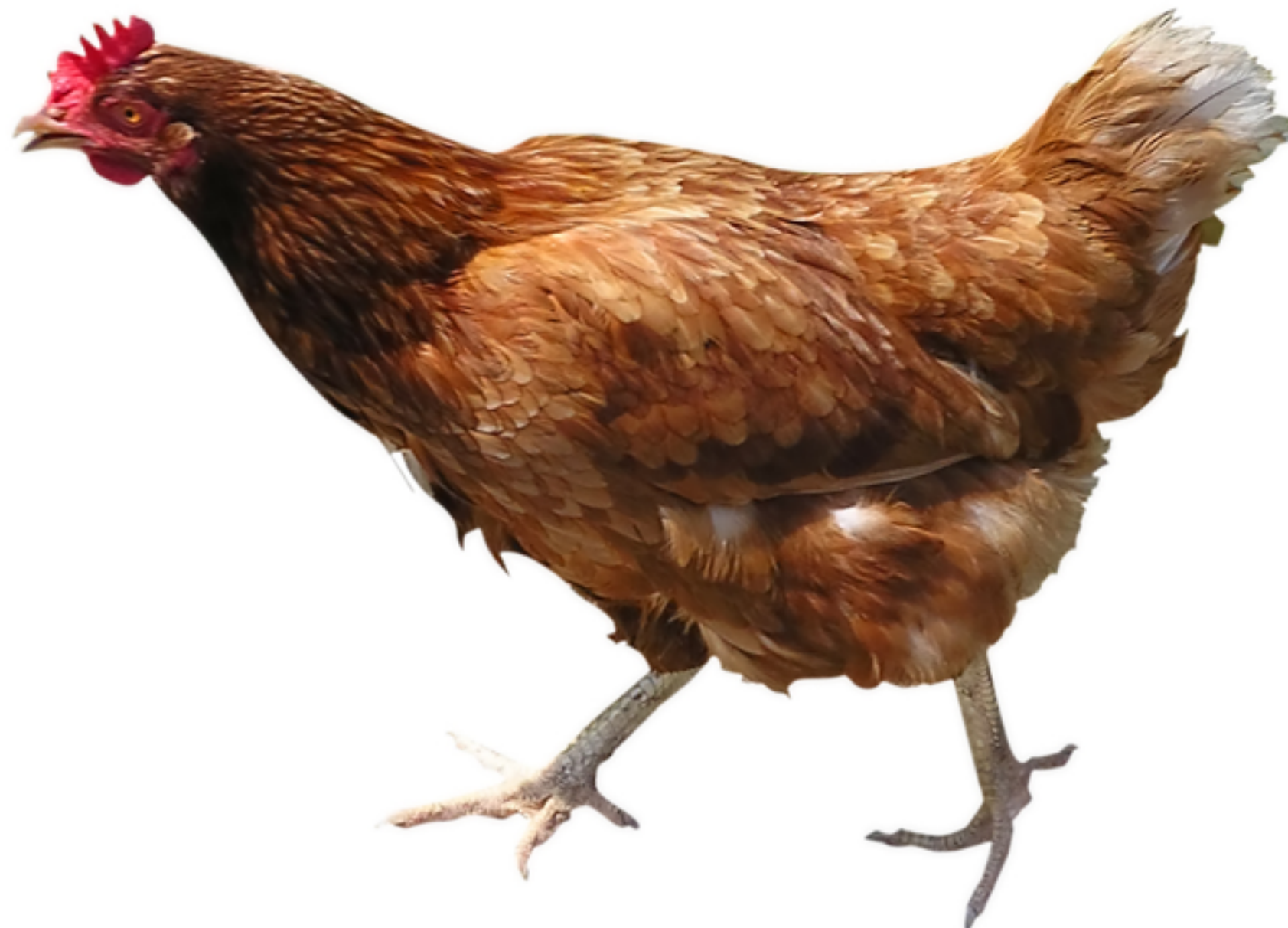
—

Loss of customers

—

Loss of revenue

# THE SKY IS NOT FALLING



# SECURE MOBILE APPS

---

## Education

*[Devs, Security, & Executives]*

---

## Mobile app vetting

*[Custom & Third-party]*



### SECURE MOBILE DEVELOPMENT BEST PRACTICES

42+ best practices. FREE from experts in  
mobile security.

READ NOW

# MOBILE SENSORS MITIGATE MOBILE RISKS

—  
Collect mobile forensic, security and sensor data

—  
Analyze to improve decisions

—  
Reduce mobile banking and payment risks



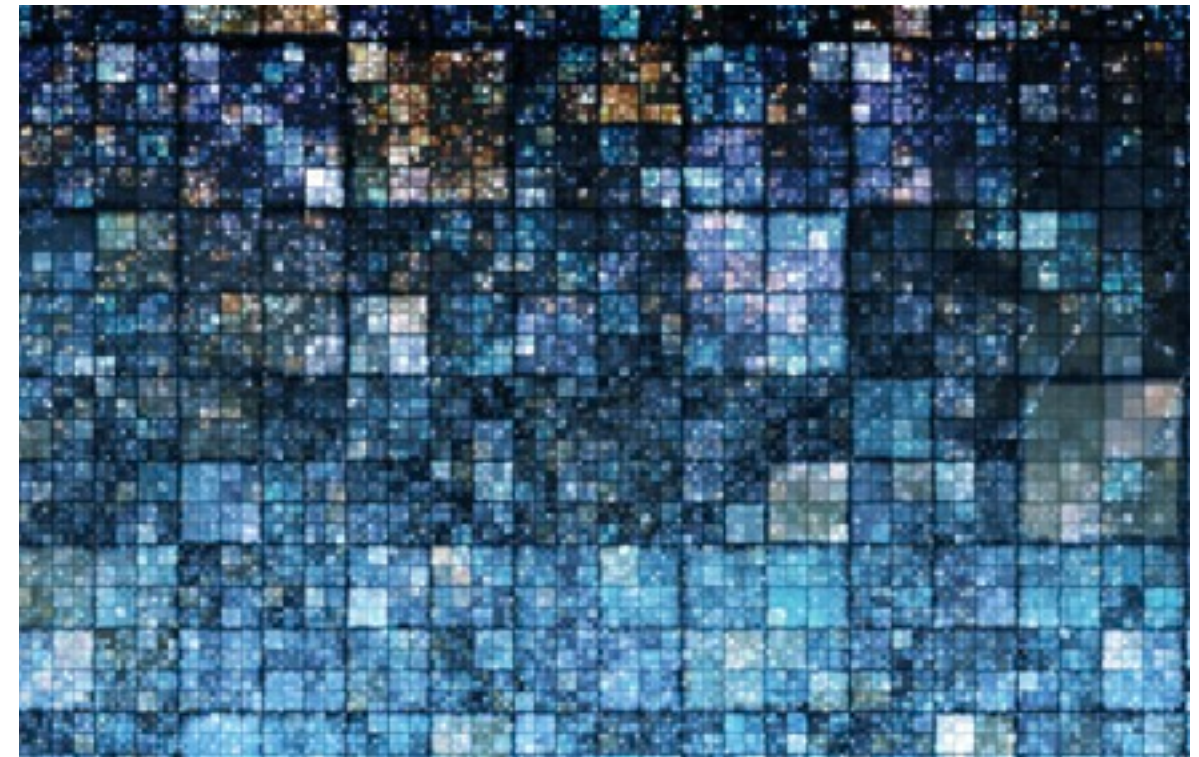
# INTELLIGENCE DRIVEN SECURITY

—  
Defense cannot prevent all attacks

—  
Big Data can detect anomalies

—  
Practical Cyber Security:

***Detect and prevent***





**VIAFORENSICS**  
advancing mobile security

Andrew Hoog

312-878-1100

[ahoog@viaforensics.com](mailto:ahoog@viaforensics.com)

Keep in touch with us on Twitter at  
[@viaforensics](https://twitter.com/viaforensics) or at [viaforensics.com](http://viaforensics.com).