NAB
NATIONAL ASSOCIATION OF BROADCASTERS

Tech Technology Update

Cybersecurity

Presented to

wba ON AIR WISCONSIN BROADCASTERS ASSOCIATION

SBE.

60th Broadcasters Clinic

October 12, 2016

Kelly T. Williams
Sr. Director of Engineering & Technology Policy
National Association of Broadcasters

Agenda

- *NAB Technology Department*
- *Broadcast Cybersecurity*
- *EAS*
- *FM in US Smart Phones*

NAB Technology Department

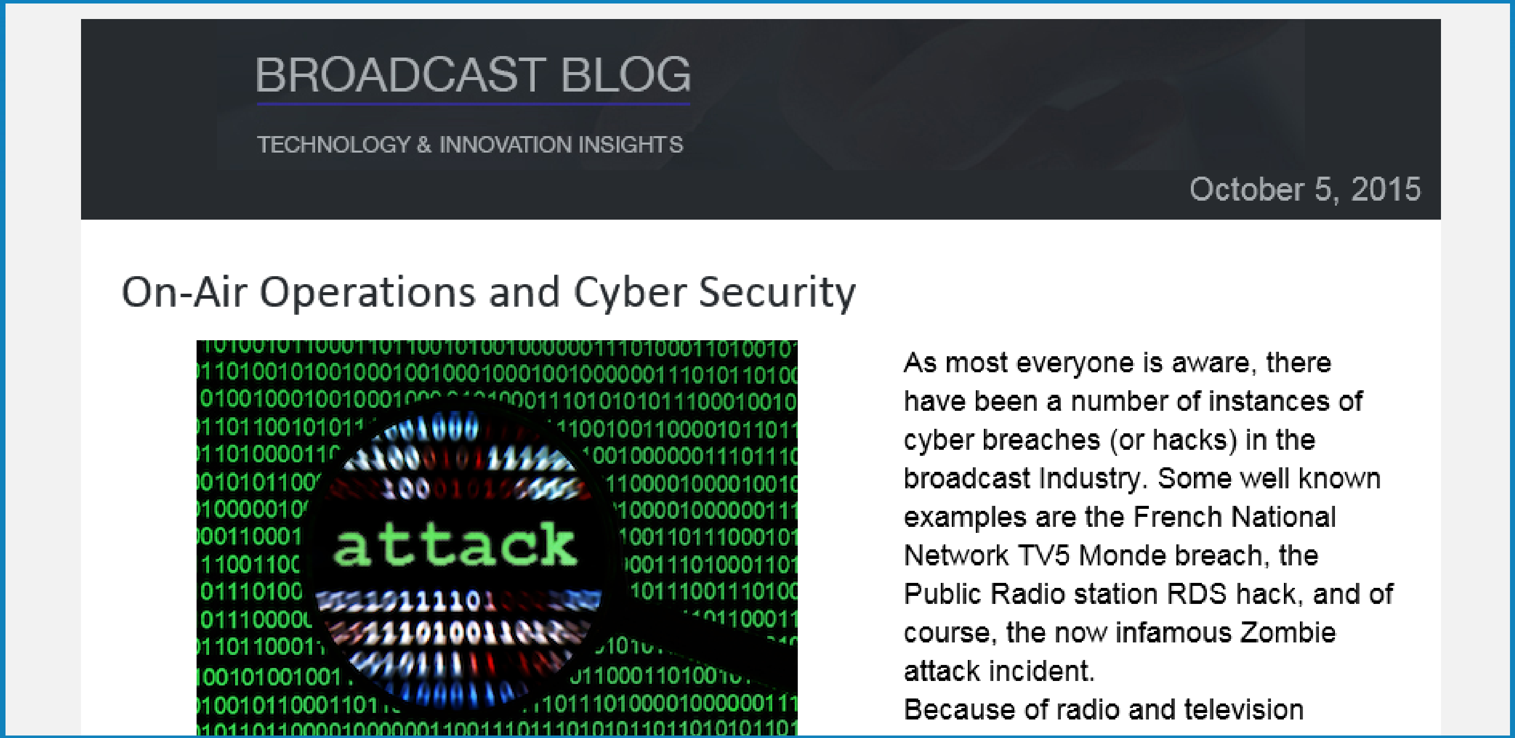
- CTO, 7 full-time engineers, support staff of 5
- Provide technical support to other NAB departments esp. Legal and Government Relations
- Responsible for technical programs at NAB events incl. NAB Show, Futures, Radio Show
- Current activities:
  - ATSC 3.0 development
  - FM chips in smartphones
  - PILOT (NAB Labs)
  - EAS

NAB Radio and TV Technology Committees

- Open to representatives from NAB-member organizations

Joint meeting at International CES in Las Vegas, NV

Broadcast Blog



BROADCAST BLOG

TECHNOLOGY & INNOVATION INSIGHTS

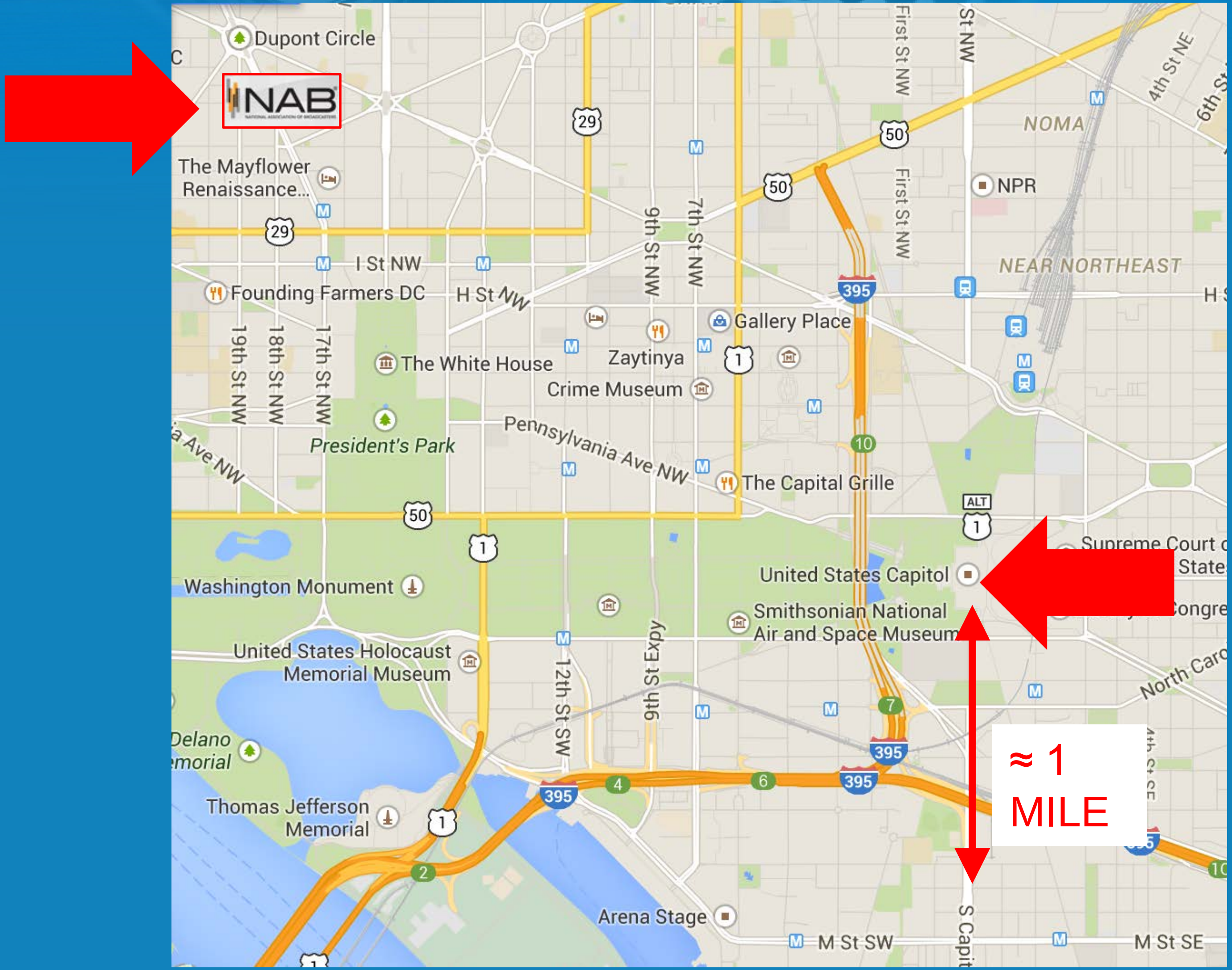
October 5, 2015

On-Air Operations and Cyber Security

As most everyone is aware, there have been a number of instances of cyber breaches (or hacks) in the broadcast Industry. Some well known examples are the French National Network TV5 Monde breach, the Public Radio station RDS hack, and of course, the now infamous Zombie attack incident.

Because of radio and television

https://www.nab.org/isgweb/login.asp


Dupont Circle
NAB
The Mayflower Renaissance...
NOMA
NPR
NEAR NORTHEAST
I St NW
H St NW
Founding Farmers DC
Gallery Place
Zaytinya
The White House
Crime Museum
19th St NW
18th St NW
17th St NW
9th St NW
7th St NW
First St NW
President's Park
Pennsylvania Ave NW
The Capital Grille
Supreme Court of the United States
United States Capitol
Smithsonian National Air and Space Museum
Washington Monument
United States Holocaust Memorial Museum
12th St SW
9th St Expy
North Carolina
Delano Memorial
Thomas Jefferson Memorial
Arena Stage
M St SW
M St SE
S Capitol
395
50
29
1
ALT

≈ 1 MILE

FUTURE HOME OF
NAB
NATIONAL ASSOCIATION OF BROADCASTERS

Broadcast Cybersecurity

Cybersecurity

- Documented Instances of Hacks in the broadcast Industry

June 12, 2016 - (Softpedia) Anonymous Attacks South African Broadcaster Over News Censorship (DDoS)

May 27, 2016 - (Radioworld) Avoid Paying a King's Ransom (Ransomware)

May 6, 2016 -(Talkers) Your Radio Station Is in Danger of Being Hacked

May 5, 2016 - (MalwareBytes) CBS-affiliated Television Stations Expose Visitors to Angler Exploit Kit (Malvertising exploit)

April 5, 2016 - (ArsTechnica) Nation-wide radio station hack airs hours of vulgar “furry sex” ramblings (STL hack)

Cybersecurity

- *On September 6th - Radio station in Alabama Hacked*
  - *Automation system wiped clean*
  - *Almost 2K files destroyed or deleted, including music, liners and over 900 ads.*
  - *Apparent ransomware*
- *The station has TWO firewalls and anti-virus software in place. Hackers went through two servers with separate IP addresses and different passwords.*
- *Station remained on-air because they had TWO backup systems.*

Cybersecurity

Feb. 2013 EAS Zombie Attack

"*Civil authorities in your area have reported that the bodies of the dead are rising from their graves and attacking the living. Follow the messages on screen that will be updated as information become available. Do not attempt to approach or apprehend these bodies as they are considered extremely dangerous*."

Cybersecurity

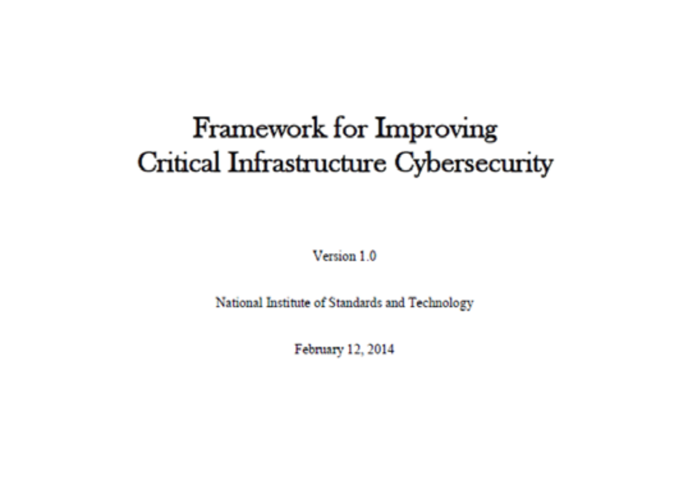
– TV Monde (French National Network)

Cybersecurity

- Broadcast station are considered by FCC & DHS Critical Infrastructure (Public Alerting Functions/EAS)
- FCC is concerned that stations On-Air ops are not adequately protected
- Fed Gov (FCC) may hold victim companies liable for hacks if adequate protections were not taken
- What to do???

Cybersecurity

- Communications Security, Reliability and Interoperability Council (CSRIC)
  - CSRIC-4 WG4 report on cybersecurity – March 2015
  - CSRIC-4 WG3 Report on EAS security – May 2014
- Based on NIST Cybersecurity Framework
  - Assess your risk then take action to protect your station



Framework for Improving
Critical Infrastructure Cybersecurity

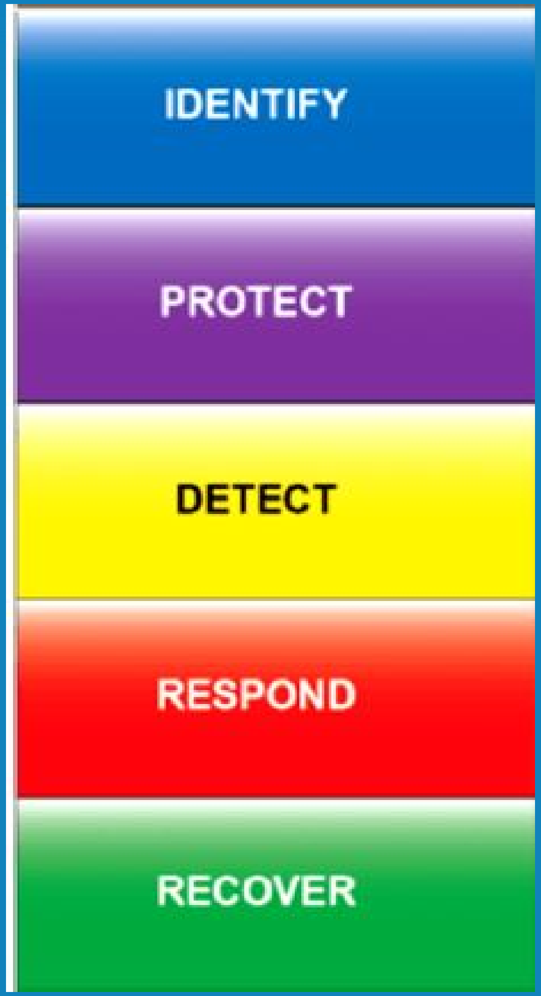
Version 1.0

National Institute of Standards and Technology

February 12, 2014

Cybersecurity

- NIST Framework



IDENTIFY

PROTECT

DETECT

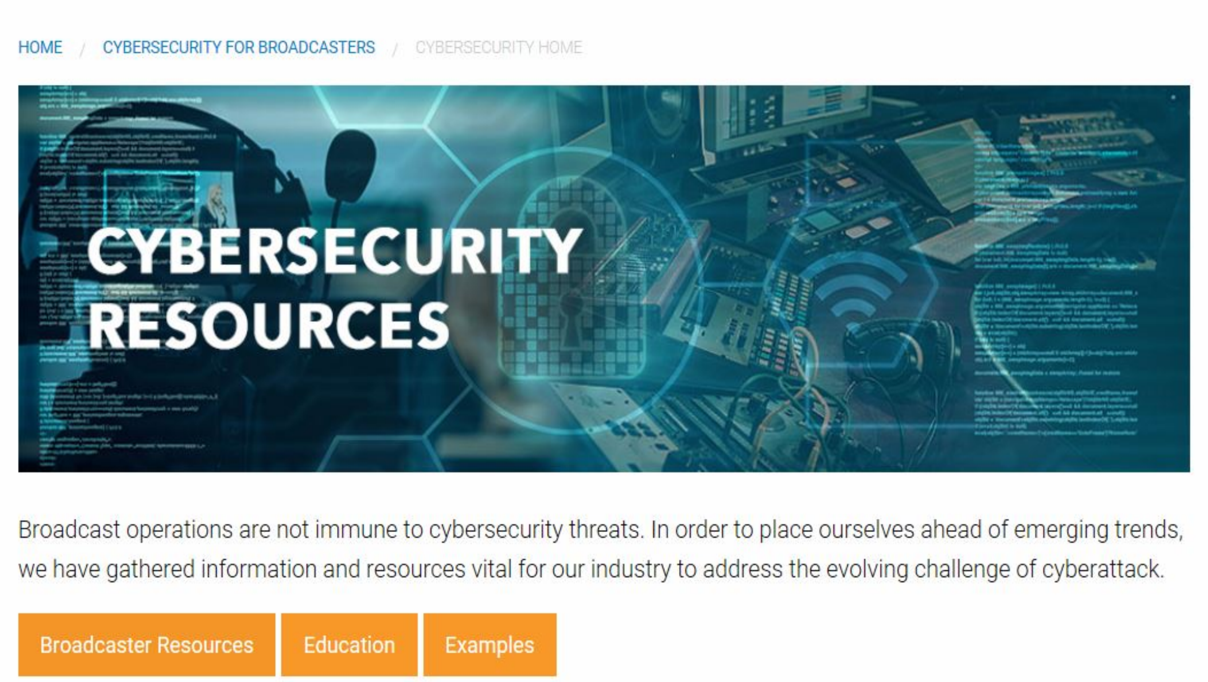
RESPOND

RECOVER

Cybersecurity

- NOT IF… BUT, WHEN!
- Most of Station's Critical Equipment is Linux or Window Machines
- Not Connected to Open Internet – Still Not Safe - e.g. Target/TV Monde
- Common Sense Approach
- Assess Your Risk (using the 5 steps – have a plan)
- Practice Good Cyber Hygiene
  - Strong Passwords (and User Names)
  - Change Default Pass Words (and User Names)
  - Firewall off B'cast network from station's general network
  - Try to Implement Station Wide Policies
- ***FCC Will be Calling Your CEO***

Cybersecurity



HOME / CYBERSECURITY FOR BROADCASTERS / CYBERSECURITY HOME

CYBERSECURITY RESOURCES

Broadcast operations are not immune to cybersecurity threats. In order to place ourselves ahead of emerging trends, we have gathered information and resources vital for our industry to address the evolving challenge of cyberattack.

35 Critical Cyber Security Activities All Broadcasters Should Know

NAB
NATIONAL ASSOCIATION OF BROADCASTERS

© Copyright 2016, National Association of Broadcasters, Washington, D.C. All rights reserved.

http://www.nab.org/cybersecurity/

Emergency Alert System

Emergency Alert System

- Nationwide test
  - Last Wednesday at 2:20 pm EST
  - Largely uneventful (i.e. went very well)
  - All participants were required to report to the FCC w/in 24 hours on the ETRS (Form 2)
  - Form three must be filed on or before November 14, 2016
- Results…
  - FCC received over 22K responses
  - Vast majority indicated that they received the test
  - FCC seems pleased.

Emergency Alert System

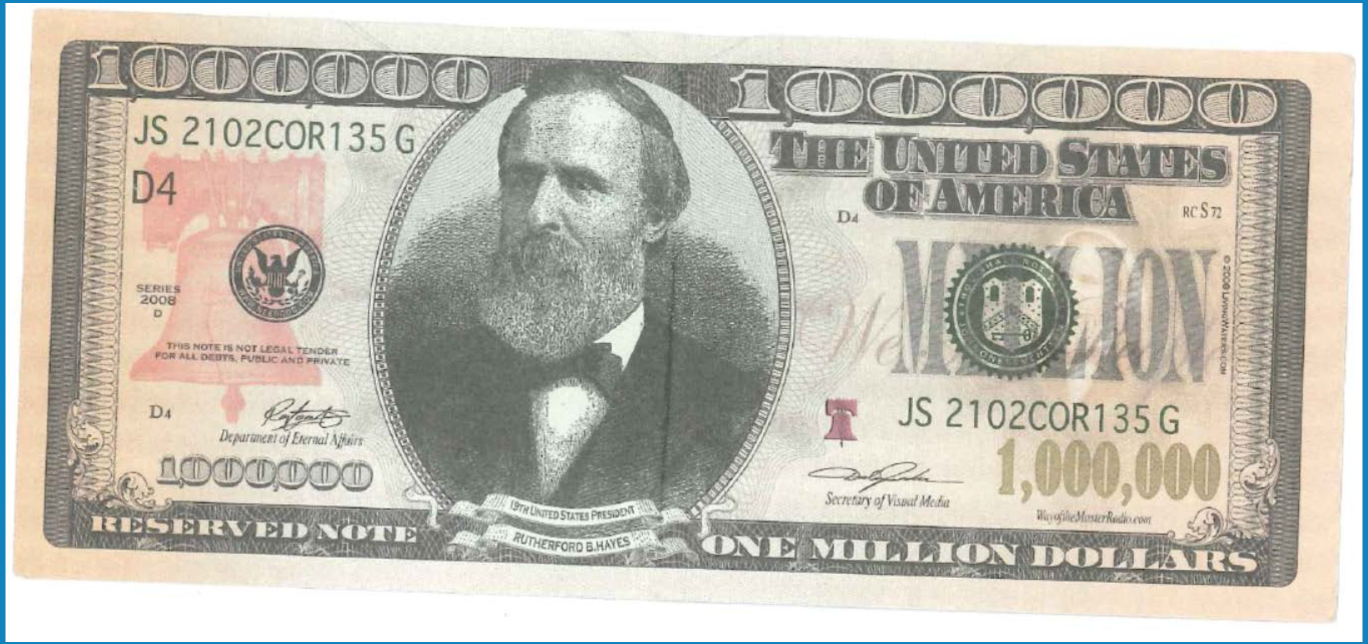
- Security
  - FCC released an R&O requiring Participants to certify that they comply with CSRIC EAS security recommended best practices.
  - https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG3-EAS_SECURITY_INITIAL_REPORT_062014.pdf
  - Via ETRS
- New Handbook
  - Used for Nationwide test
  - https://transition.fcc.gov/pshs/eas/ETRS/EASOperatingHandbook2016.pdf

Emergency Alert System

- FALSE EAS ALERTS! - Prohibition on…
  - Non-alert/non-test use of EAS tones
  - Mimicked or simulated EAS tones
  - The prohibition includes news and includes digital platforms
  - FCC Waiver for FEMA PSA

EAS Cautionary Tale

Like Taking Candy from a Baby



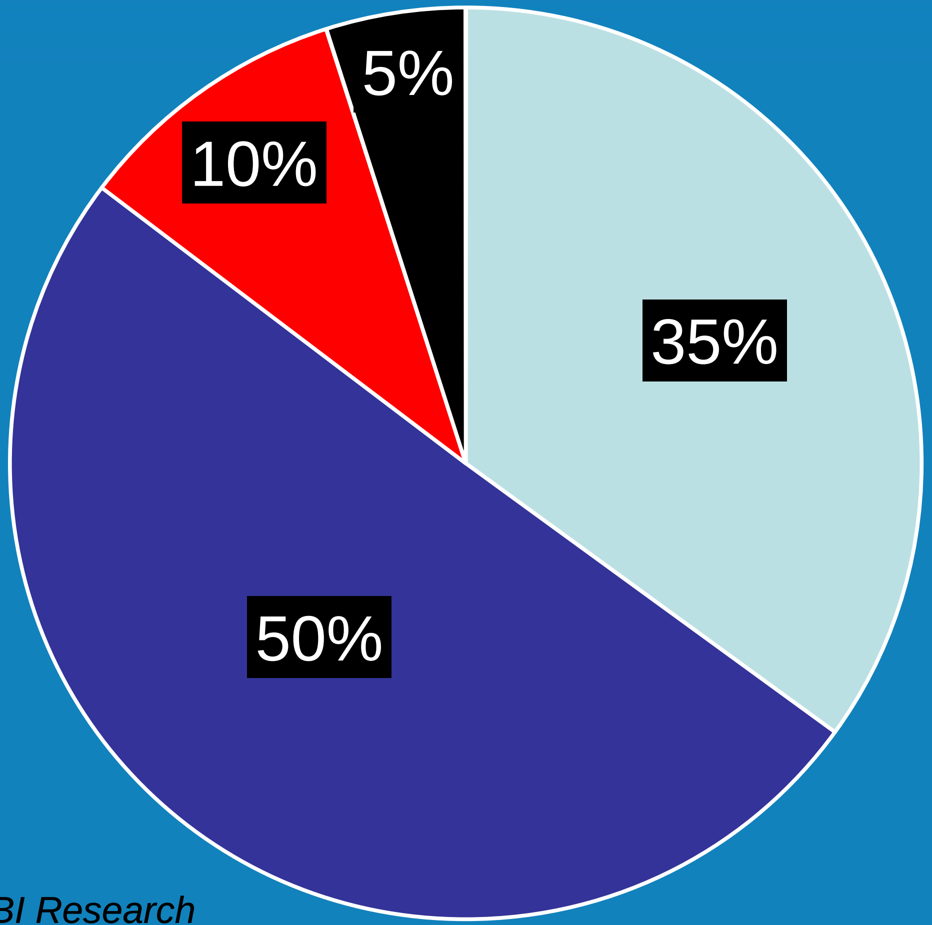
Too Close for Comfort

FM Activation Among Top-Selling Smartphones in U.S.

U.S. ACTIVATION DATA (1Q16)

FM Capability in Top-selling U.S. Smartphones 1Q 2016

(% of total sold),



*FM radio activated by at least one major U.S. carrier using these phones.

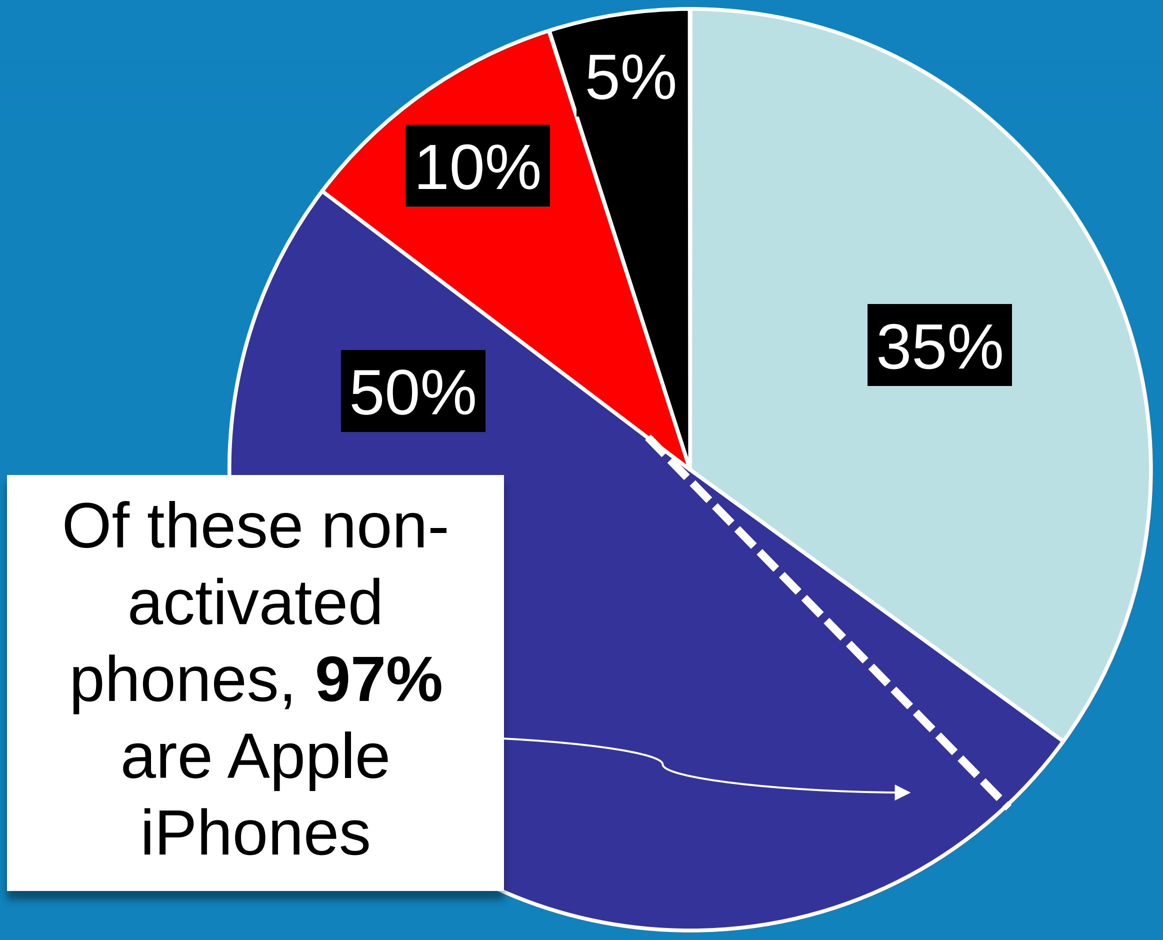
**Some international versions of these phones have activated FM radios. Activating FM in U.S. versions would likely not involve changes to hardware.

Source: *ABI Research*

NAB
NATIONAL ASSOCIATION OF BROADCASTERS

FM Capability in Top-selling U.S. Smartphones 1Q 2016

(% of total sold),



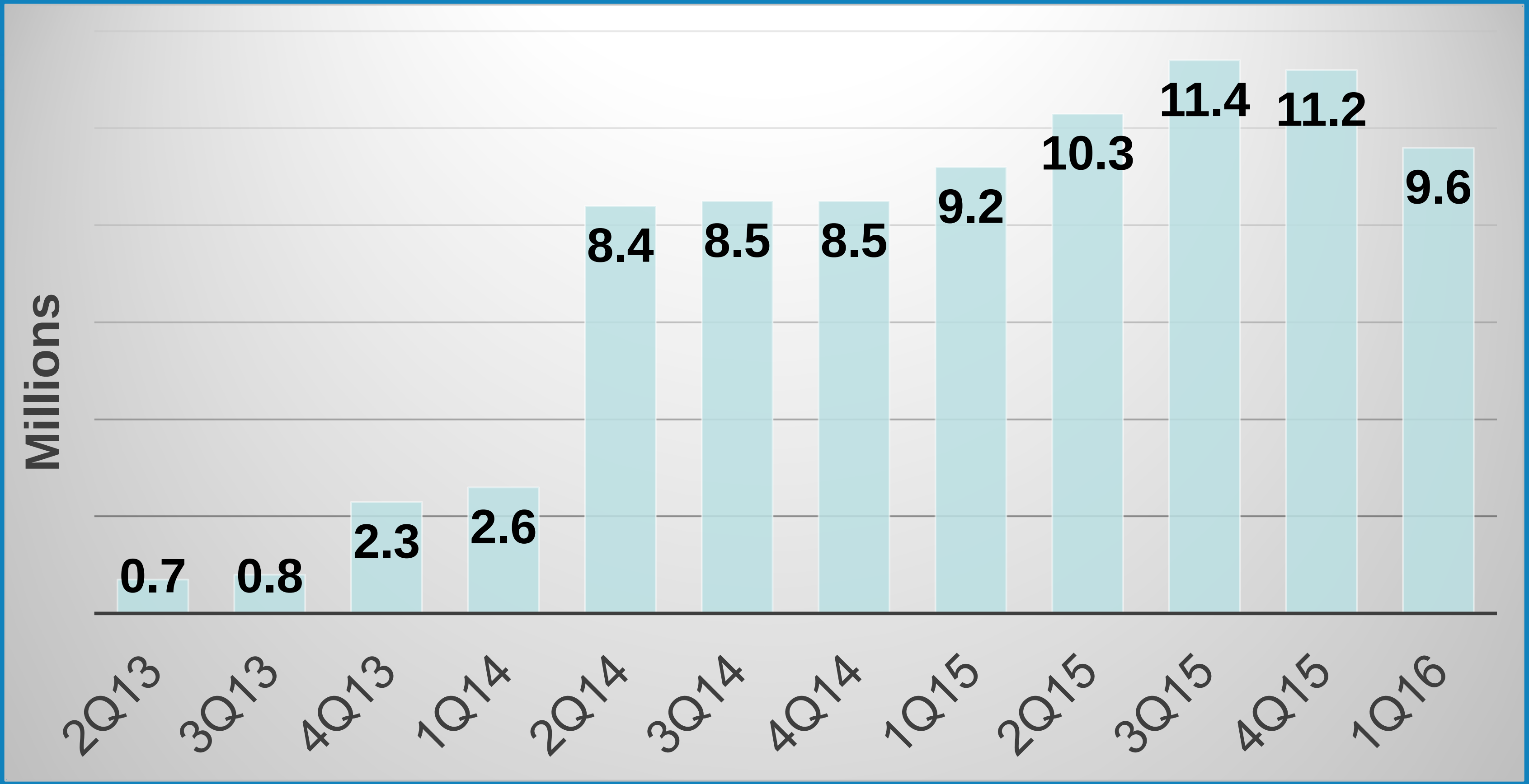
Of these non-activated phones, **97%** are Apple iPhones

Source: *ABI Research*

*FM radio activated by at least one major U.S. carrier using these phones.

**Some international versions of these phones have activated FM radios. Activating FM in U.S. versions would likely not involve changes to hardware.

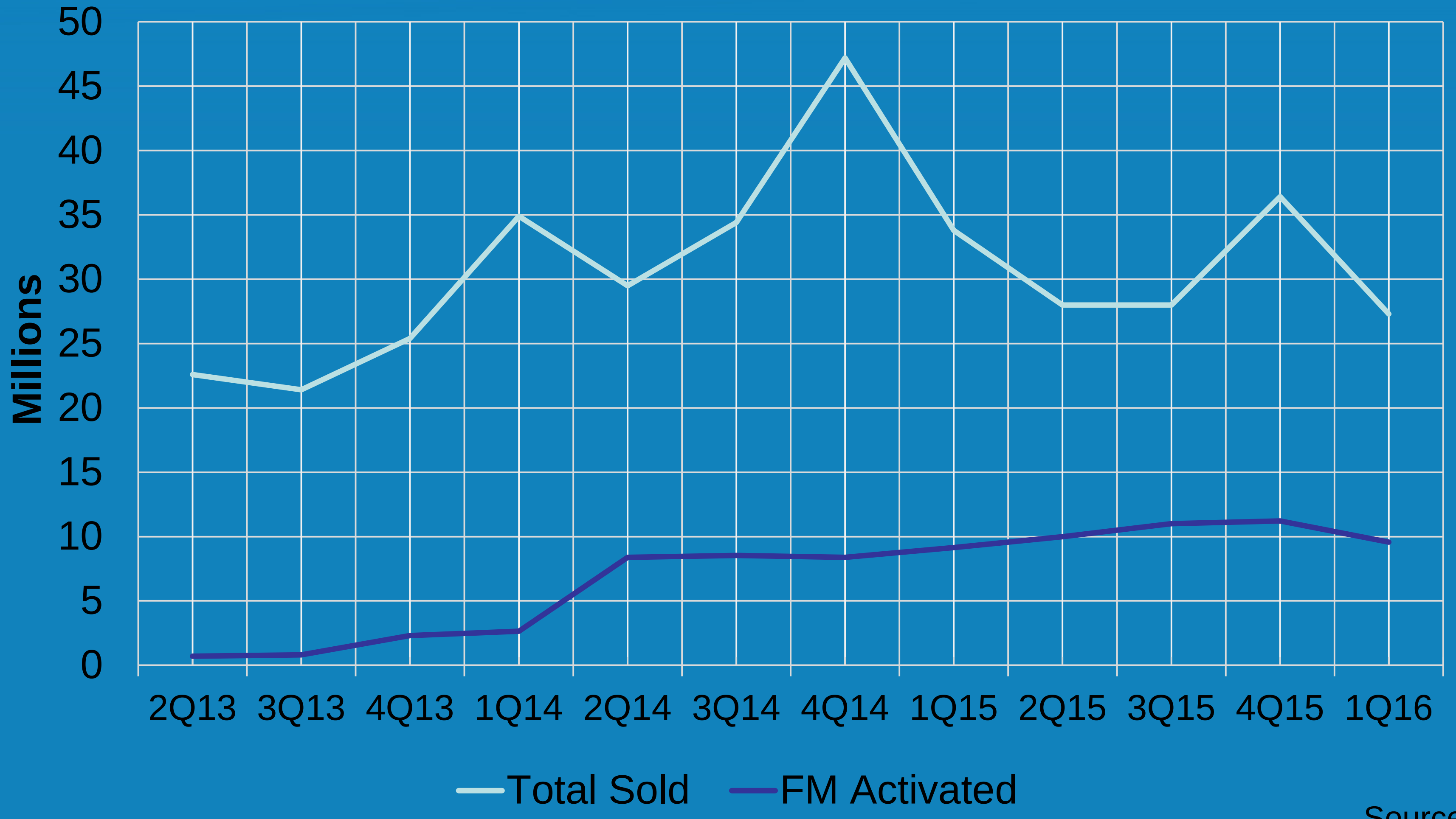
Smartphones Sold in U.S. with FM Radio Activated (millions)*



* FM radio activated by at least one major U.S. carrier using these phones.

Sources: *Strategy Analytics* and *ABI Research*

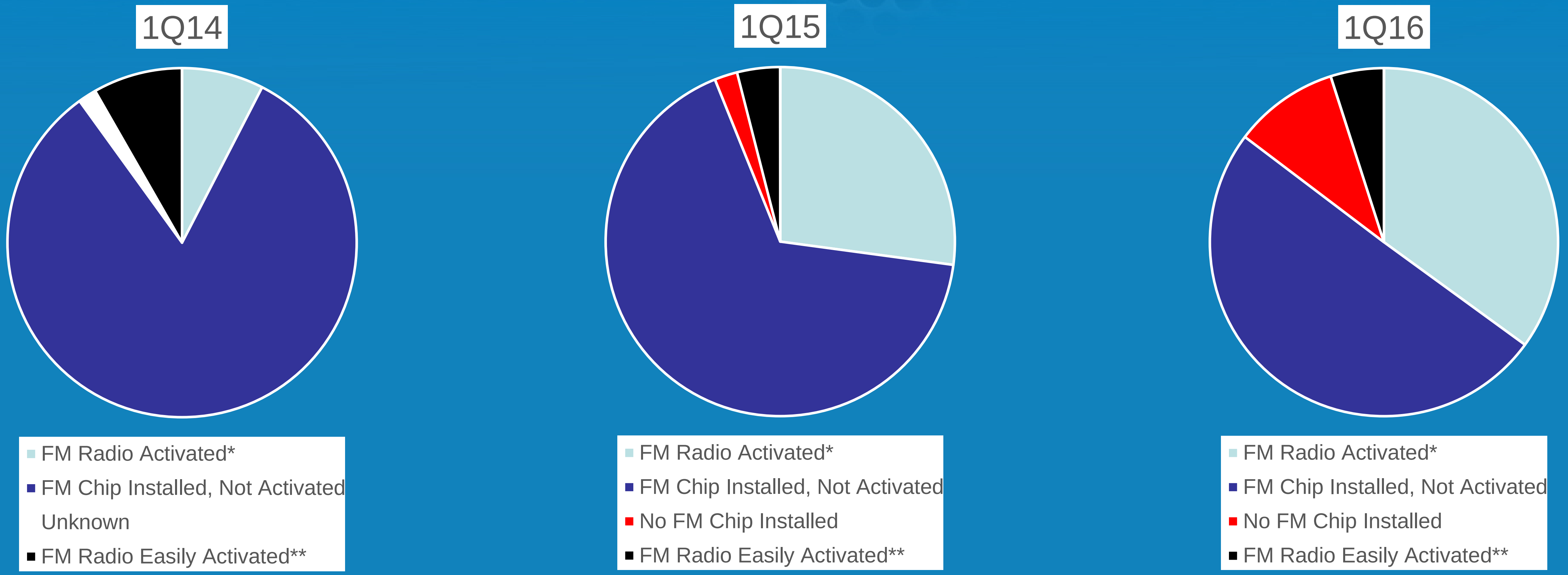
Smartphones Sold per Quarter (millions): Total Units vs. FM Activated Units*



* FM radio activated by at least one major U.S. carrier using these phones.

Sources: *Strategy Analytics* and *ABI Research*

FM Radio Capability in Top-selling U.S. Smartphones: Y2Y Comparison



*****FM radio activated by at least one major U.S. carrier using these phones.

******Some international versions of these phones have activated FM radios. Activating FM in U.S. versions would likely not involve changes to hardware.

Questions?

Kelly Williams
kwilliams@nab.org