Lynn COMMUNITY health CENTER

CUPPLES ASSOCIATES CONSULTING, LLC
Redefining Quality and Efficiency in Healthcare

Anatomy of a Breach: A Near Miss

Massachusetts League of Community Health Centers

Community Health Institute

May 17, 2018

Falmouth, MA

Massachusetts League of Community Health Centers

Presentation Overview

- Introductions:

  John Cupples, CEO, Cupples Associates Consulting, LLC.

- The Context

- Case Study of a Near-miss Breach at Lynn Community Health Center: Lisa Ewing, CHCIO, Lynn CHC.

- Lessons Learned:

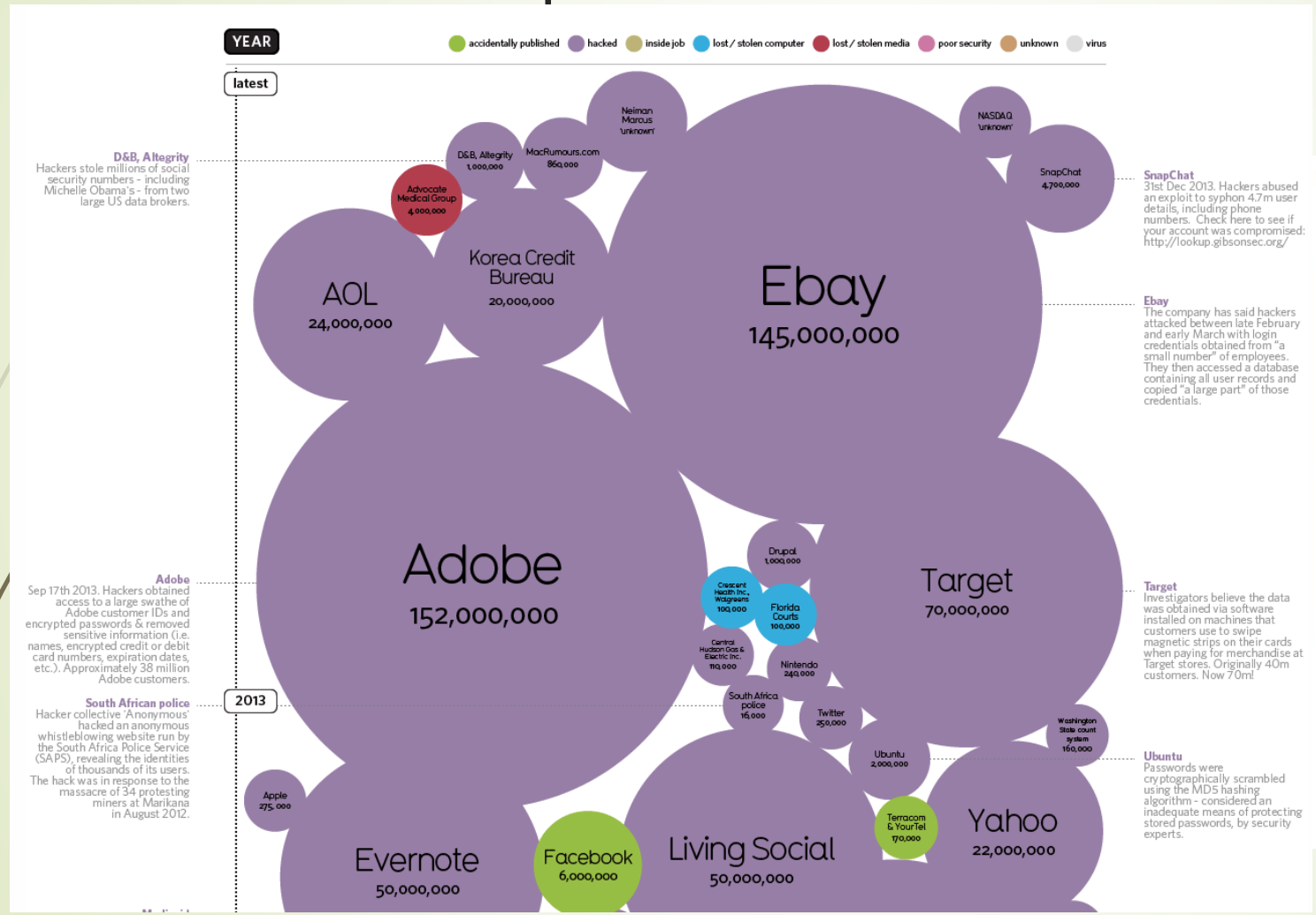
  Alicia Peters-Torrey, Consulting Partner, Cupples Associates Consulting, LLC.

The Context

- A tidal wave of Breaches
- An era of Cyber "insecurity"
- Not "If" but "When"

We're Swimming in an Ocean-sized "Swamp" of Breaches

We must assume with each passing day, our data is less secure.



U.S.-U.K. Warning on Cyberattacks Includes Private H

By DAVID D. KIRKPATRICK and RON NIXON APRIL 16, 2018

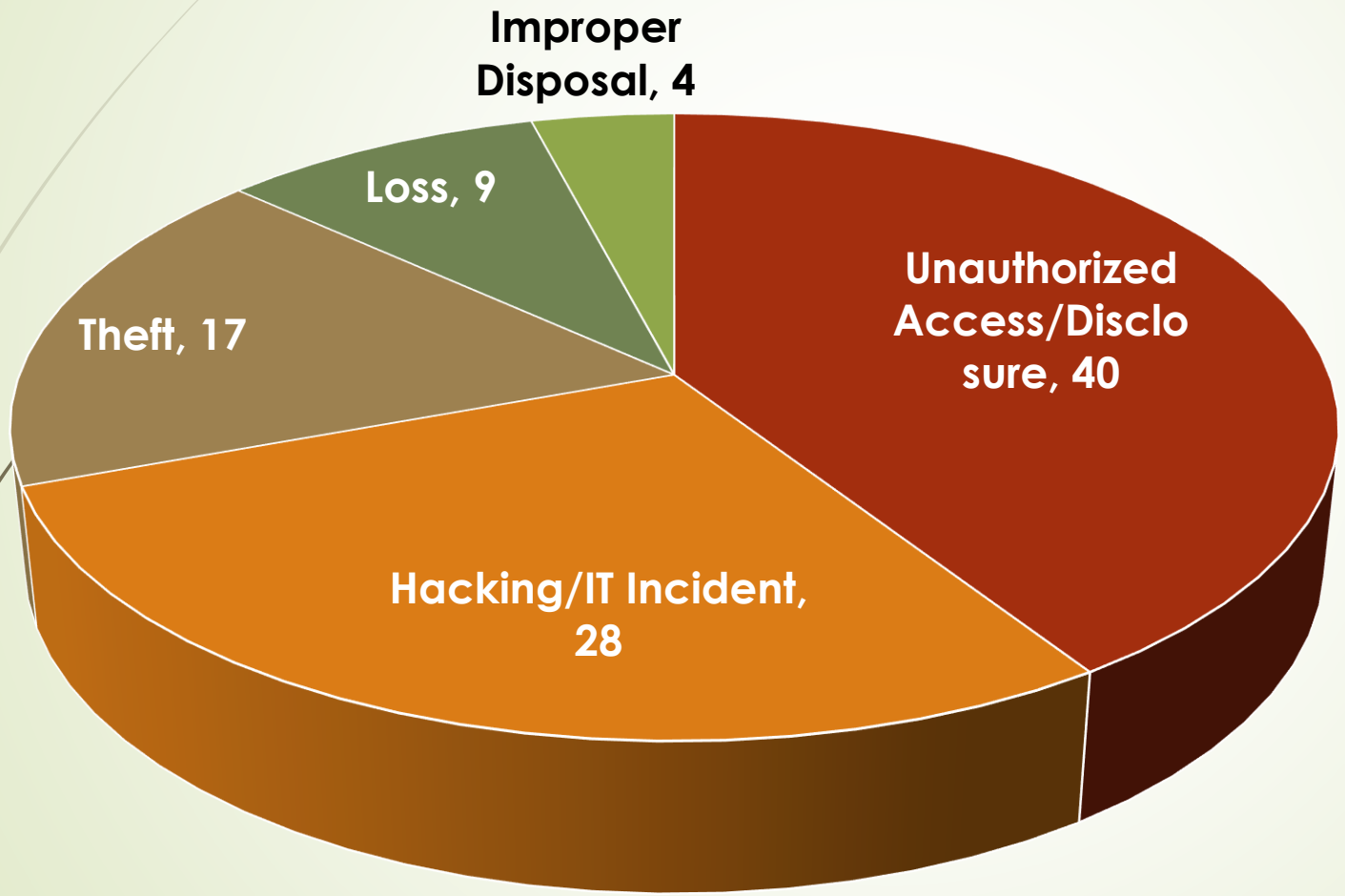
The New York Times

Prime Minister Theresa May of Britain. Britain and the United States on Monday issued warnings about possible Russian cyberattacks. Stefan Rousseau/Press Association, via Associated Press

LONDON — The United States and Britain on Monday issued a first-of-its-kind joint warning about Russian cyberattacks against government and private organizations as well as individual homes and offices in both countries, a milestone in the escalating use of cyberweaponry between major powers.

Source: https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-static/

2017 HIPAA Breaches >500



- Total medical records breached: 726,838
- 40 of the 90 Breaches (or 39%) were caused primarily by **workforce member error** or **malicious activity.**

Source: CMS report on breaches of protected health information (PHI) of 500 or greater records for CY 2017

Not if, but when

Lynn Community Health Center

A Case Study

Cyber Security at Lynn

- Cyber insurance
- Sage Data Security – log analysis and alerts
- Encryption
- Firewalls – new Palo Alto
  - Multiple levels of internet access depending on role
- Password Protection Practices
  - Change every 90 days
  - Minimum 8 mixed characters
  - Recommend use of phrases for complexity and ease of use
- Quantros Incident Reporting system
- Dedicated Information Security Officer with CISSP credential
- HIM Director – Certified Privacy Officer
- Regular meetings of our Privacy and Security Committee
- Weekly tips and information in our ITS Weekly Newsletter
- Training – orientation and ongoing
  - Phishing campaigns

What Happened?

- Email was received by several senior leadership staff
  - At first glance, this appeared to be a follow up to an actual request that had come from a partner organization
  - A staff member opened the link and entered their user name and password
  - 22 hours passed before we became aware and had the staff member change their password
- Implemented Incident Response plan (IT Director, Privacy Officer, ISO)
  - Opened Quantros incident and opened and Incident Response form
  - Reimaged 2 laptops
  - Created temporary rule to block emails (I/O) with 'see attached'
  - Contacted our security partner to review logs
  - Contacted our legal counsel to review our cyber insurance to ensure we were compliant with the insurance contract (i.e., notifications, etc.)
  - Reviewed O365 logs
  - Contacted Cupples Associates for input and to assist with a review of our process

Incident Response Program

- Quantros Incident Reporting Application
- Incident Response form
- Daily meetings with CIO, IT Director, Privacy Officer, ISO for the duration of the event
- Engage security partner(s)
- Post incident Lessons Learned meeting with Privacy and Security Committee
- Regular review of SRA and Security Audit to ensure we are making progress on our gaps

A Fortunate Resolution

- Only one document that contained patient data (PHI or PII) was accessed
- Patient was notified by registered mail

- Follow up:
  - Additional traffic monitoring was added that will allow us more insight in the event of future compromises
  - Using the event as a JC training exercise
  - Used the event as an educational tool for staff
  - Used the event to learn more about tools available to us in O365 (logs, auditing reports)

Lessons Learned:

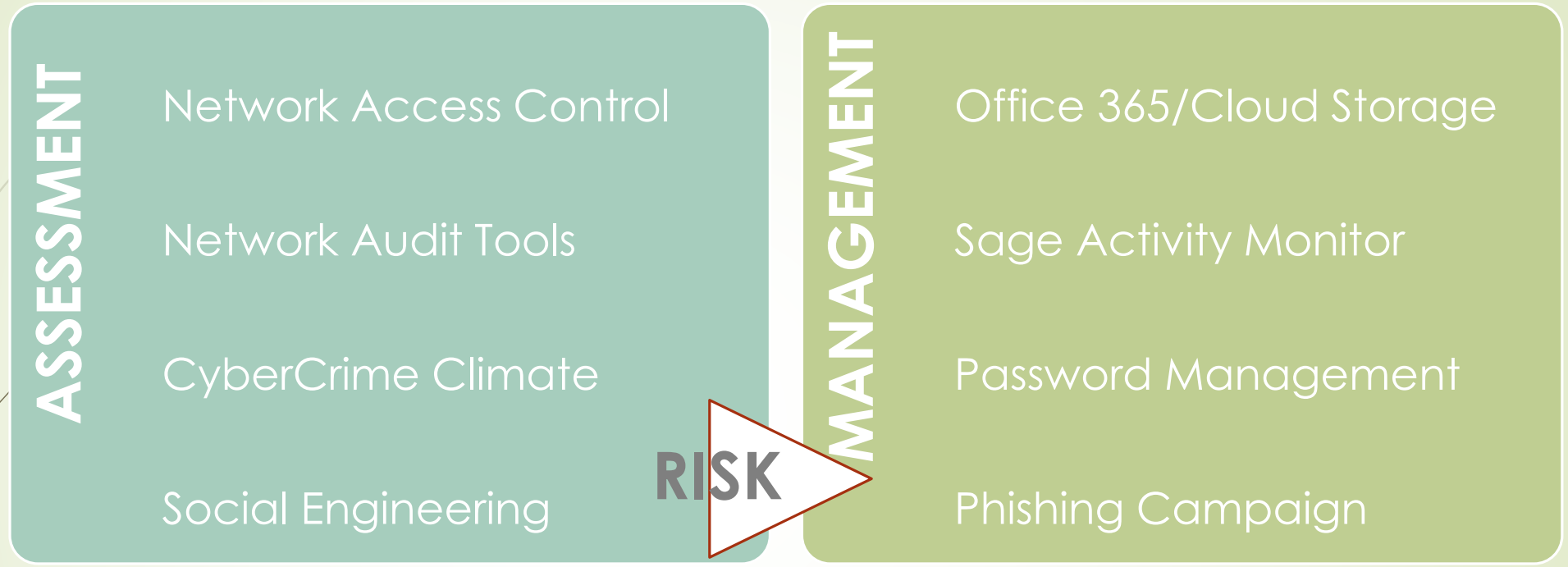
From the Lynn Case

From the Increasingly Insecure Context

"Expect the Best,
Prepare for the Worst,
Capitalize on What Comes"

– Zig Ziglar

Expect the Best



~~if~~ *when a new threat emerges,*

how will your team

- **Prioritize**
- **Decide**
- **Document**

Prepare for the Worst

C.F.R. §164.308 (6) Security Incident Response and Reporting:

(i) *Standard: Security incident procedures.* Implement policies and procedures to address security incidents;

(ii) *Implementation specification: Response and reporting.* Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes

~~if~~ when a breach happens, how will your team

- **Respond**
- **Communicate**
- **Document**

Capitalize on What Comes

~~if~~ when you've completed your breach response, how will your team

- **Learn**
- **Change**
- **Leverage**

Today's Presenters

- **Lisa Ewing:** Lisa is the CHCIO at Lynn Community Health Center, and has held that position for more than six years. She is a board member as well as past president of New England HIMSS. Lisa can be reached at lewing@lchcnet.org

- **Alicia Peters-Torrey:** Alicia is a consulting partner with Cupples Associates Consulting. Previously she served as CIO at Joslin Diabetes Clinic. Alicia has a long career in community health center information technology. Alicia can be reached at apeterstorrey@gmail.com

- **John Cupples:** John began his health center career in 1974 as founding director of Southern Jamaica Plain Health Center. After a career in hospital management, he founded Cupples Associates Consulting with a mission of assisting safety-net providers in improving access, quality and efficiency. John can be reached at jcupples@cupplesassociates.com

For More Information:

1. Graphical presentation of breach data worldwide: https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-static/
2. HIPAA Basics regarding the Privacy, Security, and Breach Rules: https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurityTextOnly.pdf
3. The basics of the Breach Notification Rule: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html