Security in knowledge

ACTIONABLE INTELLIGENCE FOR THE ENTERPRISE

Cary E. Moore CISSP, CFE, EnCE

SVP, Emerging Threats Manager
Bank of America

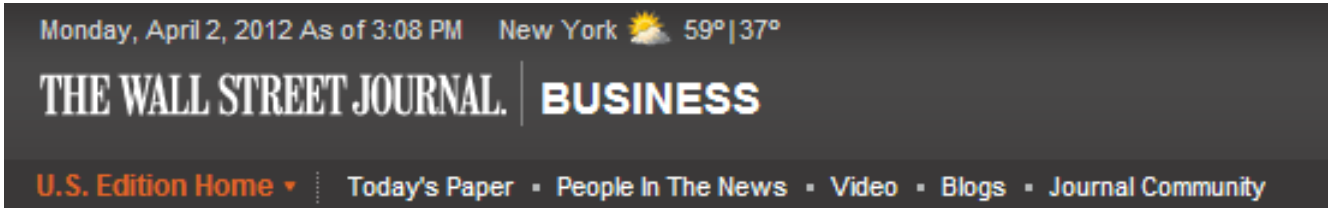
RSA CONFERENCE 2013

Session ID: END-R3

Session Classification: General Interest

Scenario

- 1.5 Million Account numbers stolen…
  - Global Payments Inc



Monday, April 2, 2012 As of 3:08 PM New York 59°|37°

THE WALL STREET JOURNAL. | BUSINESS

U.S. Edition Home ▾ | Today's Paper ▪ People In The News ▪ Video ▪ Blogs ▪ Journal Community

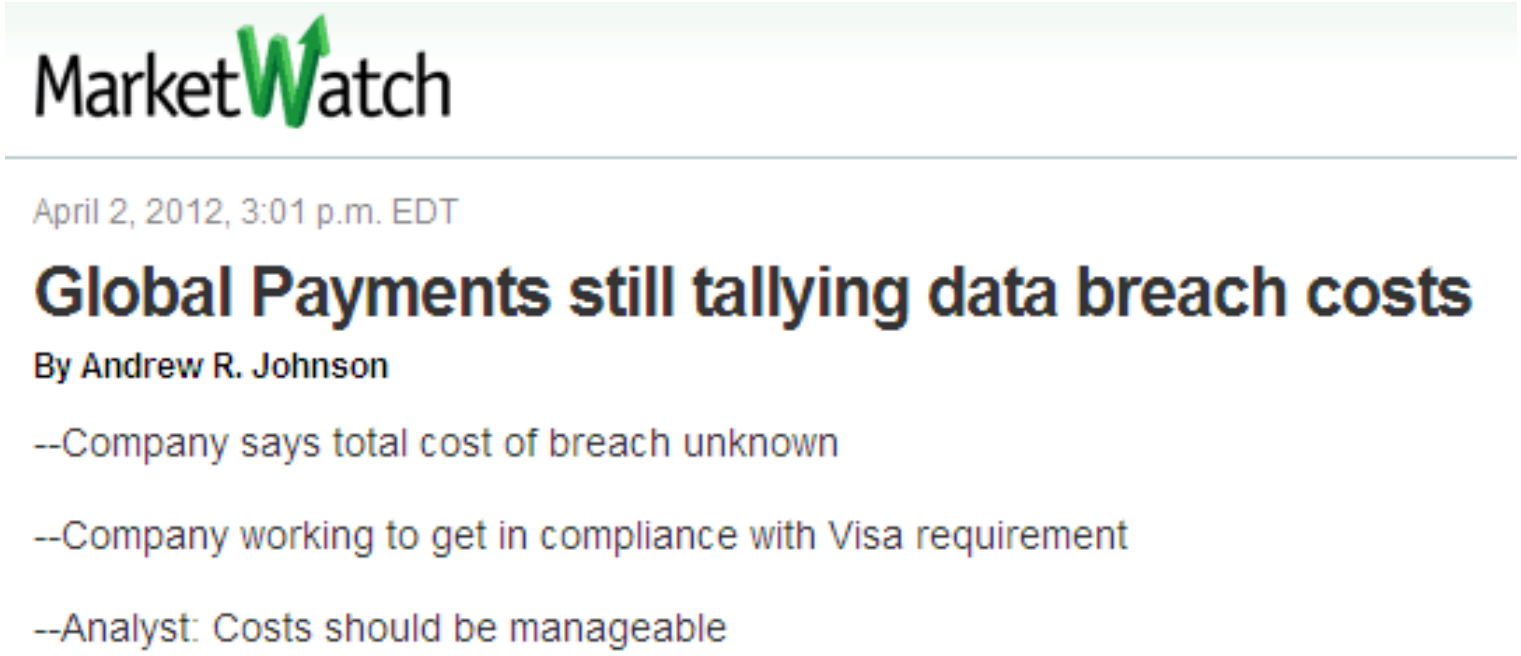
BUSINESS | Updated April 2, 2012, 4:08 p.m. ET

Card Processor: Hackers Stole Account Numbers

BY ROBIN SIDEL

Global Payments Inc., the credit-card processor that reported a significant security breach Friday, said that hackers stole account numbers and other key information from up to 1.5 million accounts in North America.

Scenario



MarketWatch

April 2, 2012, 3:01 p.m. EDT

Global Payments still tallying data breach costs

By Andrew R. Johnson

--Company says total cost of breach unknown

--Company working to get in compliance with Visa requirement

--Analyst: Costs should be manageable

- Greg Smith, an analyst with Sterne Agee, said he expects expenses stemming from the breach to be in the **"tens-of-millions of dollars."**

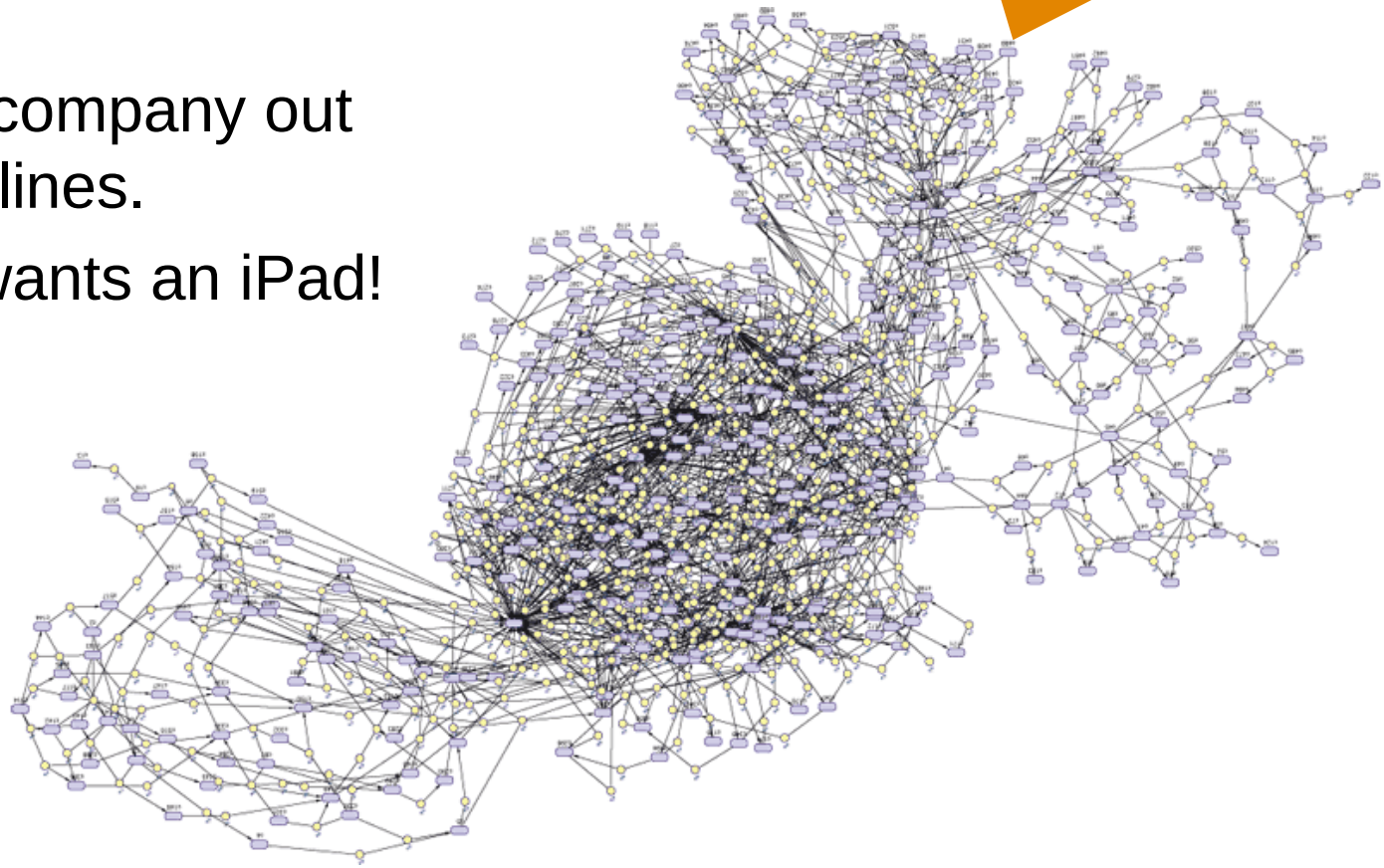
Scenario

- What's the total cost?
  - Global Payments' shares sank more than **9% to $47.50** midday Friday before the stock was halted for the rest of the day.
  - Heartland expensed about **$147.1 million** in costs related to its breach, including about **$110 million for settlements** with Visa and MasterCard, according to analysts.
  - TJX Cos. (TJX), which disclosed a breach in 2007 that involved 40 million to 90 million card accounts, incurred **$256 million** in costs…

Your Goals

- Secure Everything
- BYOD
- System Migrations
- IPV6
- Keep your company out of the headlines.
- Everyone wants an iPad!

You Are Here



The Attacker's Goals

Find the weakest link…

http://blogs.technet.com/b/rhalbheer/archive/2011/01/14/real-physical-security.aspx

Takeaways

- Understand Emerging Threat Management
- New ways to Identify Threats
- Link Threats Back to the Environment
- Evaluate Mitigation Controls
- Assess Overall Risk
- Real World Examples

Emerging Threat Management

- Cyber or physical threats that are **not yet generally recognized and expected to or may affect** the integrity and normal operation of a business process, customer experience and/or sensitive customer information.

- The threat may also affect an initiative or a current business process if the process changes without proper adjustments to controls.

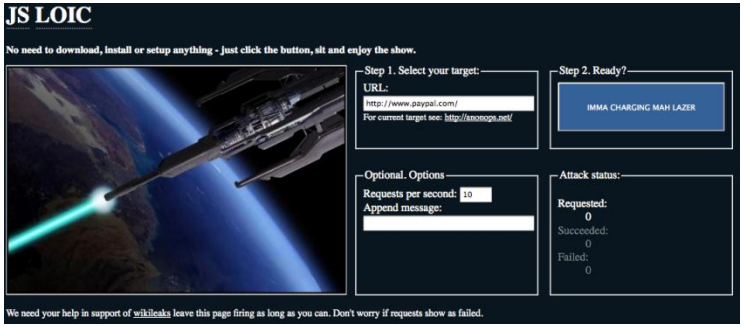
Emerging Threat Management

- Charter
  - **Provide early warning** on threats to the business or customers from a holistic perspective **to drive change** and provide catalyst to create response plans for imminent threats.

- Function
  - Threat Intelligence Process

Identify Threats

Identify Threats



Actionable Intelligence

- What is Actionable Intelligence?

IP Address

File Signature

Credit Card Number

File Hash value

These are considered tactical.

Actionable Intelligence

- What is Actionable Intelligence?
- Strategic Intelligence can include:
  - New Technologies
  - Consumerism
  - Trends and Analytics
  - Government Policy
  - New Fraud Techniques

Threat Intelligence Board

Top 5 Current Threats

Threat Name	High-Level Classification	Impact	Likeliness	Detection	Overall Rating	Trend	Quick Threat Summary
Malware	Endpoint Security	High	High	Low	Critical	Up	This includes Malware on the customer's system and the internal bank information assets.
Application Security	Application Security	High	Moderate	Low	Critical	Flat	A risk of abuse or penetration at the code or application layer as a result of a design or development flaw; which can be used to gain customer data or direct the customer into a non-BAC website.
Phishing Attacks	Customer Spoofing	High	High	Moderate	Critical	Flat	The act of a fraudster sending an email or other communication to a customer falsely claiming to be Bank of America in an attempt to scam the customer into providing information that can be used for identity theft.
Mobile Malware	Endpoint Security	High	Moderate	Low	Critical	Up	The ikee and Duh iPhone worms (and variants) target "jailbroken" iPhones by using the default remote administration password to connect to the iPhone and spread to other iPhones. This would affect customers using mobile banking via the iPhone.
ATM Skimming	Infrastructure Compromise	Moderate	Moderate	Low	MODERATE	Up	Skimming is the processes of collecting a copy of credit or debt card information throught the use of a magnetic stripe reader.

1 - 5

Emerging Threats

High-Level Classification	Threat Name	Impact	Likeliness	Trend	Horizon
Infrastructure Compromise	Compromise of 3DES Encryption	High	Low	Up	Near (>1 yr < 2yr)
Infrastructure Compromise	Electromagnetic Interception of Keyboard or ATM Keypad Entries	High	Low	Flat	Distant (> 2 Years)
Endpoint Security	Malicious Code on ATMs	High	Low	Flat	Distant (> 2 Years)

Threat Intelligence Committee

Full Name	Organization

FS-ISAC

FS ISAC Alert Level

FS ISAC Alert Level

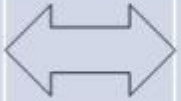
MS-ISAC Cyber Alert Level:

GUARDED

ISS AlertCon

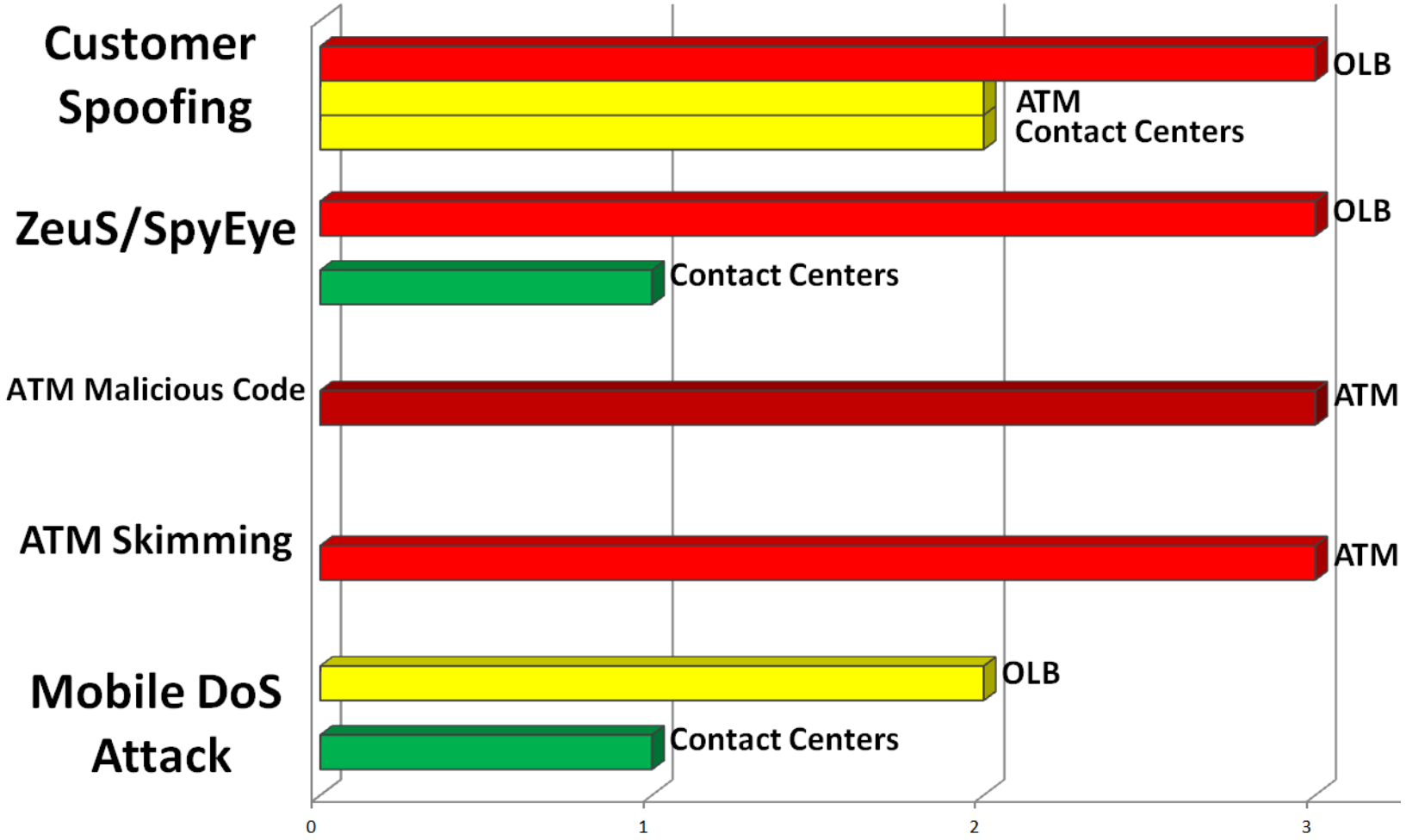
National Alert Status

Threat Intelligence Board

Name	Threat	Impact	Likelihood	Risk	Horizon	Trend	Action
Customer Spoofing					Current		Critical
ZeuS v.1.3.4 Variant					Near (>1 < 2yr)		Important
ATM Malicious Code					Distant (> 2 Yrs)		Important
ATM Skimming					Current		Important
Mobile DoS Attack					Near (>1 < 2yr)		None

Threat Intelligence Board

- Linking threats back to the environment:



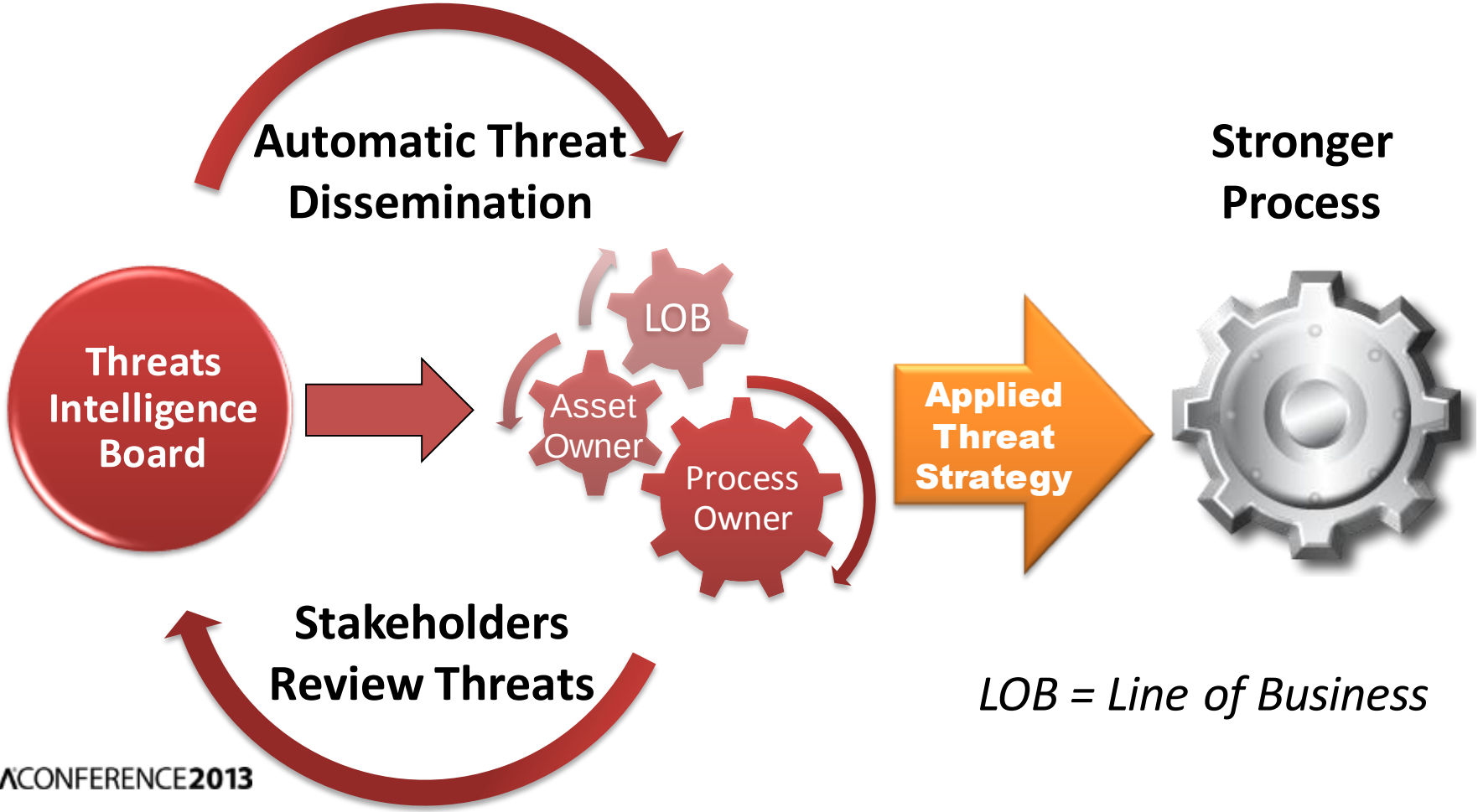
Threat Intelligence Board

- Linking threats back to the environment:

Project	Owner	Status
Authentication Enhancements P31027 173812 OSE	Bob Smith	Analyze June 2011
Device Fingerprinting P34445 186474	Mike Johnson	Measure 2011
Phishing Mitigation P31900 177331	Nicole Jones	Control Email Authentication

Threat Intelligence Board

- Linking threats back to the environment:
- The Communication Process



LOB = Line of Business

Real World Examples

- Phishing via QR-Codes!

Using the Address Bar Spoofing on an iPhone.

Sticker by the Fraudster

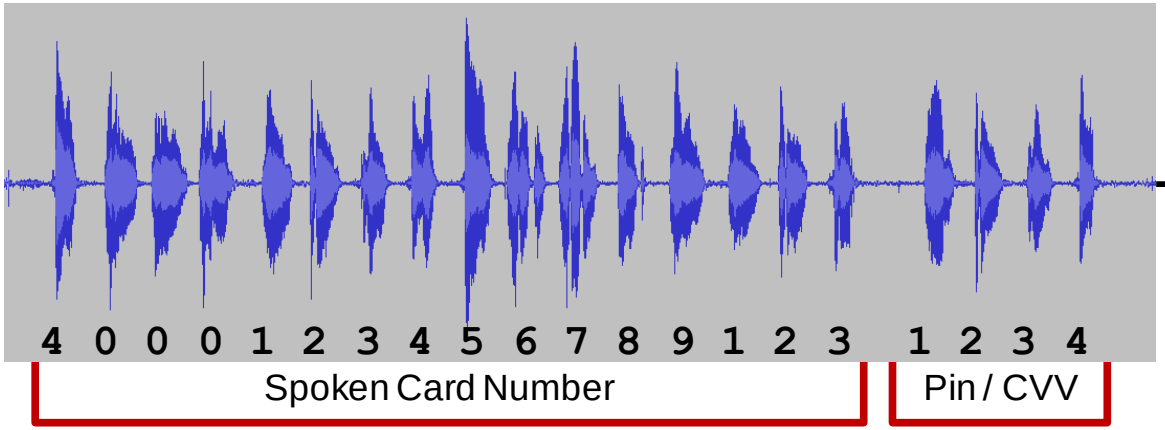
References: http://www.dhanjani.com/blog/2010/11/ui-spoofing-safari-on-the-iphone-.html

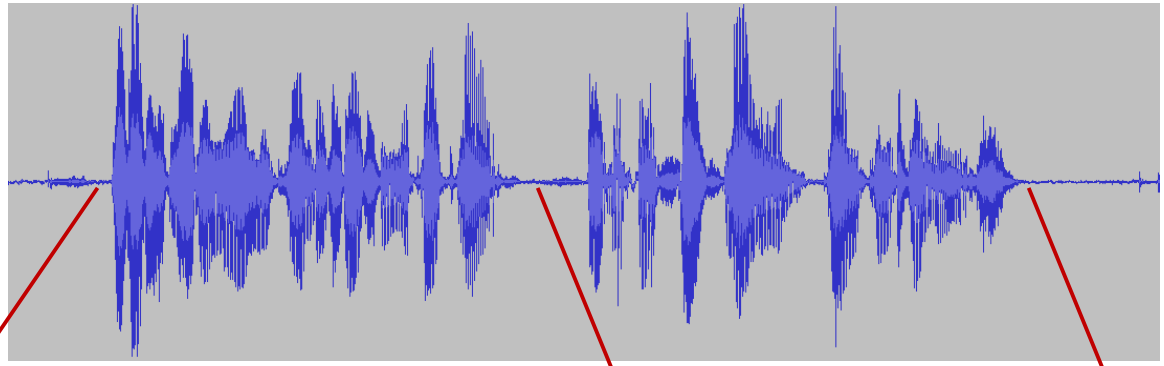
Real World Examples

- Phishing via QR-Codes!
  - Sign into “mobile banking”
  - Open a new account
  - Instant Credit Approval Offer!

Real World Examples

- Soundminer: The first sensory malware
  - Trigger > 1-800-732-9194 > BofA Credit Card Customer Service





This is what a normal speech pattern looks like.

It will flow and be consistent.

SMS Text

To: Fraudster
4000123456789123 1234

References: http://www.cs.indiana.edu/~kapadia/papers/soundminer-ndss11.pdf

Real World Examples

- Phishing via NFC Tags!
  - Not only a new phishing attack vector, but a whole new way to attack the phone.

  - Settings & Applications
    - Change phone settings (Bluetooth®, Wi-Fi, ringer/media volume, screen brightness, etc.)
    - Launch an application
    - Join a Wi-Fi Network
    - Show a message
  - Communication
    - Make a call
    - Send a text message
    - Share a contact or business card

References: http://www.samsung.com/us/microsite/tectile/

Real World Examples

- Phishing via NFC Tags!
  - Location & Web
    - Show an address on a map
    - Foursquare or Facebook check-in
    - Open a web page < No User Interaction!
  - Social (Fun ways to ruin someone's life…)
    - Post a tweet or follow a contact on Twitter
    - Automatic Facebook "Like"
    - Update Facebook status
    - Connect on LinkedIn

References: http://www.samsung.com/us/microsite/tectile/

Real World Examples

- The evolution of mobile banking.

Reference: http://framework.latimes.com/2012/08/13/mobile-banking-in-1967/

Real World Examples

- The new endpoint
  - Mobile

Real World Examples

- The new endpoint
  - Portables
    - Mac App Store
    - Google App Store
    - Windows App Store

Cloud Centric
Operating Systems
Windows 8
Google OS

Real World Examples

- The new endpoint
  - Hybrid Devices
    - Internet TV
    - Internet Connected Devices
    - Smart Home Devices
    - Portable (Dashboard) Devices

Reference: http://www.engadget.com/photos/samsung-wi-fi-enabled-rf4289-fridge/
http://www.engadget.com/2010/05/01/sony-dash-review/

Takeaways

- Understand Emerging Threat Management
- New ways to Identify Threats
- Link Threats Back to the Environment
- Evaluate Mitigation Controls
- Assess Overall Risk
- Real World Examples

Questions?

Cary E. Moore CISSP, CFE, EnCE
SVP, Emerging Threats Manager
Bank of America

Contact info vCard
Yes, Really…

Security in knowledge