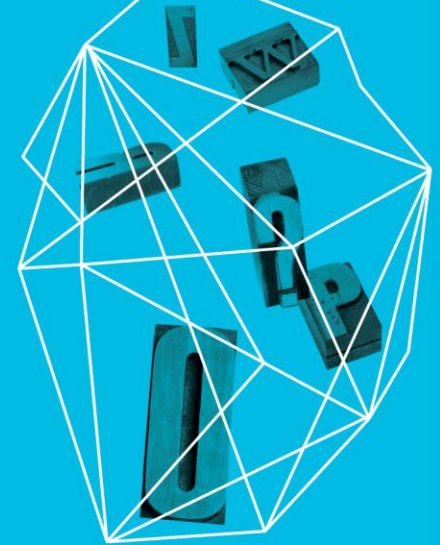


## THE CYBER THREAT LANDSCAPE: NEW THEMES IN PREVENTION, DETECTION, RESPONSE

Kimberly Peretti  
Partner, Alston & Bird, LLP

Security in  
knowledge



# — AGENDA

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

# THREAT LANDSCAPE





... the constant electronic theft of information that has silently occurred over the past several years has caused **harm to our national and economic security.** Hackers have infiltrated corporate network information — from defense-related data to important security information to business records — and stolen trade secrets. Cybercriminals are stealing sensitive information, source code, negotiation plans, design documents, and other confidential data. Sen. Jay Rockefeller and Michael Chertoff, in a report to the Intelligence Committee

# Cyber Warfare



# RESPONSE – NEW THEMES



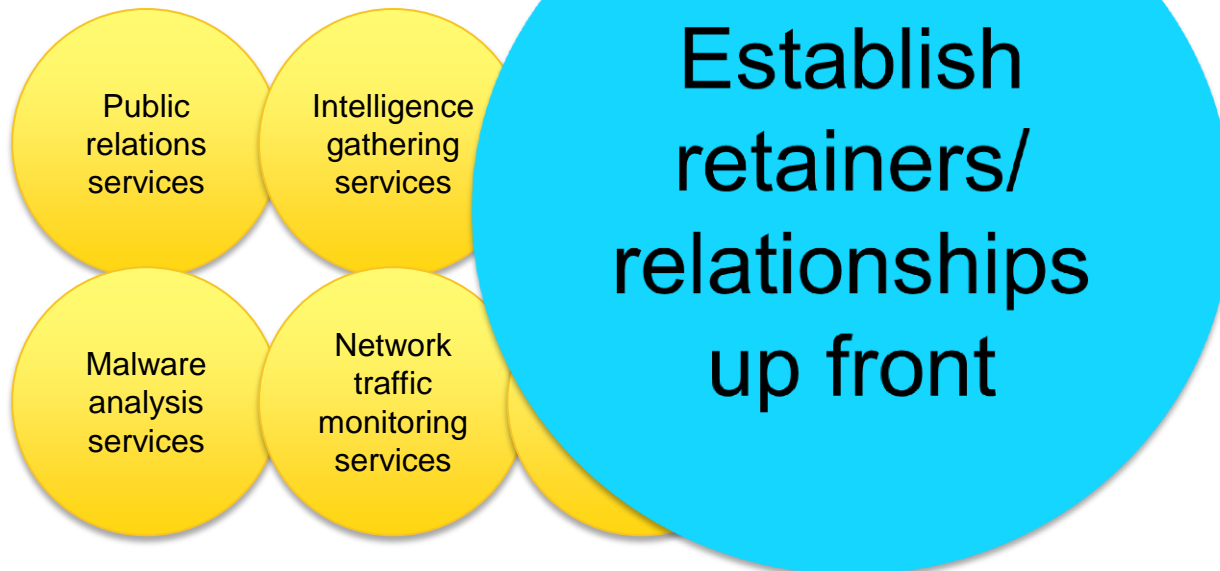
# ENTERPRISE IMPACT INVESTIGATIONS

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



# CRISIS MANAGEMENT

- ▶ What types of services are relevant in a cyber response / data breach?



- ▶ 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

**Upcoming Events**  
Wednesday, January 23, 2013  
1:00pm ET  
How To Complete Your Patch

**FINANCIAL SERVICES ISAC**  
HOME ABOUT FS-ISAC

**FS-ISAC 8th Annual Summit 2013**

**InfraGard**  
a collaboration for infrastructure protection

**Cyveillance**  
a QinetiQ Company  
World Leader in Cyber Intelligence  
Home | Contact Us

**PASTEBIN** | #1 paste tool since 2002  
create new paste | tools | api | archive | faq | search...  
Follow @pastebin Like 19k  
create new paste trending pastes sign up | login | my alerts | my settings | my profile

**We Recommend: Boost Your PC Speed 216% in 2 Mins?**  
Don't like ads? PRO users don't see any ads ;-)

**3.0% No Closing Cost Refi**  
GreenlightLoans.com/866.557.6024  
No Closing Cost APR Refi. Quote As Seen on CNN News. Call Today!

**Public Pastes**

- Untitled 4 sec ago
- TBS Draft 0: Epis... 10 sec ago
- Untitled 7 sec ago
- Untitled 8 sec ago
- Untitled 14 sec ago
- Untitled 11 sec ago
- Untitled 16 sec ago
- Untitled 17 sec ago

**Optional Paste Settings**

Syntax Highlighting: None  
Paste Expiration: Never

Hello Guest  
Sign Up or Login  
Sign in with Facebook

**New Social Media Guidebook**  
Provides social media policy best practices and more.  
Download »

**Nationwide Insurance**  
IN THE NATION, SAFE DRIVING IS REWARDED.

# — 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](http://www.alstonprivacy.com)  
[www.alstoncyber.com](http://www.alstoncyber.com)  
[www.alstonsecurity.com](http://www.alstonsecurity.com)

