

Understanding and Managing Your Threat Landscape

Eric Kurnie, SVP, Wells Fargo

Cybersecurity Essentials – E11



Trust in, and value from, information systems

San Francisco Chapter

The "CyberSizelT" logo is set against a background of a stylized city skyline and bridges, including the Golden Gate Bridge. The word "CyberSizelT" is written in a large, bold, red font with a white outline. The "T" is significantly larger than the other letters and has a unique shape.

CyberSizelT

CHANGING RISK LANDSCAPE



Trust in, and value from, information systems

San Francisco Chapter

A stylized graphic of the San Francisco skyline at sunset, featuring the Golden Gate Bridge and various skyscrapers. The word "CyberSizelT" is overlaid on the skyline in a large, red, outlined font. The "T" is significantly larger than the other letters.

CyberSizelT

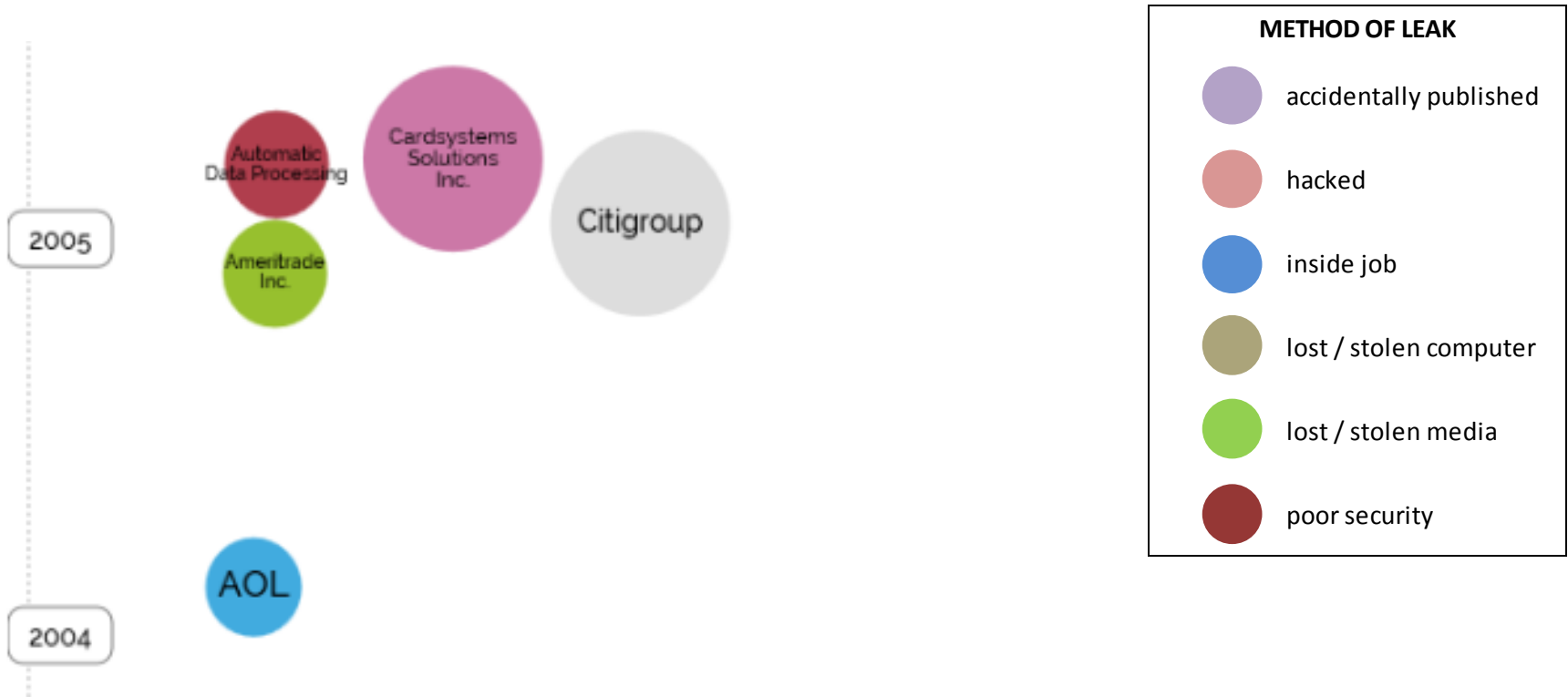
Cyber History



Cyber Current

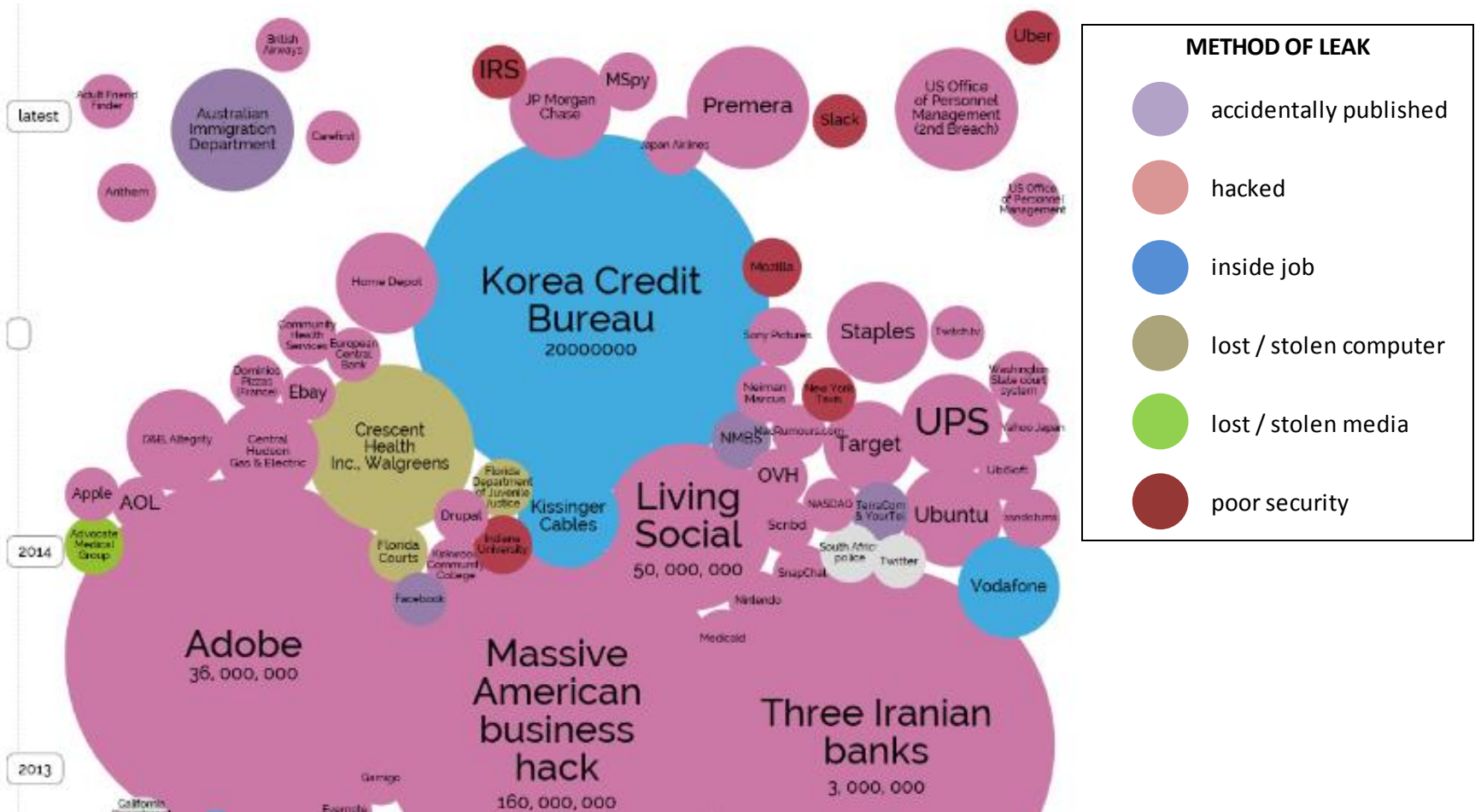


World's biggest data breaches: 2004 - 2005



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...

WHO: Threat Actors

- Cyber Terrorist
- Hacktivists
- Nation State
- Financially Motivated
- Insider

WHY: Goals

- Disruption / Reputation
- Attention
- Espionage
- Theft
 - Monetary
 - ID
- Revenge

HOW: Vectors

- DDoS-Distributed Denial of Service
- Malware
- Direct Hack
- Phishing
- Social Engineering

What: Vulnerability

- Missing Patches
- Code Vulnerability
- Zero Day vulnerabilities
- “Un-patchable” and End of Life Assets
- Data Back up and Recovery
- Lack of Encryption
- Human issues
- ID and Access Mgmt
- Password Mgmt

Impacts:

- Reputational
- Lost Business / Unavailable Services
- Regulatory
- Fraud Losses

THREATS

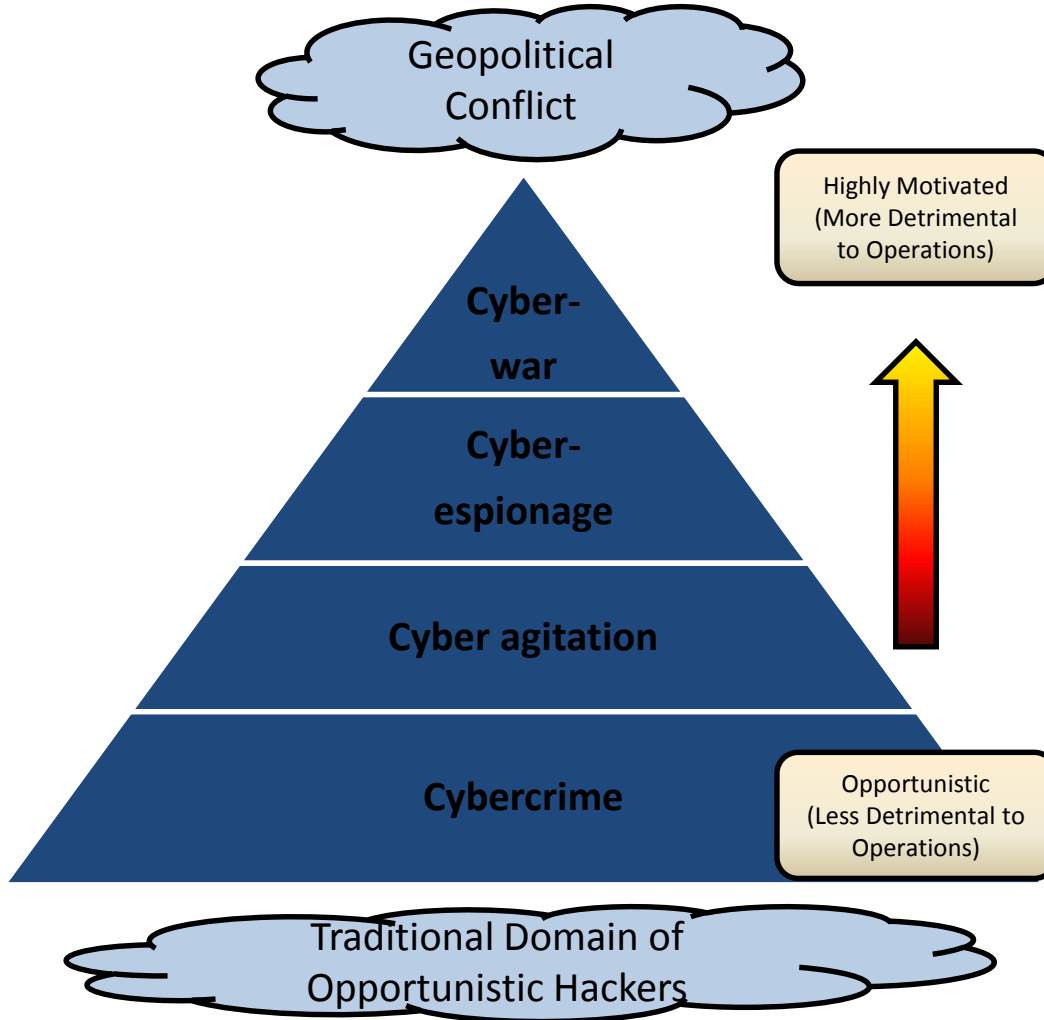


Trust in, and value from, information systems

San Francisco Chapter



Threat Landscape



Examples Targeted Assets

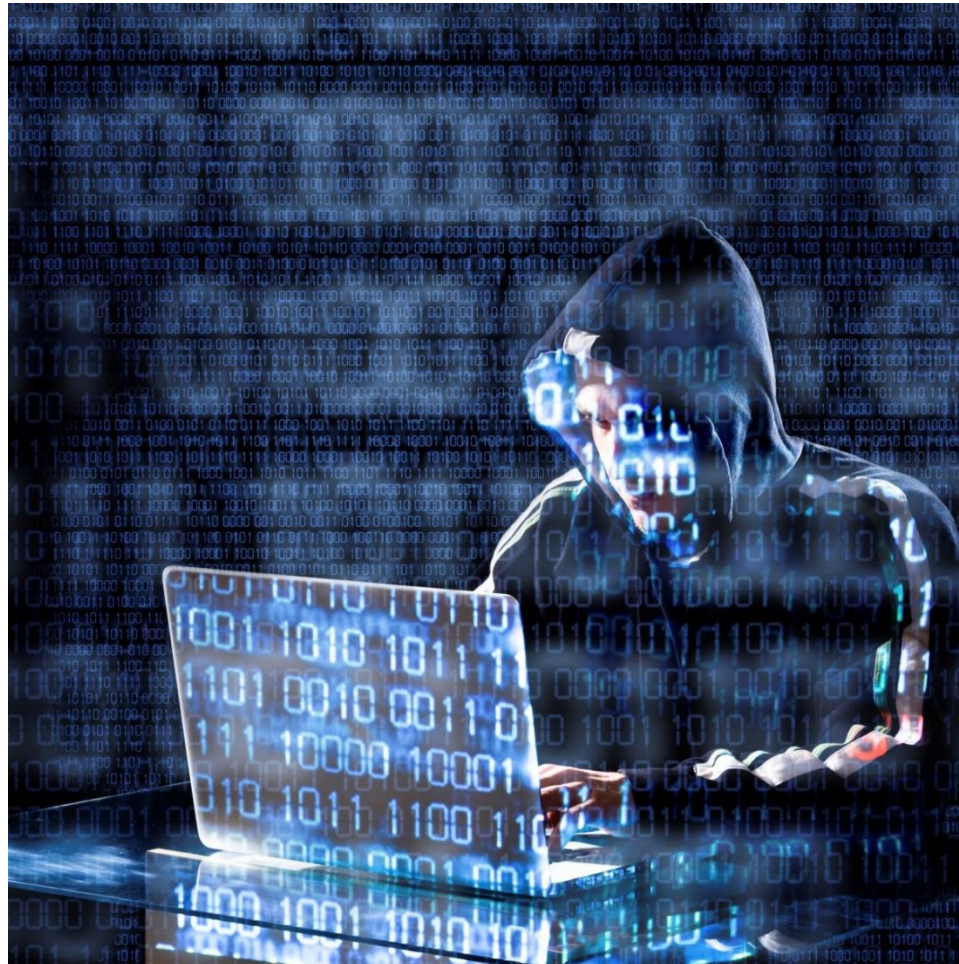
Estonia	Internet backbone
Georgia	Government sites
Stuxnet	Nuclear facility

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



2015 Fall Conference – “CyberSizeIT”
November 9 – 11, 2015

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

External Threat Landscape

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

Shifting Threat Landscape

Increased Targeting of
Informational Assets
for Monetary Gain

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

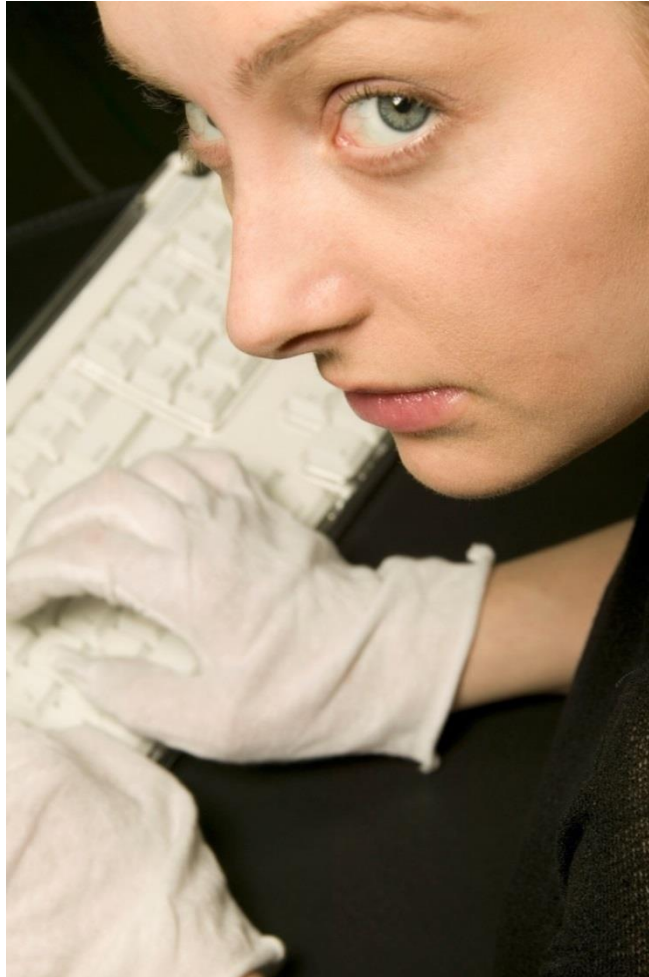
Miscellaneous Errors



Crimeware



Insider Misuse



VULNERABILITIES

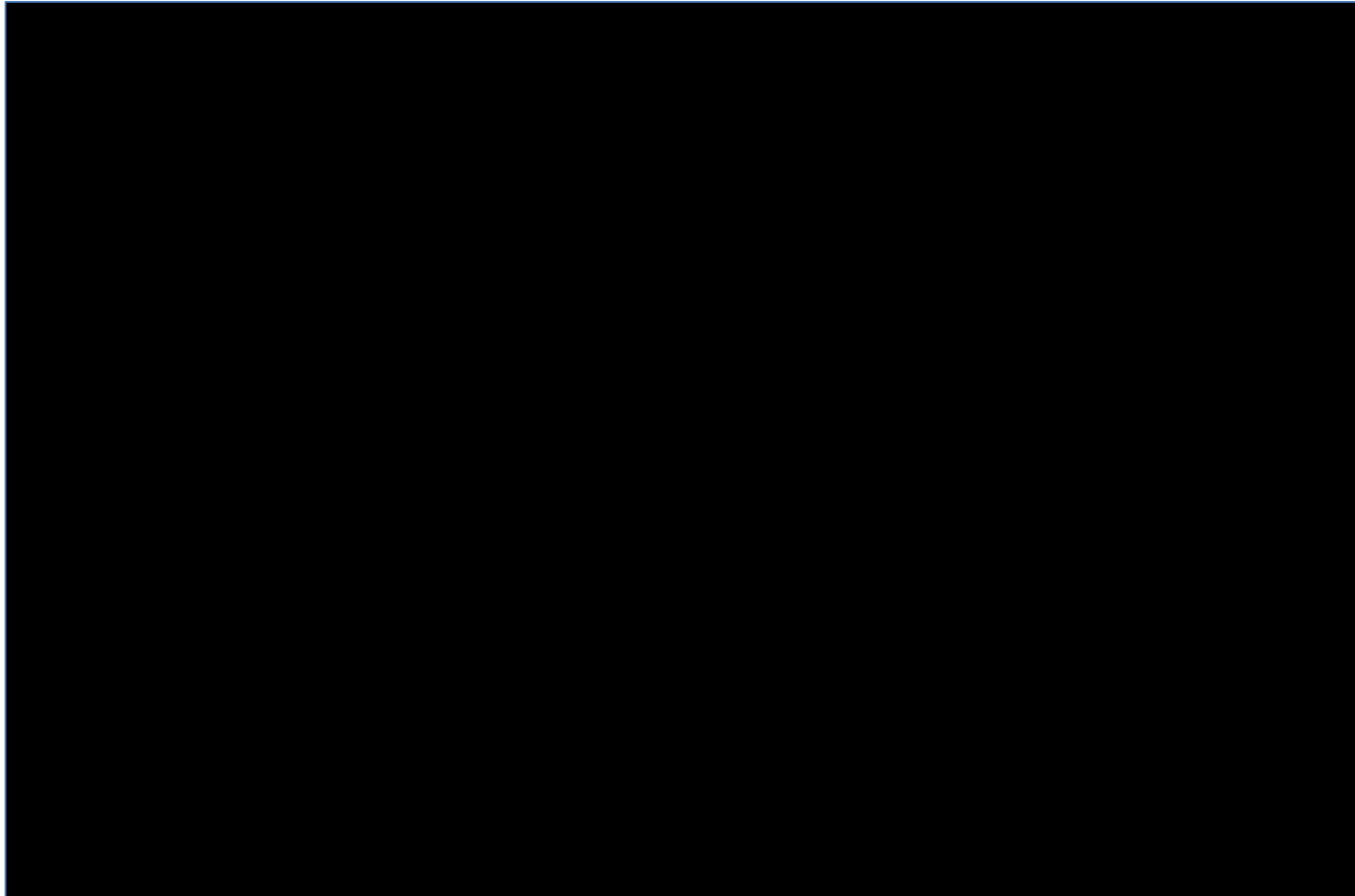


Trust in, and value from, information systems

San Francisco Chapter

The "CyberSizelT" logo is rendered in a large, stylized font with a red-to-brown gradient and a white outline. The background of the slide features a silhouette of the San Francisco skyline, including the Golden Gate Bridge and various skyscrapers, set against a warm, yellowish-orange sky.

Don't be a... (video)



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

Passwords



Password1?



$\$m = gC + M \& cH$



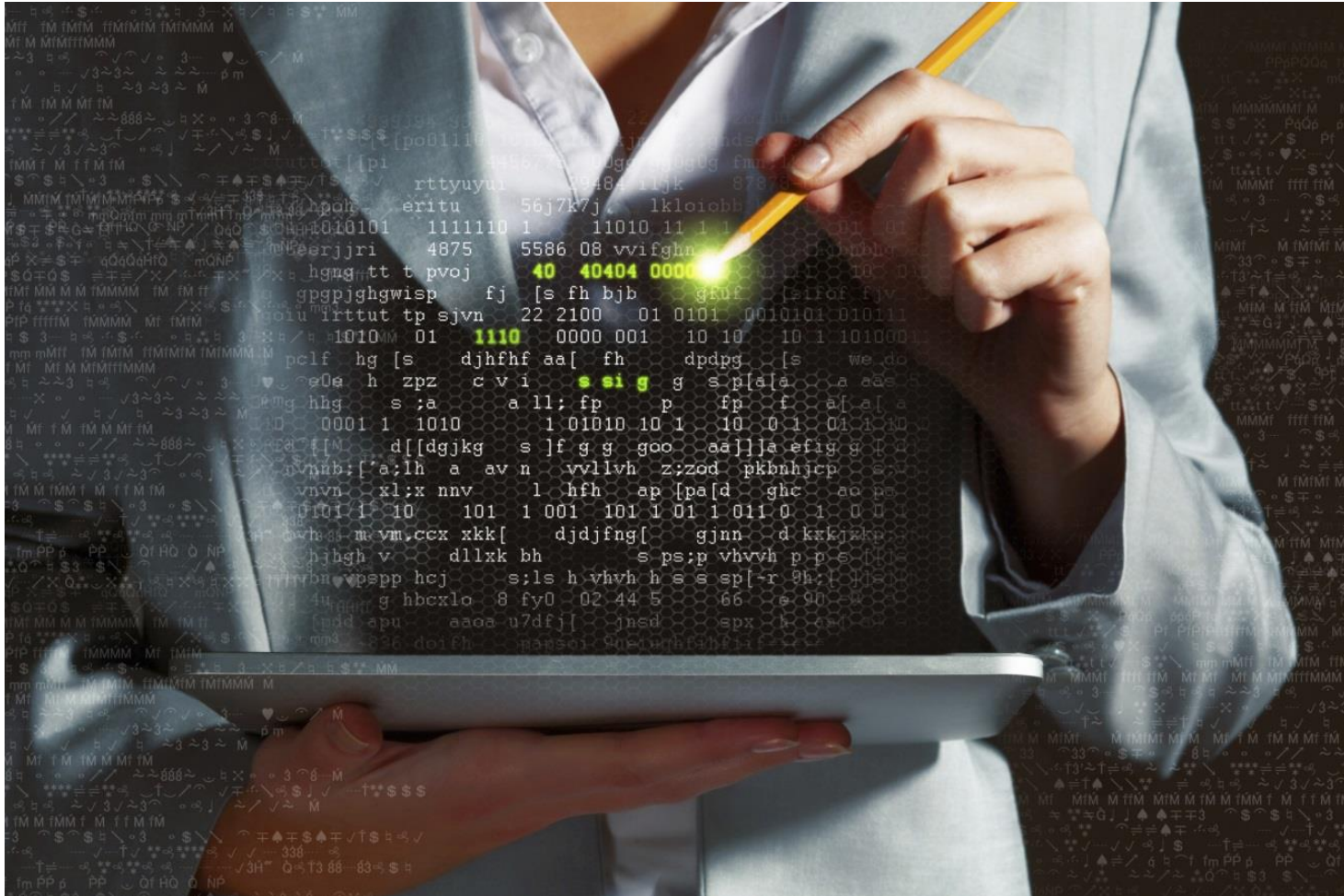
Passwords – additional controls



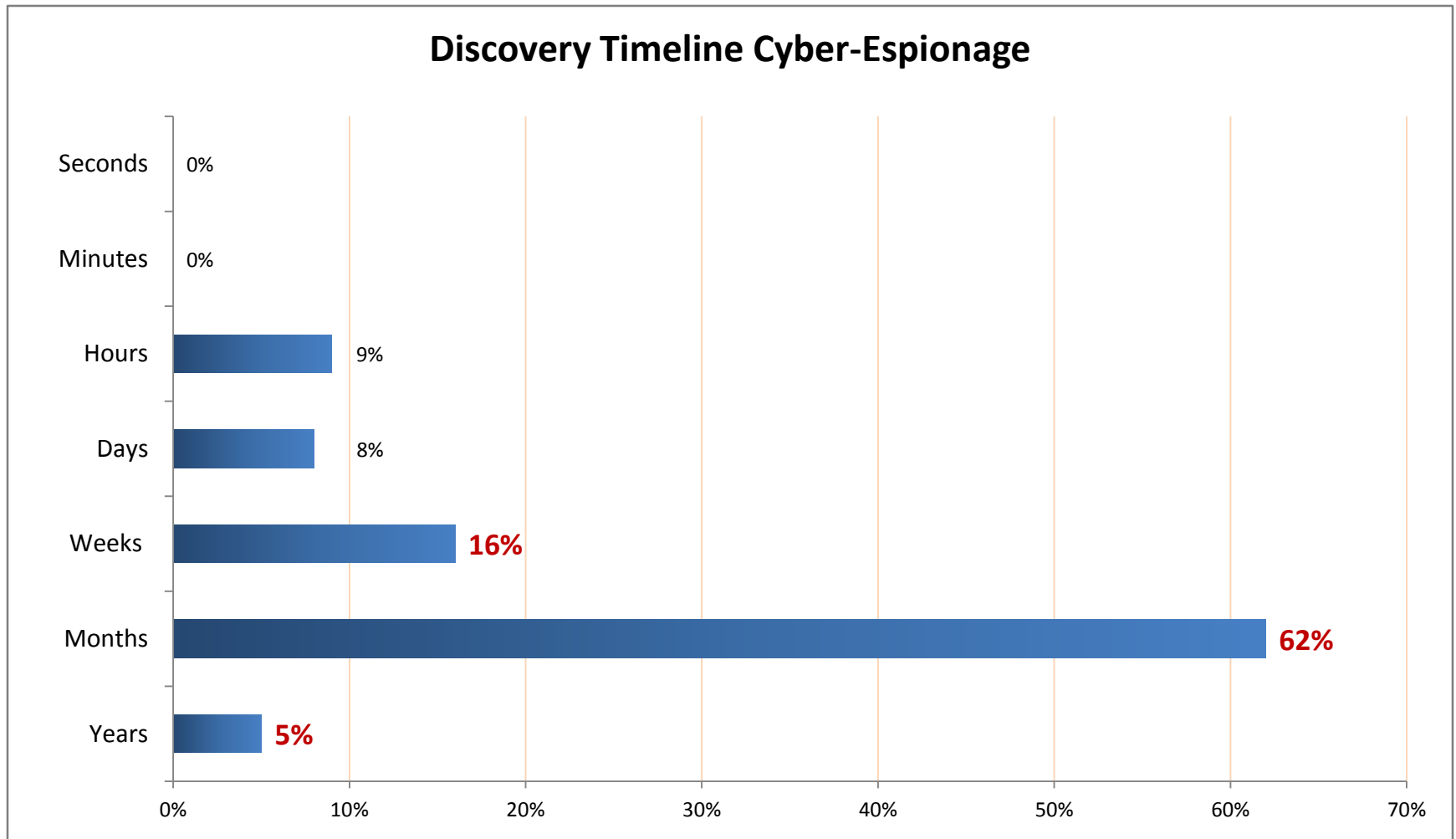
Social Engineering



Published Vulnerabilities



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

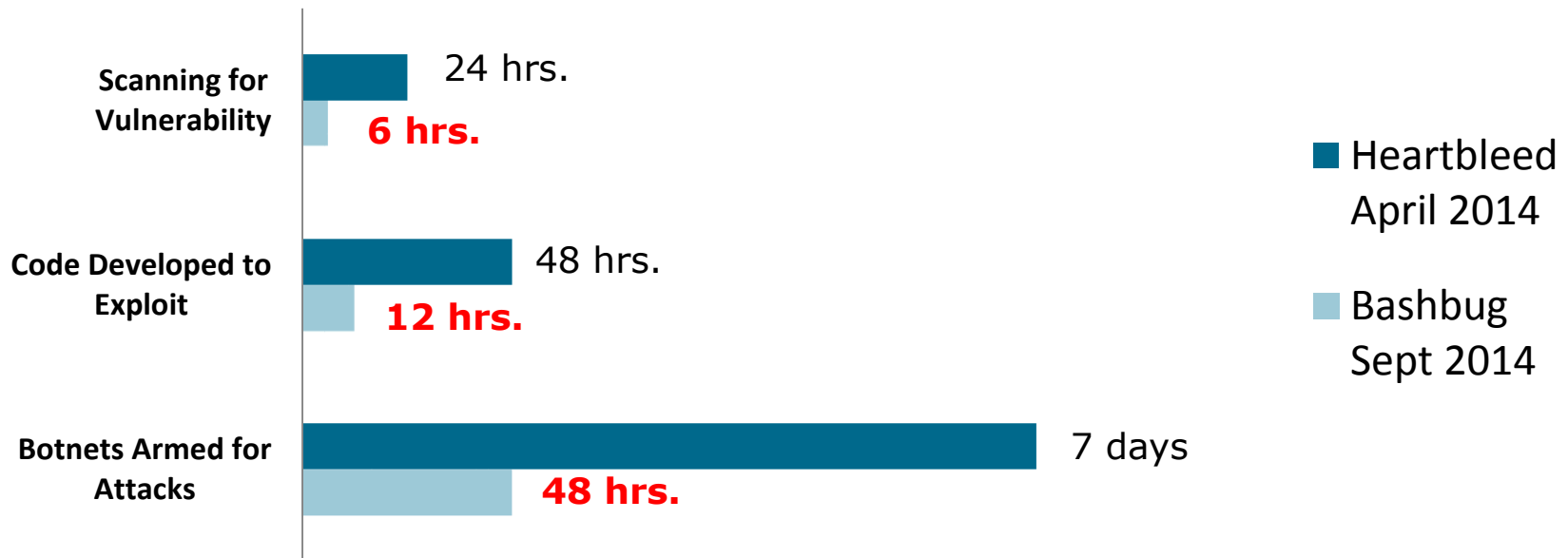


Zero-Day Vulnerabilities



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.

Avoid

Mitigate

Accept

Transfer



Conclusion



QUESTIONS? COMMENTS?

CONTACT INFORMATION:

ERIC KURNIE

(650) 773-0044

KURNIE@WELLSFARGO.COM



Trust in, and value from, information systems

San Francisco Chapter

The "CyberSizelT" logo is set against a background illustration of the San Francisco skyline, including the Golden Gate Bridge and various skyscrapers. The word "CyberSizelT" is written in a large, stylized font where the letters are filled with a red-to-orange gradient and have a white outline. The "T" is notably larger than the other letters.

CyberSizelT