Understanding and Managing Your Threat Landscape

Eric Kurnie, SVP, Wells Fargo

Cybersecurity Essentials – E11

CHANGING RISK LANDSCAPE

Cyber History

Cyber Current

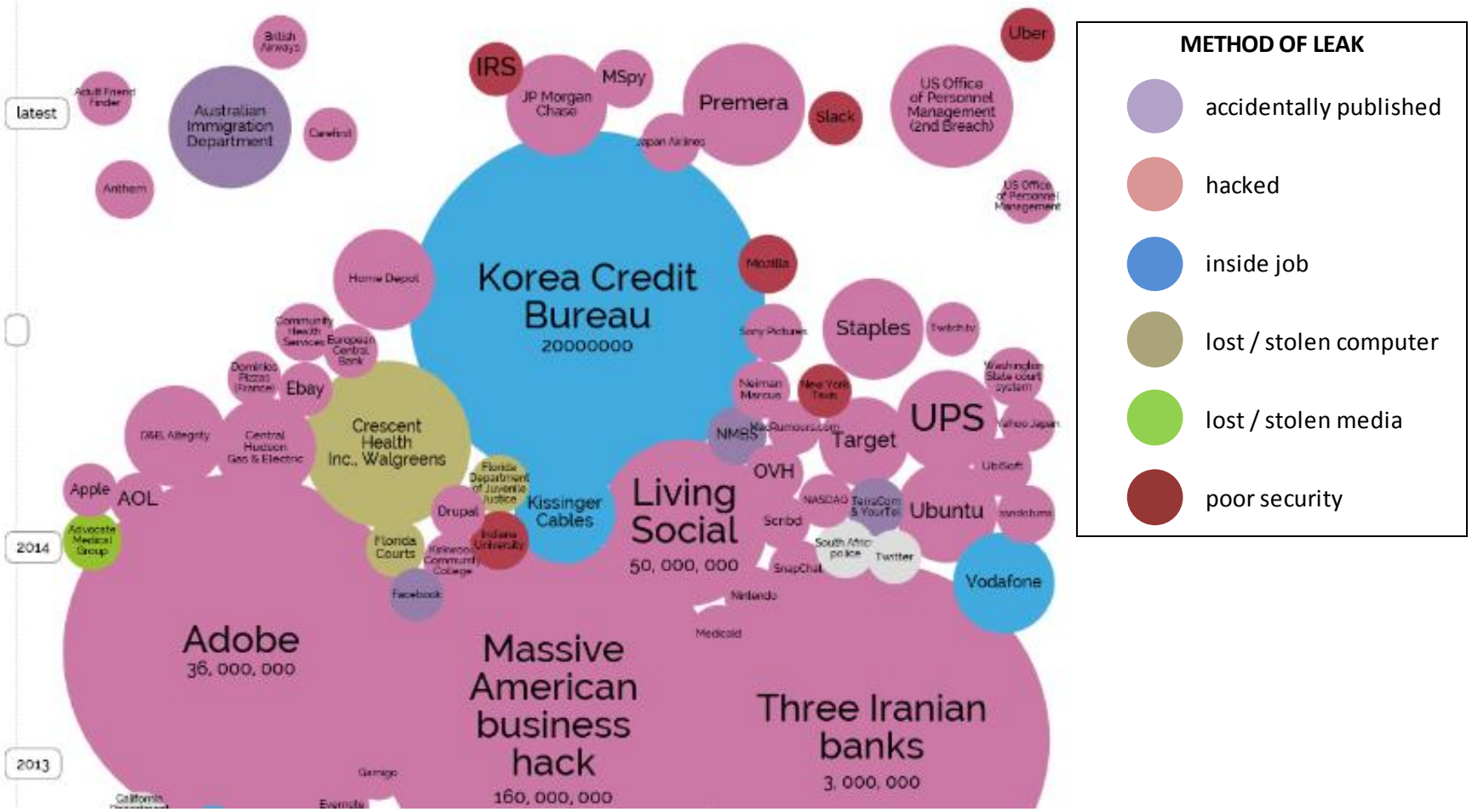
World's biggest data breaches: 2004 - 2005

METHOD OF LEAK

- accidentally published
- hacked
- inside job
- lost / stolen computer
- lost / stolen media
- poor security

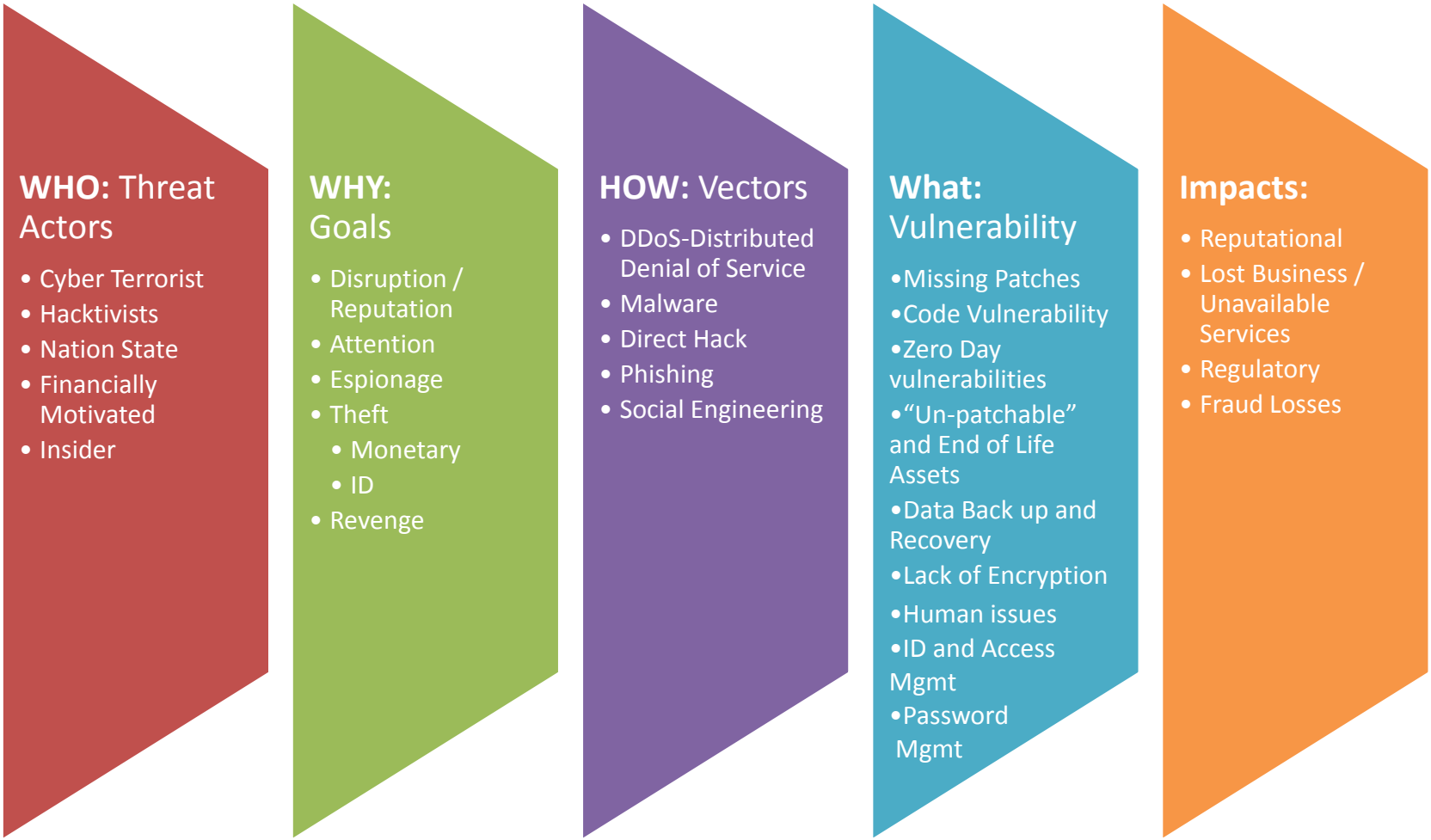
Source: www.informationisbeautiful.net. World's Biggest Data Breaches

World's biggest data breaches: 2013 - 2015



Source: www.informationisbeautiful.net. World's Biggest Data Breaches

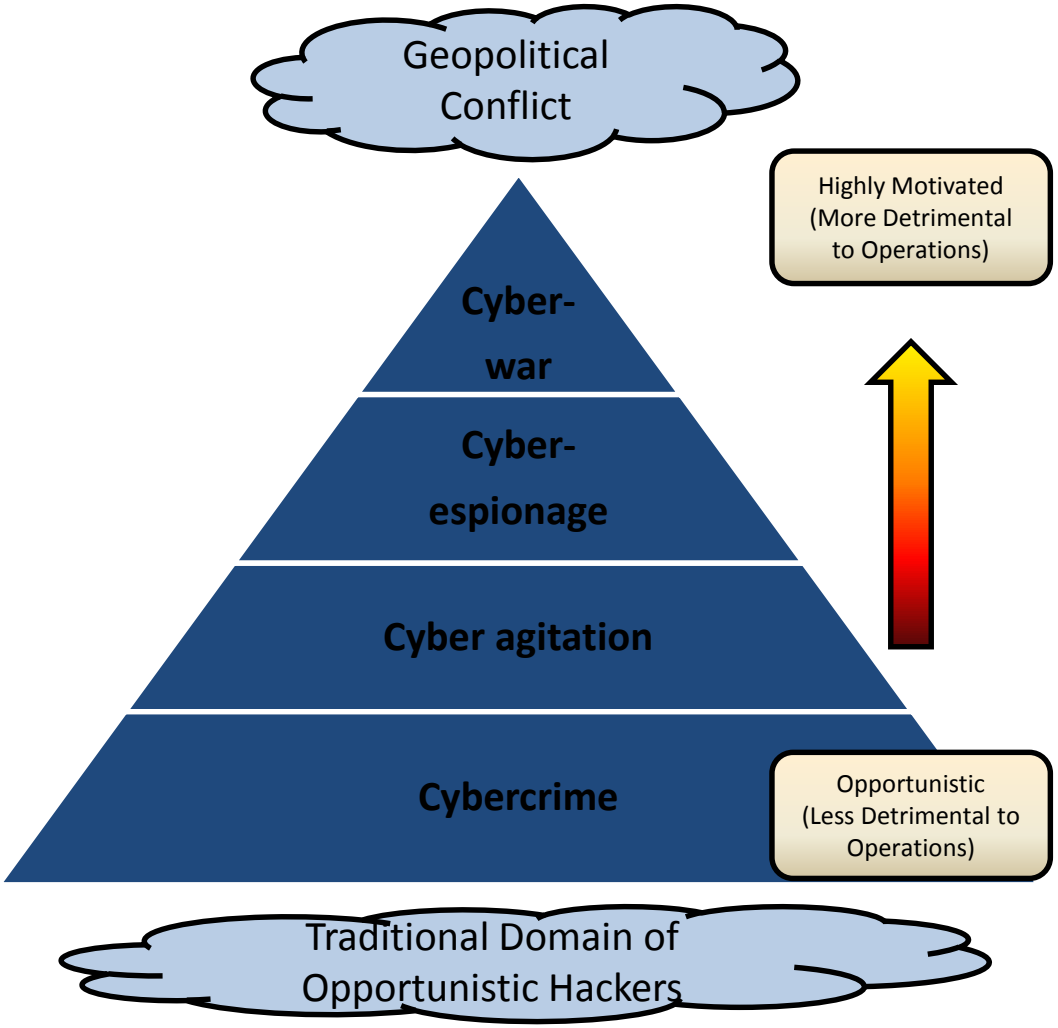
Who, Why, How, What, Impacts…



THREATS


ISACA
Trust in, and value from, information systems
San Francisco Chapter
CyberSizeIT
SF ISACA FALL CONFERENCE
NOVEMBER 9-11, 2015
HOTEL NIKKO-SAN FRANCISCO

Threat Landscape



Examples Targeted Assets

Estonia	Internet backbone
Georgia	Government sites
Stuxnet	Nuclear facility
Dupont	Trade Secrets
Night Dragon	Source code
Operation Aurora	Intellectual property
Rio Tinto	Strategic legal docs
Shady RAT	Bidding plans
Anonymous	Sensitive data ,various
Chevron	Public reputation
HBGary Federal	Sensitive emails
Sony	Executive's details
Scientology	DDoS, reputation
WikiLeaks	Classified documents
JPMC	Account information
Target/HD	Credit card data
Epsilon	Email addresses
Sony	Player accounts
SpyEye and Zeus	Login credentials, PIN

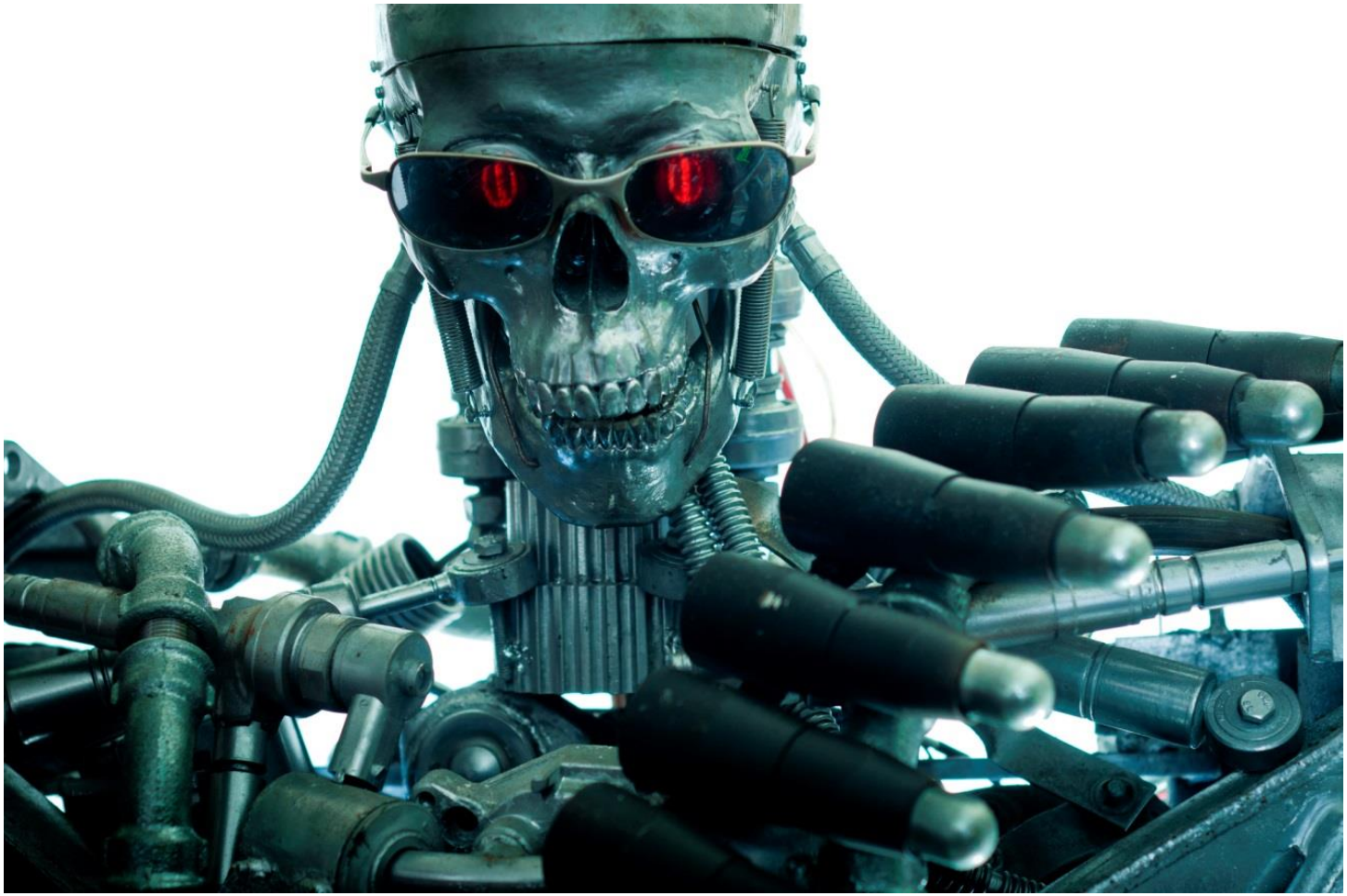
Opportunistic Hackers

Cybercrime

Cyber Agitation

Cyber Espionage

Cyber War



Today's Financial Industry Security Threat Landscape

Evolved Ecosystem

- Business growth drives more systems in the environment
  - Massive complexity and asset intimacy
  - Harder to understand all technical risks
- Requires more complex application / system development
- Attack surface has expanded significantly (mobile, wireless, cloud)

Adds to Defense in Depth

Increased Targeting of Informational Assets for Monetary Gain

External Threat Landscape

- More attackers, characterized as:
  - Sophisticated
  - Better resourced than their targets
  - Monetized incented attacks
  - Security controls also targets (e.g. tokens)
- Targets no longer limited to certain industry sectors
- Emergence of social engineering

Shifting Threat Landscape

The price of a data breach

Scottrade Stock Trading Service Hacked
possibly affecting 4.6 million customers

- October 2015

Anthem Hacked
Nearly 80 million Anthem members impacted

- February 2015

JP Morgan Chase Cyberattack affected 76 million households

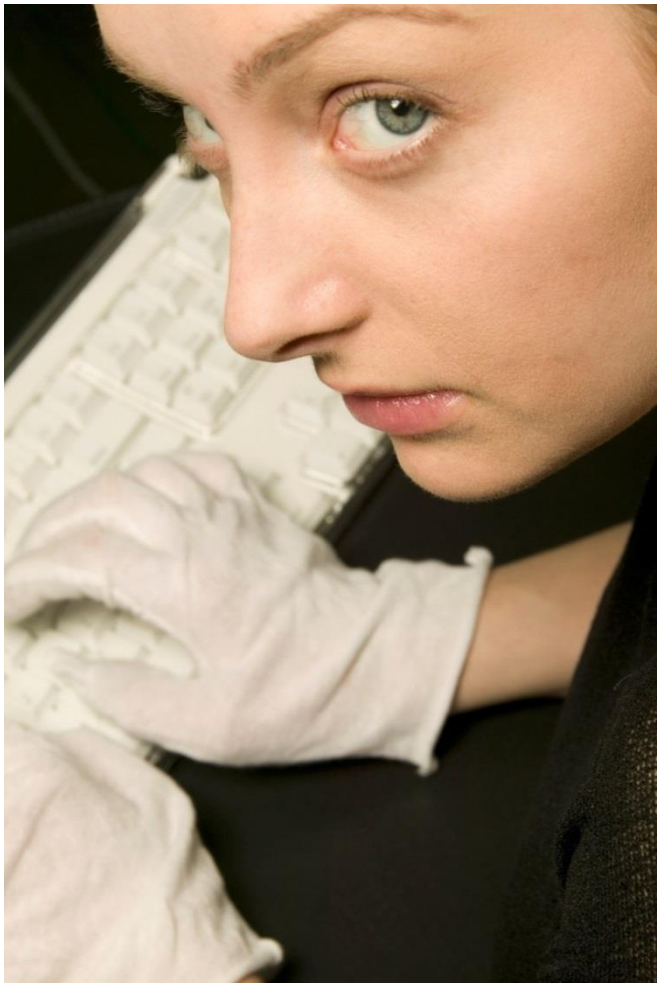
- July 2014

Miscellaneous Errors

Crimeware


spyware
spam
phishing
trojan
data security
virus
attack
25%
30%
malware
virus alert!
virus detected

Insider Misuse



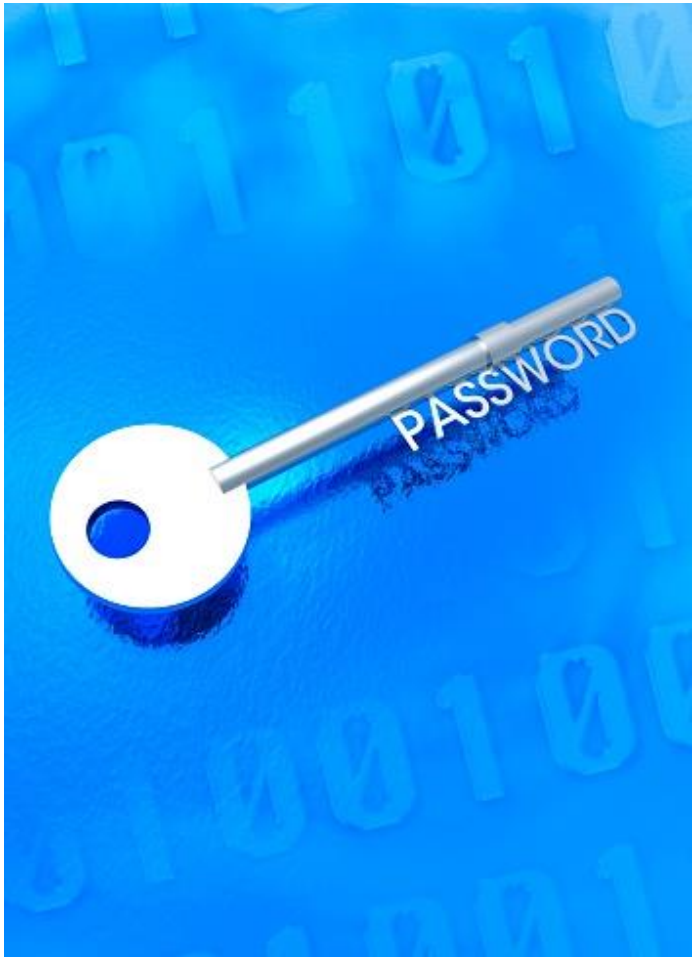
VULNERABILITIES

Don’t be a… (video)

https://www.youtube.com/watch?v=nPR131wMKEo

Passwords

Password1?

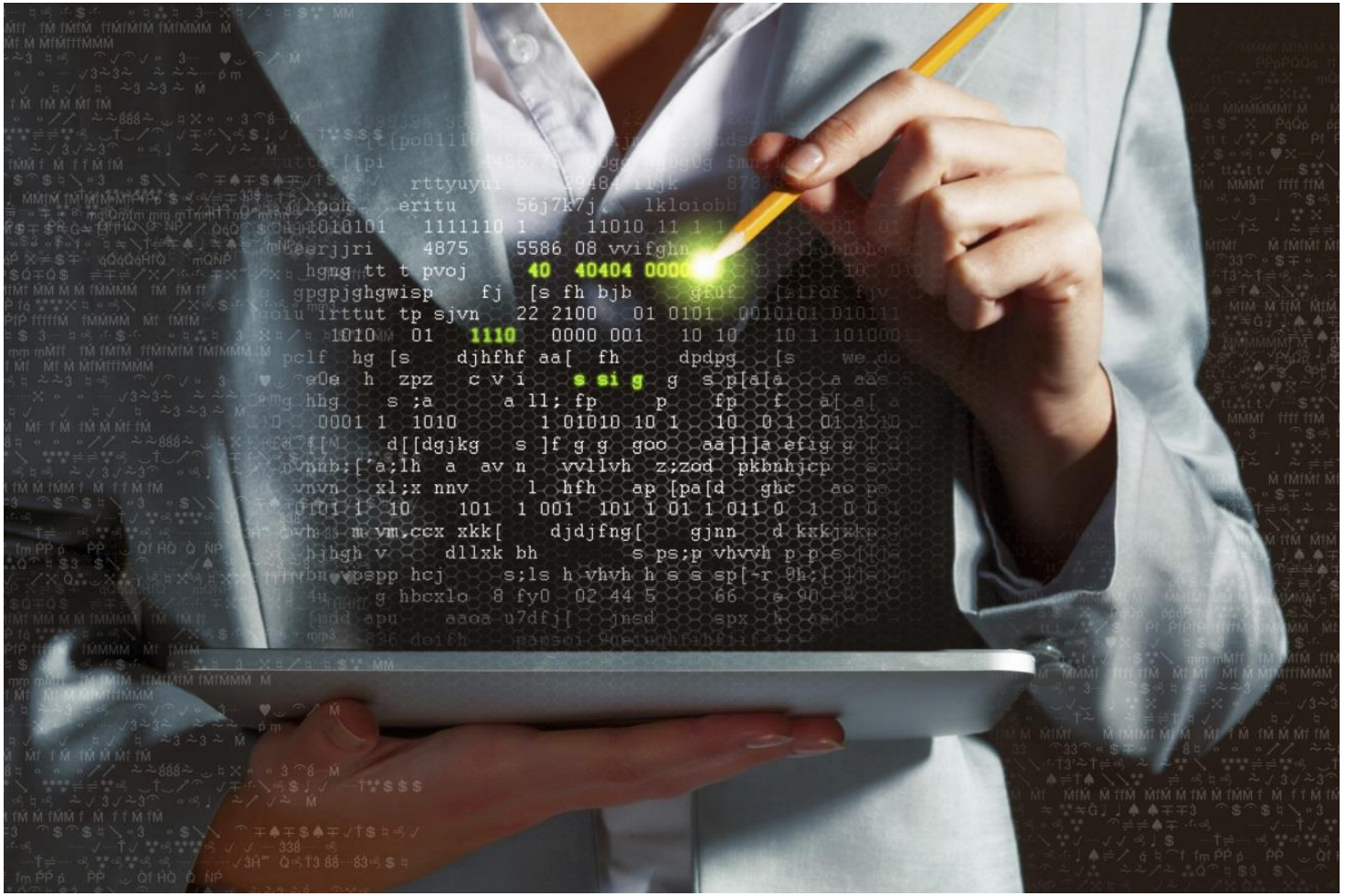


$m=gC+M&cH

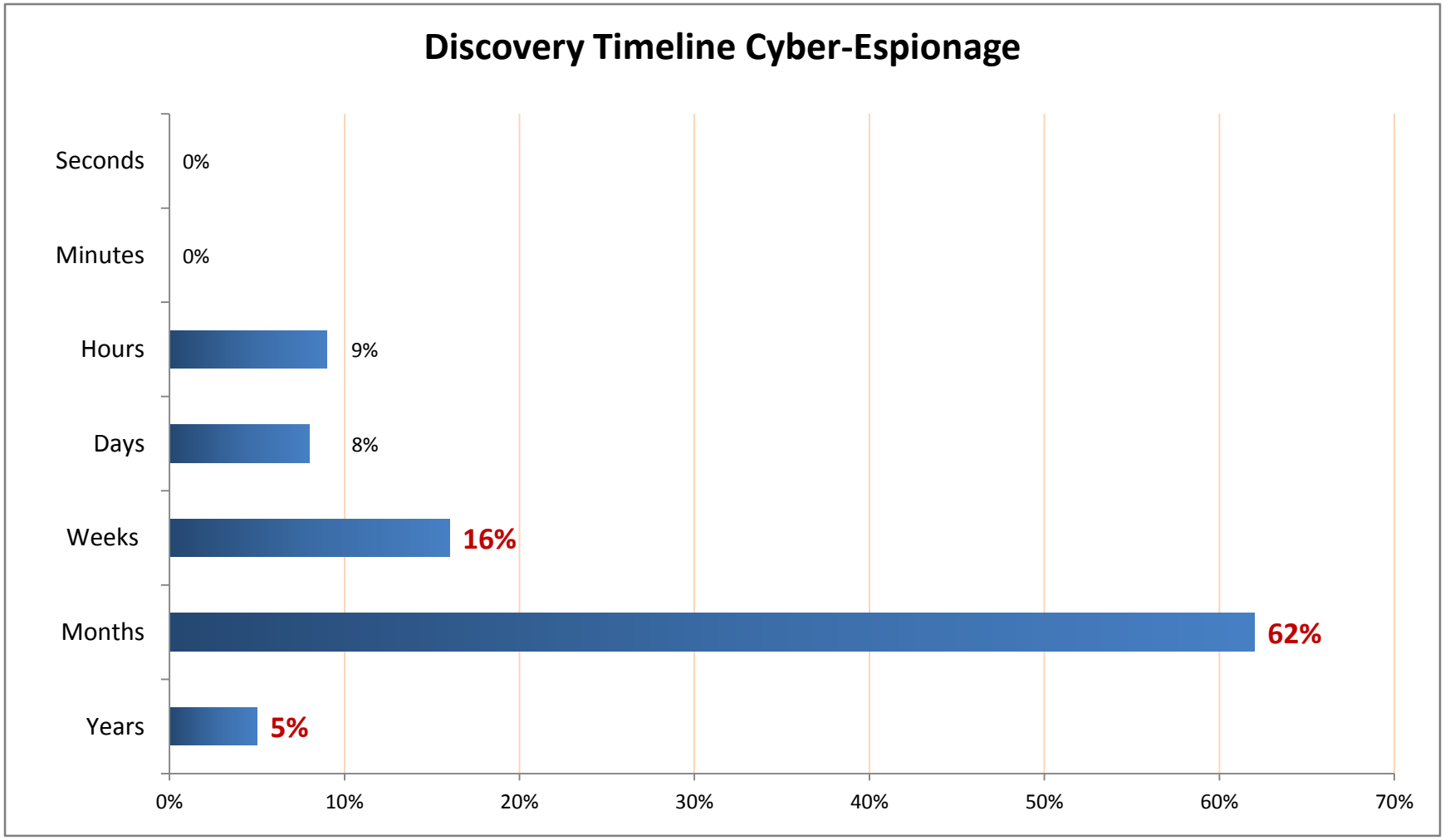
Passwords – additional controls

Social Engineering

Published Vulnerabilities



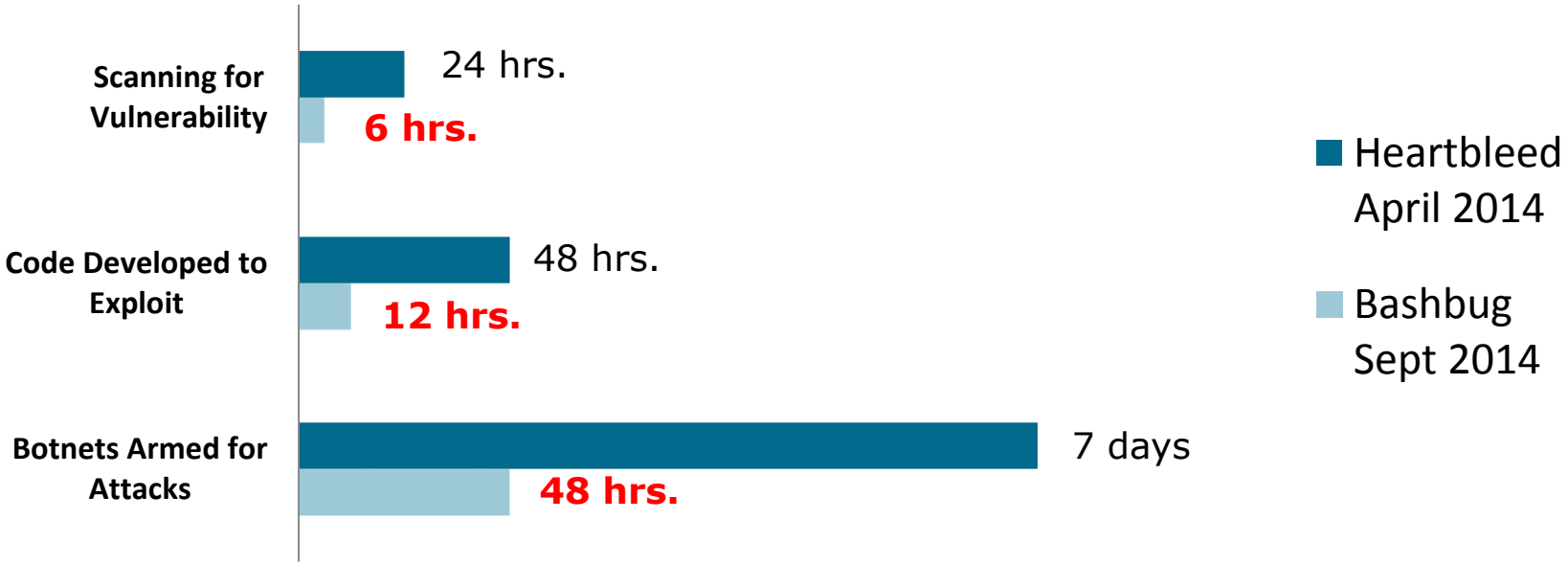
83 percent+ of compromises go undetected for long periods of time



Zero-Day Vulnerabilities

Attackers moving at an increasing speed

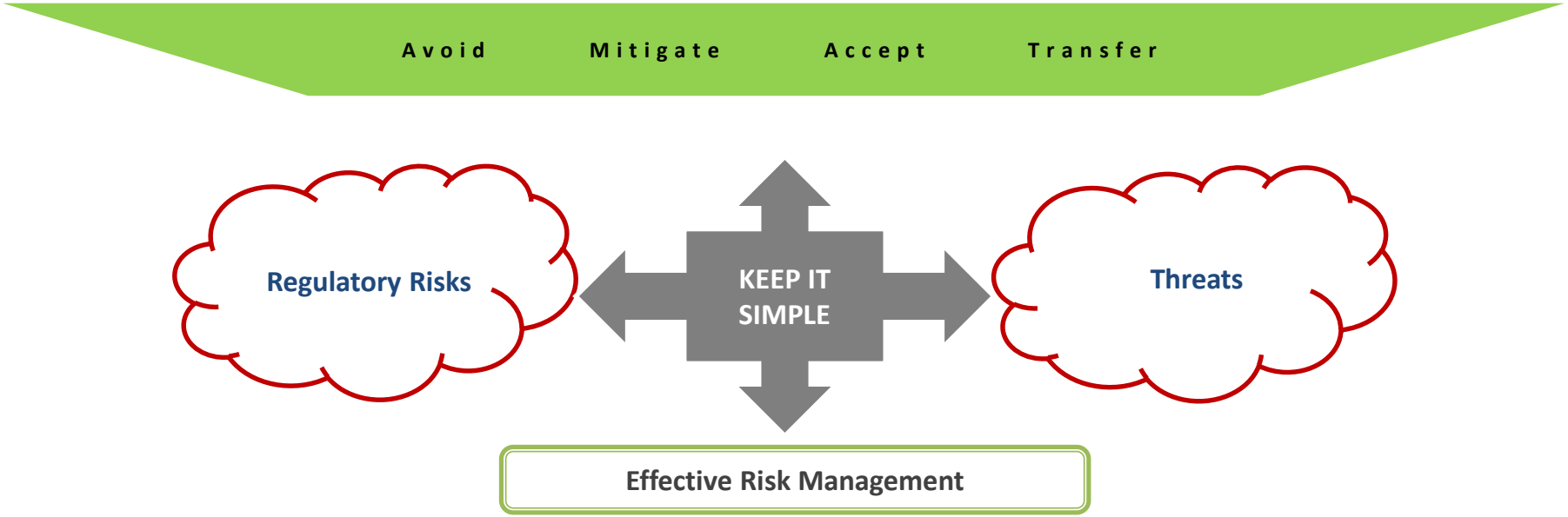
In five months, the attacker's average time to exploit was reduced by almost two-thirds



* Data points compiled from several public sources

Managed evolution results in effective risk management

Focus on the current state of risk and the impact that the evolving risk landscape, new technologies, and business processes present during this journey.



Conclusion

QUESTIONS? COMMENTS?

CONTACT INFORMATION:
ERIC KURNIE
(650) 773-0044
KURNIE@WELLSFARGO.COM