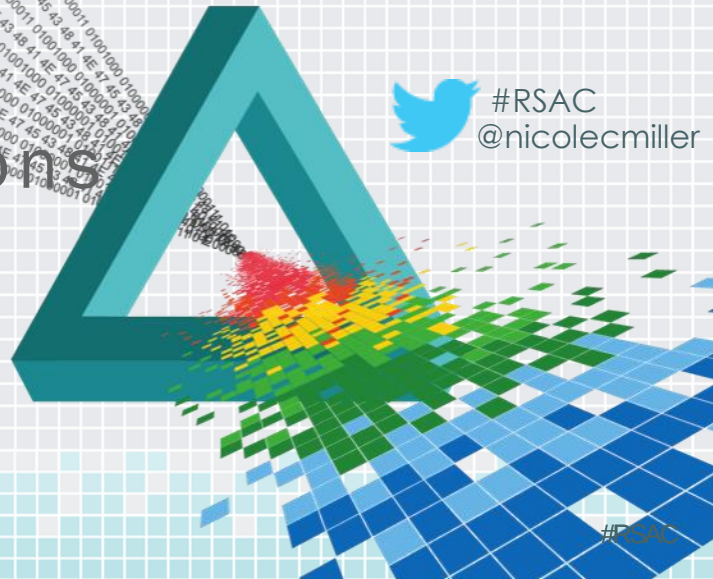
RSAConference2015

San Francisco | April 20-24 | Moscone Center

From the Battlefield:
Managing Customer Perceptions in a Security Crisis

Nicole Miller, SVP

WAGGENER EDSTROM COMMUNICATIONS



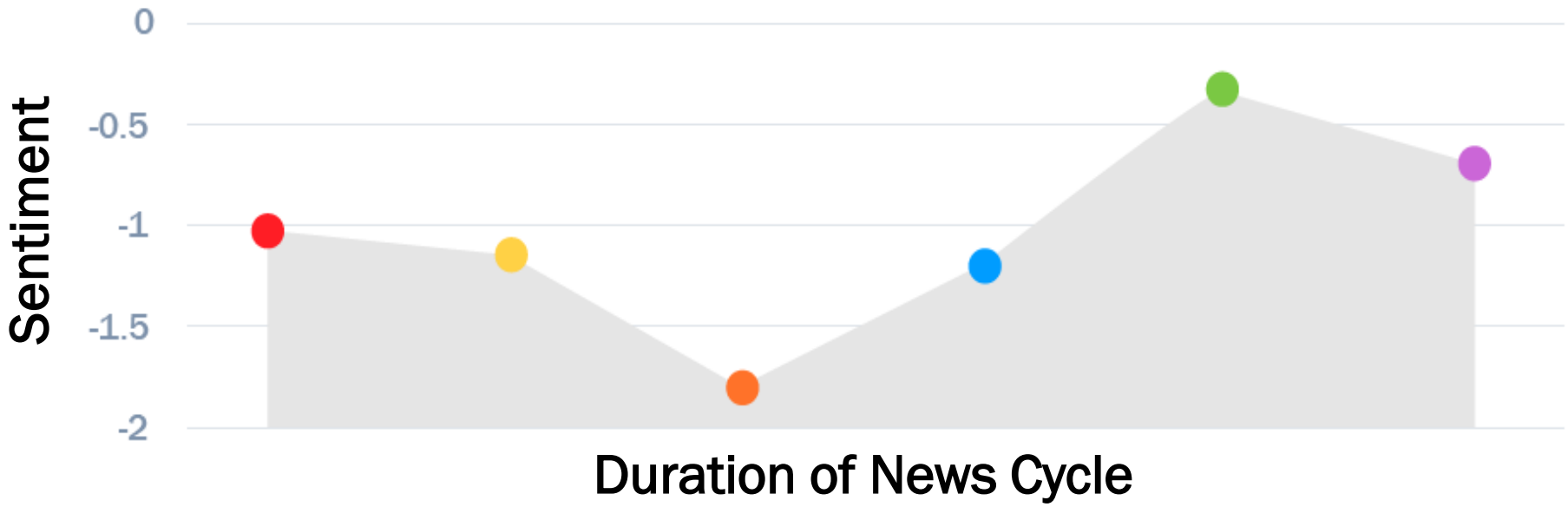
#RSAC
@nicolecmiller

GOOD to KNOW

- Cybersecurity news follows a pattern
- Showing up to the party improves coverage
- You need to speak up to counteract other voices
- Closure is the strongest part of your story

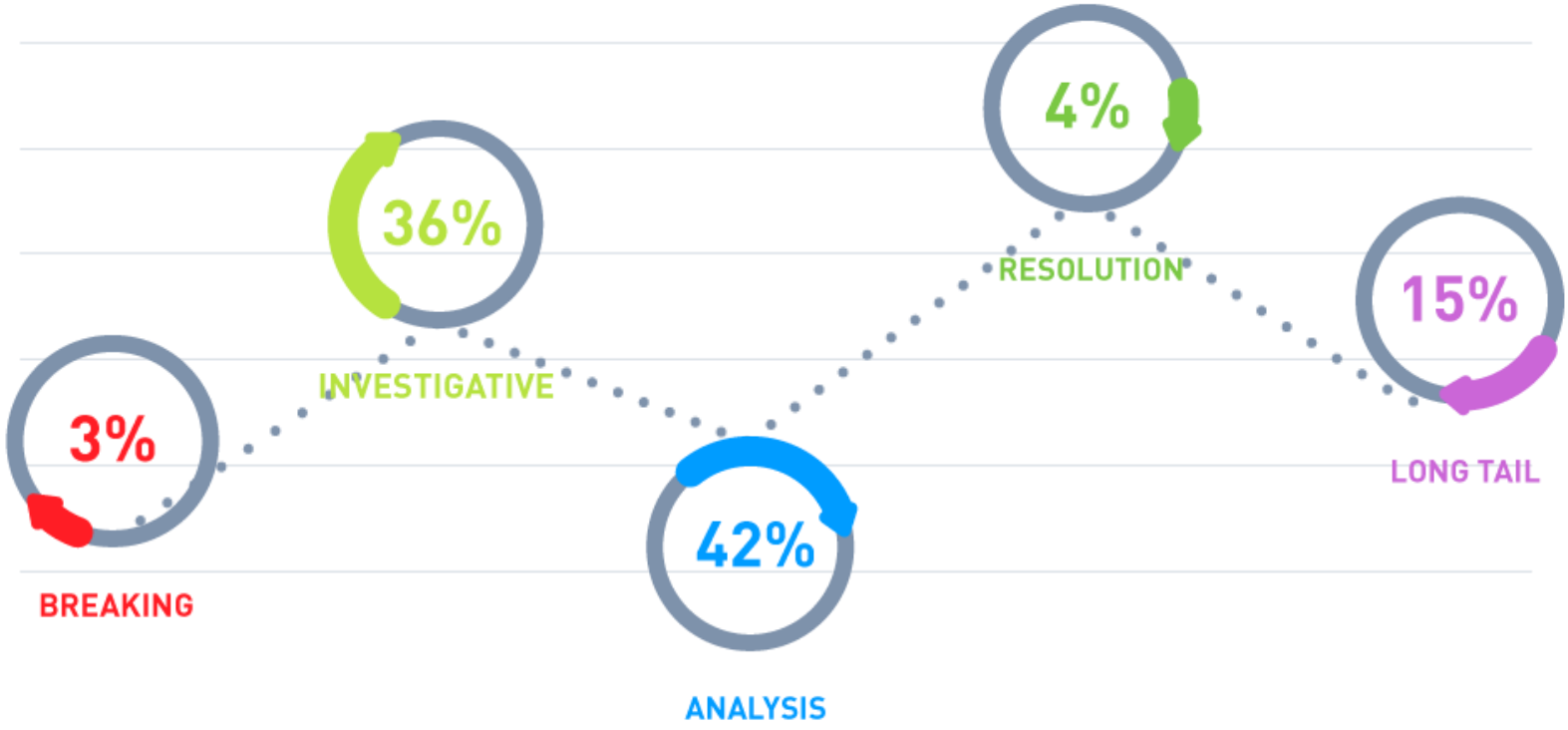
Another Flash Patch Released
Server for Malware
Microsoft Fixes Dangerous
Yet Another Flash Zero-Day
Yet Another Flash Zero-Day Used in APT Attacks
Yet Another Flash Zero-Day Used in Cyber Weapon
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware Attacks
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware Attacks Vulnerability
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware Attacks Vulnerability Found
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware Attacks Vulnerability Found in
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware Attacks Vulnerability Found in Android
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware Attacks Vulnerability Found in Android Phones
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware Attacks Vulnerability Found in Android Phones Fueled
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware Attacks Vulnerability Found in Android Phones Fueled Bank
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware Attacks Vulnerability Found in Android Phones Fueled Bank Hackers
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware Attacks Vulnerability Found in Android Phones Fueled Bank Hackers Steal
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware Attacks Vulnerability Found in Android Phones Fueled Bank Hackers Steal Millions
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware Attacks Vulnerability Found in Android Phones Fueled Bank Hackers Steal Millions From
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware Attacks Vulnerability Found in Android Phones Fueled Bank Hackers Steal Millions From Target
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware Attacks Vulnerability Found in Android Phones Fueled Bank Hackers Steal Millions From Target Banks
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware Attacks Vulnerability Found in Android Phones Fueled Bank Hackers Steal Millions From Target Banks in
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware Attacks Vulnerability Found in Android Phones Fueled Bank Hackers Steal Millions From Target Banks in XSS
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware Attacks Vulnerability Found in Android Phones Fueled Bank Hackers Steal Millions From Target Banks in XSS Vulnerability
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware Attacks Vulnerability Found in Android Phones Fueled Bank Hackers Steal Millions From Target Banks in XSS Vulnerability Found
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware Attacks Vulnerability Found in Android Phones Fueled Bank Hackers Steal Millions From Target Banks in XSS Vulnerability Found in
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware Attacks Vulnerability Found in Android Phones Fueled Bank Hackers Steal Millions From Target Banks in XSS Vulnerability Found in Another
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware Attacks Vulnerability Found in Android Phones Fueled Bank Hackers Steal Millions From Target Banks in XSS Vulnerability Found in Another Flash
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware Attacks Vulnerability Found in Android Phones Fueled Bank Hackers Steal Millions From Target Banks in XSS Vulnerability Found in Another Flash Patch
Yet Another Flash Zero-Day Used in Cyber Weapon with ISIS Backing Website Found Hacking Devices Connected MacBooks with Perfect Malware Attacks Vulnerability Found in Android Phones Fueled Bank Hackers Steal Millions From Target Banks in XSS Vulnerability Found in Another Flash Patch Released

SHARED 315 TIMES


Sentiment
0
-0.5
-1
-1.5
-2
Duration of News Cycle

TECHNOLOGY
BUSINESS
CONSUMER
POLICY
InformationWeek DARKReading
WIRED
KrebsonSecurity
THE VERGE
cnet
Mashable
FINANCIAL TIMES
THE WALL STREET JOURNAL
The New York Times
FAST COMPANY
REUTERS
Bloomberg Business
CNBC
theguardian
USA TODAY
Los Angeles Times
BuzzFeed
NBC NEWS
ConsumerReports
The Seattle Times
The Washington Post
THE POLITICO
THE HILL
NationalJournal
ROLL CALL

Sentiment


3%
BREAKING
36%
INVESTIGATIVE
42%
ANALYSIS
4%
RESOLUTION
15%
LONG TAIL

theguardian
Winner of the Pulitzer prize 2014

US national security
Glenn Greenwald on security and liberty

NSA Prism program taps in to user data of Apple, Google and others

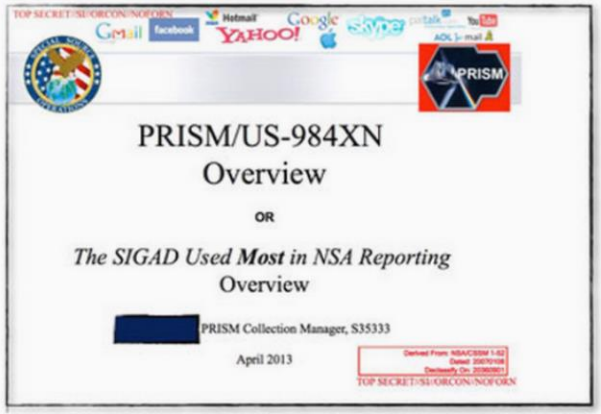
- Top-secret Prism program claims direct access to servers of firms including Google, Apple and Facebook
- Companies deny any knowledge of program in operation since 2007

- Obama orders US to draw up overseas target list for cyber-attacks

Glenn Greenwald and Ewen MacAskill

Friday 7 June 2013 15.23 EDT

Shares 2,290 Comments 2,935



A slide depicting the top-secret PRISM program. Guardian

The National Security Agency has obtained direct access to the systems of Google, Facebook, Apple and other US internet giants, according to a top secret document obtained by the Guardian.

3%

BREAKING

- News doesn’t wait
- Centralized communications teams move faster in a crisis

Long news cycle = Coverage sentiment

BREAKING

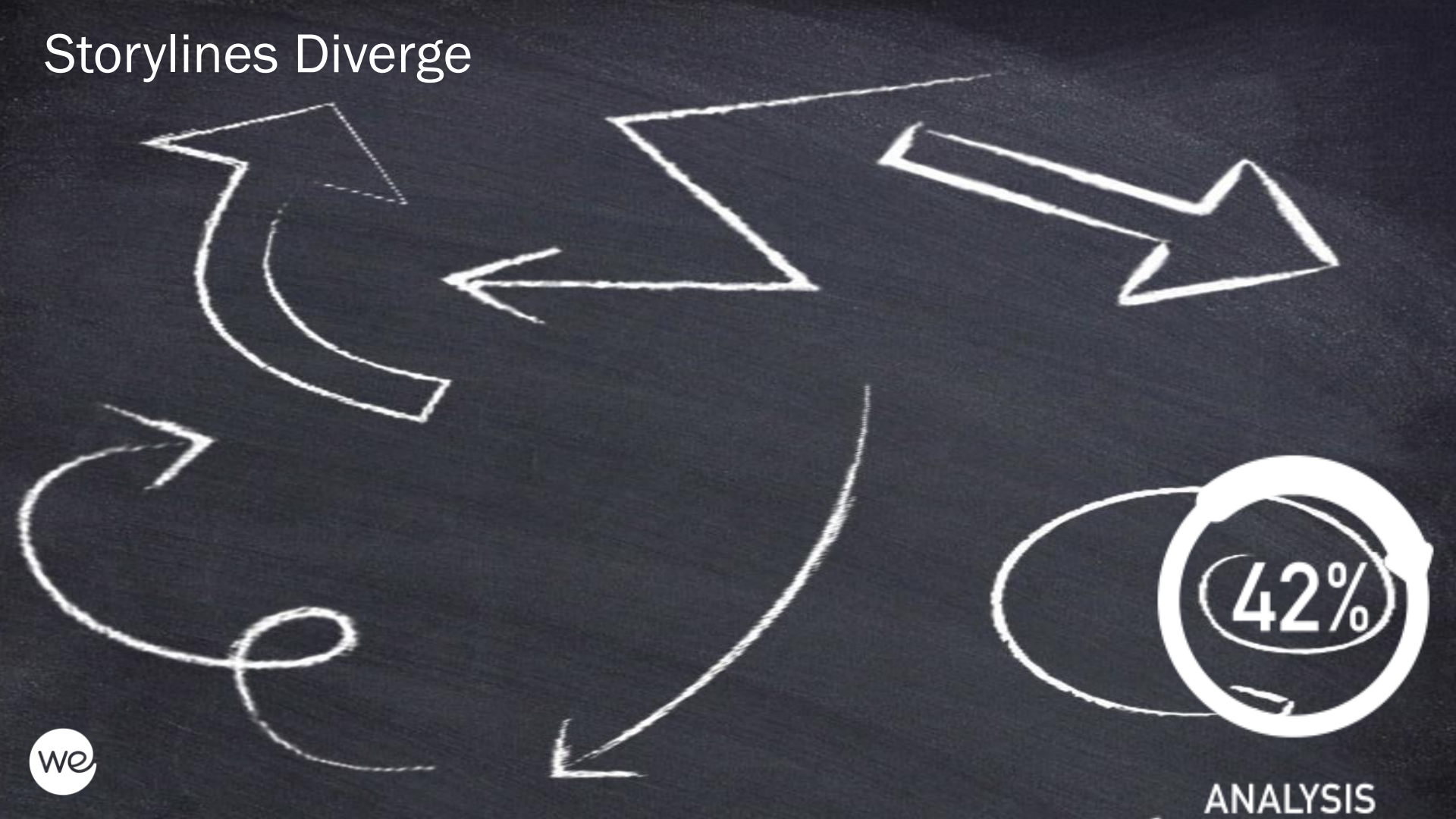
- Messages from company spokespeople are shared 40% more
- Being quoted isn't your only option

No participation = Coverage sentiment

INVESTIGATIVE

Coverage Sentiment

Storylines Diverge



- Analysis phase is the longest and skews the most negative for you
- Line up your own third party security voices in advance

Security experts = Coverage sentiment + shares

200 %

11%

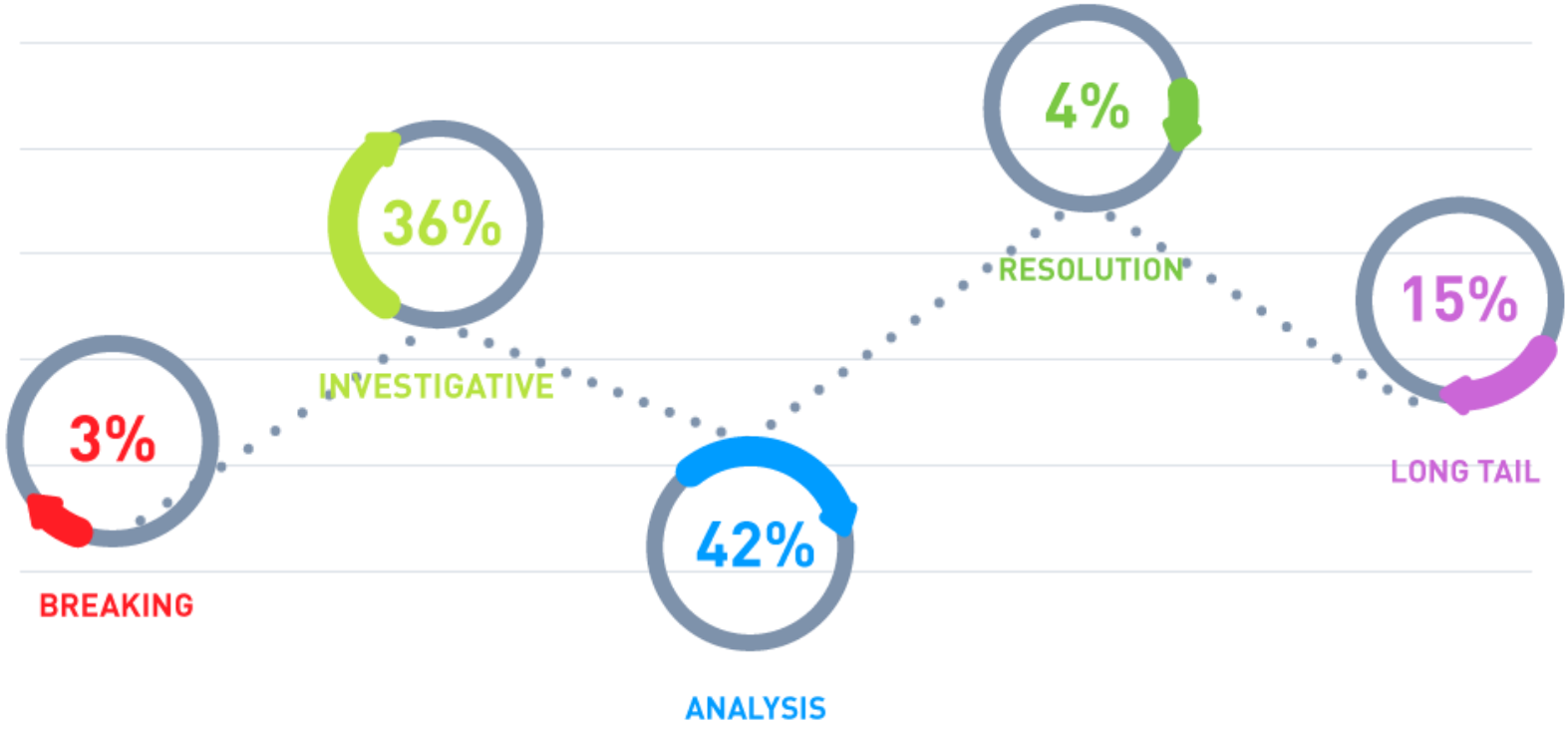
4%

RESOLUTION

15%

LONG TAIL

Sentiment


3%
BREAKING
36%
INVESTIGATIVE
42%
ANALYSIS
4%
RESOLUTION
15%
LONG TAIL

- Fight the instinct to close the door on the crisis
- Resolution coverage is the most positive for a company
- If not, long tail coverage will focus on what broke not how you fixed it

GOOD to KNOW

- Fortune (and news coverage) favors the prepared
- You’re the star of the party—don’t hide
- Focus on customers, not headlines
- Make friends & know your frenemies
- If you try, history might reward you

THANK YOU

Nicole Miller • Senior Vice President • @NicoleCMiller

WAGGENER EDSTROM®
COMMUNICATIONS

waggeneredstrom.com/cybersecurity

Apply What You Have Learned Today

- Next week you should:
  - Gather a team of technical, legal, executive and communication decision makers
- In the first three months following this presentation you should:
  - Develop a playbook
    - Threat assessment
    - Spokespeople
    - Messaging
- Within six months you should:
  - Battle test your plan and practice practice practice
  - Develop a supportive network of third parties that can speak on your behalf