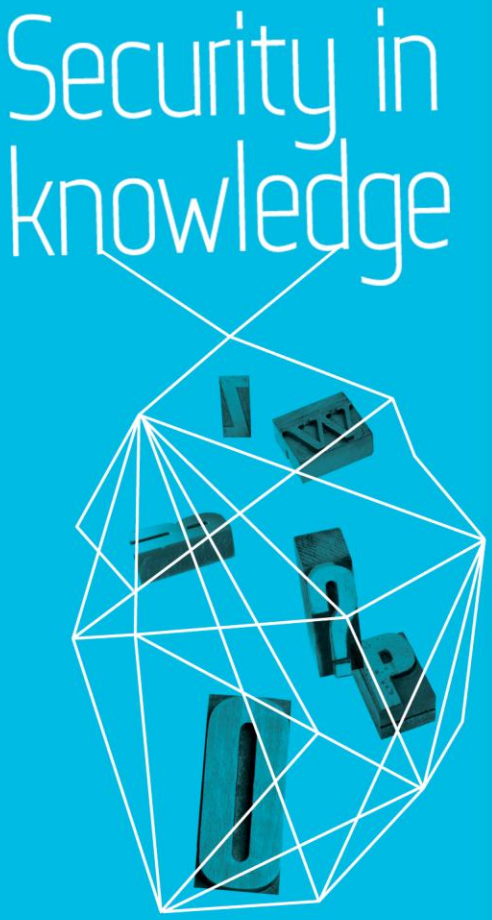
THE CYBER THREAT LANDSCAPE: NEW THEMES IN PREVENTION, DETECTION, RESPONSE



Kimberly Peretti
Partner, Alston & Bird, LLP

Session ID: STU-W22B
Session Classification: Intermediate

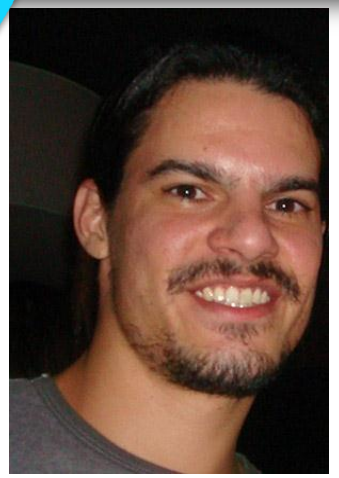
AGENDA

- Cyber Threat Landscape
  - Lessons learned
- New Themes
  - Response
  - Detect
  - Protect
- Take-aways

THREAT LANDSCAPE

… the constant electronic theft … that has silently occurred over the past several years h… **harm to our national and economic security**. Hacker… orporate network imaginable — from defer… important security information to business … trade secrets. Cybercriminals are steal… , source code, negotiation plans, desig… Sen. Jay Rockefeller and Michael Chertoff, in … ance

Cyber Warfare



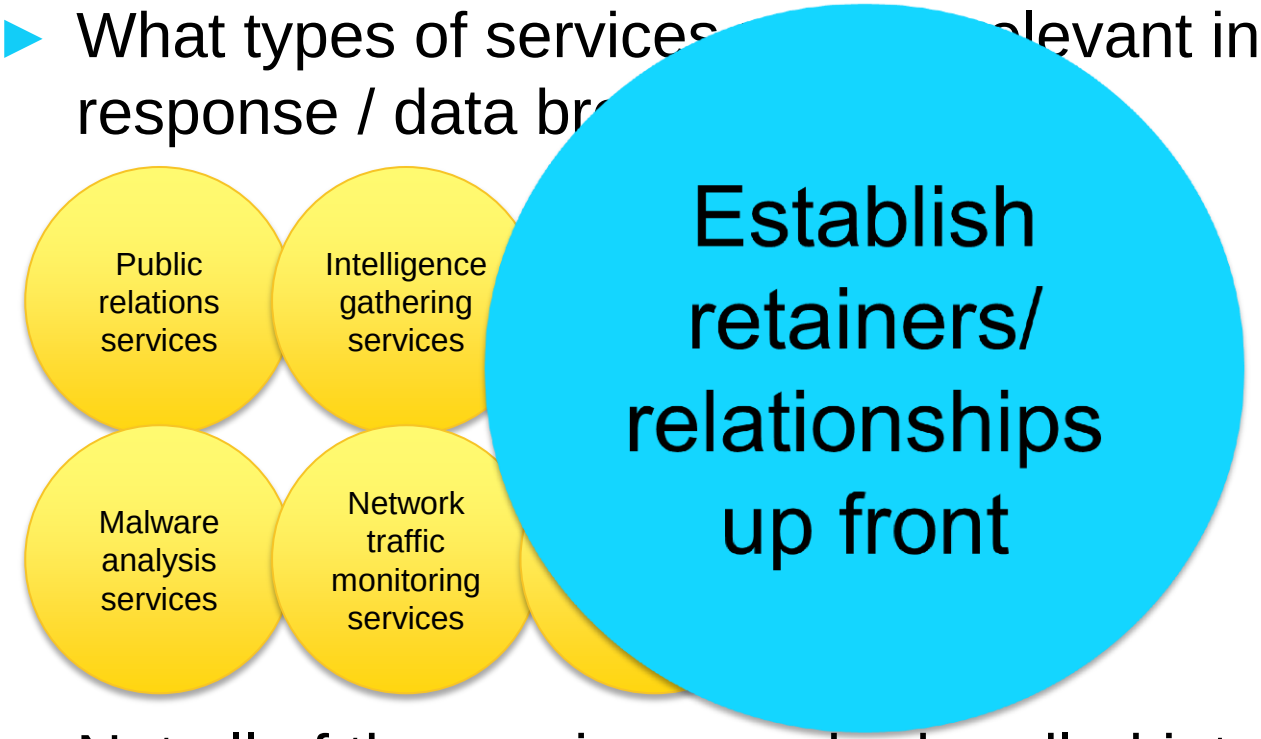
RESPONSE – NEW THEMES

ENTERPRISE IMPACT INVESTIGATIONS

- Three common breach response scenarios
- Hallmarks of enterprise impact investigations
- Are enterprise impact investigations necessary? And, when?

CRISIS MANAGEMENT

- What types of services … levant in a cyber response / data br…



- Not all of the services can be handled internally or even with one vendor

ACTIVE DEFENSE

- Active defense vs. hacking back
- Current legal landscape
  - The CFAA
  - The ongoing debate
- New technologies and creative solutions
  - Some, clearly legal
  - Some in gray area

http://www.alstonprivacy.com/?entry=4793

http://articles.latimes.com/2012/dec/04/business/la-fi-cyber-defense-20121204

DETECT

PREVENTATIVE FORENSICS

- Periodic scanning for breach indicators
  - Key systems
  - Assortment of endpoints
  - Updated list of indicators
- Component of cyber risk assessment

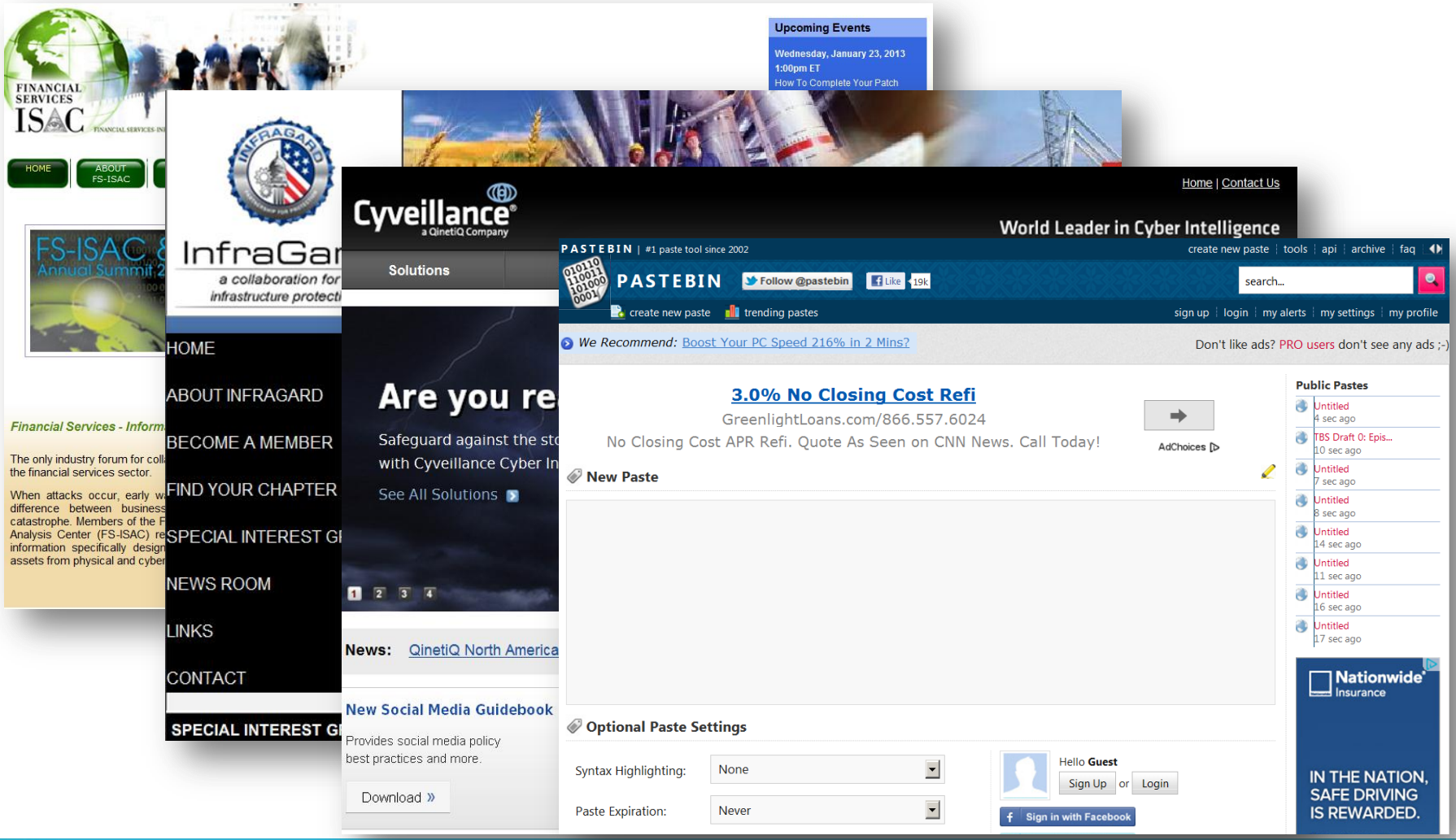
BIG DATA FORENSICS

Training big data's eye on cybersecurity threats

Summary: *The data explosion is upon us. Big data analytics is supposed to help us sift through it all. Can it also help keep enterprise hackers at bay? We talk to the founders of Seculert.*

PROTECT

THREAT INTELLIGENCE



THREAT MODELING / ASSESSMENT

- Threat models/assessment
  - Understanding current defenses in place to protect against most likely threat vectors
  - Should be part of cyber risk assessment

FINAL THOUGHTS / LESSONS LEARNED

5 TIPS TO TAKE HOME

- Invest in information sharing
  - Real-time mechanisms are the key to threat intelligence
- Don’t get caught in trap of narrowly-tailored investigations
  - The sooner you uncover the scope, the better
- Use Big Data concepts to manage investigations
  - The technology is there, use it
- Explore creative solutions in active defense space
  - But this is especially an area to include counsel
- Hail to the Board
  - Board involvement necessary in protect, detect, and respond

QUESTIONS?

Kimberly.peretti@alston.com
202.251.8118

For additional information, please see:
www.alstonprivacy.com
www.alstoncyber.com
www.alstonsecurity.com