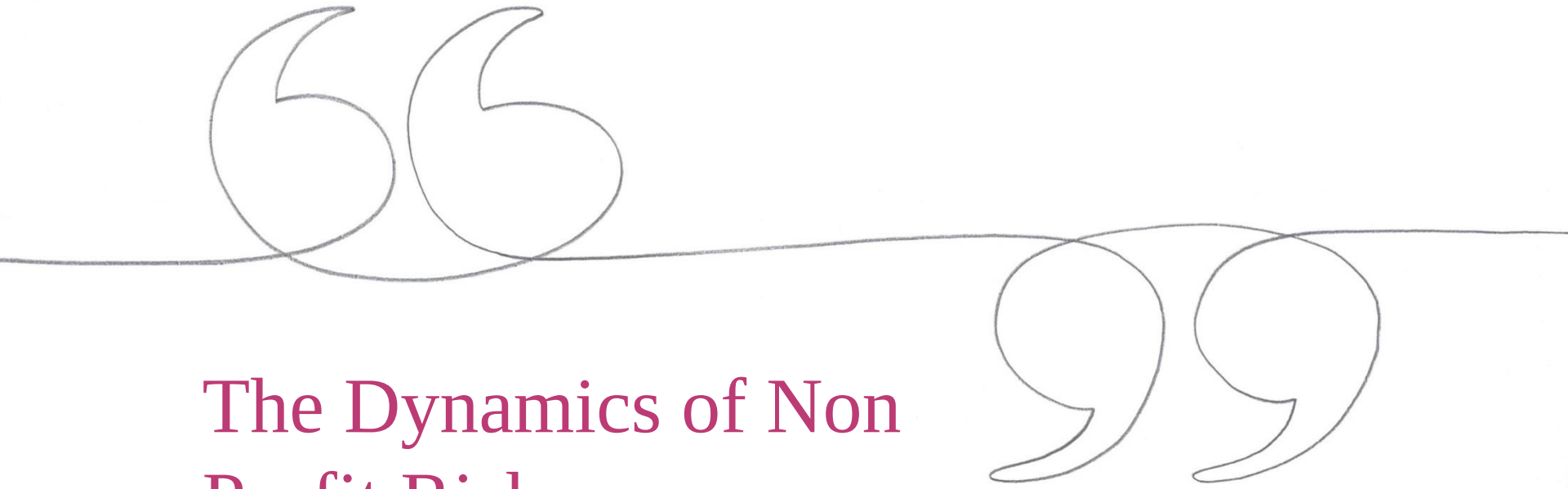
MMA Non Profit Vertical

CYBER INITIATIVE

BEAZLEY BREACH RESPONSE

December 2016

beazley



The Dynamics of Non Profit Risks

What is a Breach?

A breach is simple.

A breach is theft of data, loss of data or unauthorized access to data.

One more time….

A breach is theft of data, loss of data or unauthorized access to data.

Period.

The insured does not have receive a law suit to trigger a breach law.

The insured does not have to have proof of harm to trigger a breach law.

What Kinds of Information are at Risk?

Member/Donor/Fundee/Grantee/Participant Information

- Credit Cards, Debit Cards, and other payment information
- Social Security Numbers, ITIN's, and other taxpayer records
- Protected Healthcare Information (PHI), including medical records, test results, appointment history
- Personally Identifiable Information (PII), like Drivers License
- Financial information, like credit reports
- Educational Records
- Non-PII, like mailing lists with email addresses, phone lists, and home address that may not be independently sensitive, but may be more sensitive with one or more of the above

Employee Information

- Employers have at least some of the above information on all of their employees

Many people think that without credit cards or PHI, they don't have a data breach risk. But can you think of any not-for-profits *without* any of the above kinds of information?

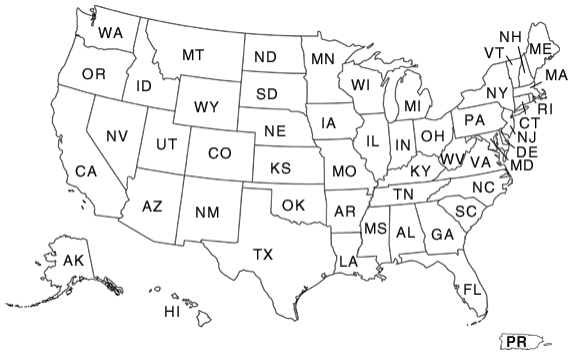
Why Are Non Profits a Target?

- Small and Mid-Sized nonprofits are quite vulnerable to hackers and other forms of breaches for several reasons:
    - They are often understaffed, utilize volunteers instead of paid professional staff and don't have the expertise or the infrastructure to implement and maintain best practices for security.
    - They often have staff or volunteers who work from home, and they are likely to be taking sensitive organizational information home with them on unsecured USBs, laptops or mobile devices. The exposure to lost or stolen devices or hard copy files is large.
    - They have large spreadsheets of data which if emailed to the wrong person poses a huge threat.
    - They hold sensitive information that is of interest and goes well beyond a credit card number: User names, email addresses, physical addresses, and, potentially, passwords can all be put to use by hackers.
    - They often use free software or inexpensive hosting.
    - They can use shadow databases which are prevalent and easy for hackers to get into. While they may have a central donor or CRM system, licenses can be expensive. When nonprofits need to involve volunteers, they may extract information from the secure database into an unencrypted spreadsheet and email it out.
    - They have trusted employees or volunteers who could go rogue.
    - They are vulnerable to hackers who might take over their computers with malware that can turn their hardware into bots waiting for an activation to participate in larger hacks or attacks on bigger systems.

The Legal & Regulatory Landscape

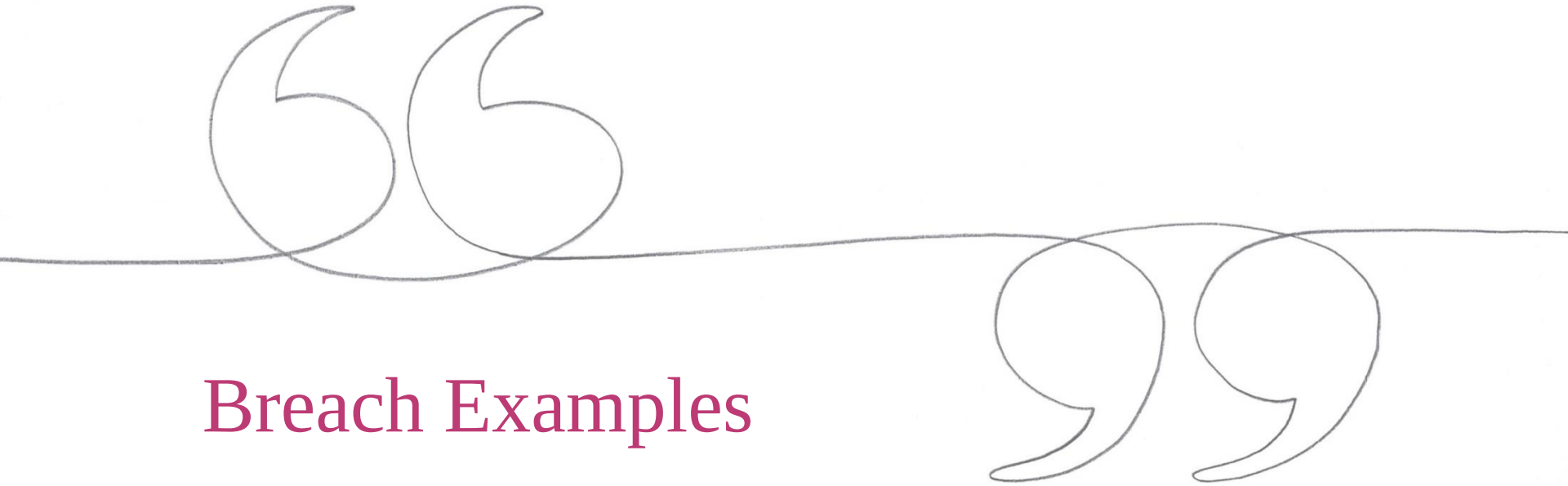
The Legal Landscape – US State Laws

- State Laws
  - 47 States + DC, PR, VI, GM (SD, NM and AL do not have laws)
  - No "lowest common denominator"
- Encryption is a safe harbor to most (not all) – (i.e. MA)
- Laws differ with respect to:
  - Notice Triggers
    - Definition of a Data Breach (acquisition vs access)
    - Data types (definition of PII)
    - Format of data (paper, electronic)
  - Timeliness
  - Required content for notification
  - Notification of attorneys general and various state agencies



The Legal Landscape – US Federal

- HIPAA-HITECH
  - Do you handle PHI? – CE or BA (Final Rule Changes as of 9-23-2015)
- PCI-DSS (v 3.1)
  - Do you accept transactional data? (Credit Card Data)
- FTC's Red Flags Rule
  - Are you a creditor?
- FACTA (Fair & Accurate Credit Transactions Act)
  - Do you use credit reports in the course of pre-employment background screening? (Not allowed – CA, CO, CT, IL, HI, OR, NV, MD, WA)
- FISMA (Federal Information Security Management Act of 2002)
  - Are you a federal contractor?
  - Notice to Congress (as of 1/1/2015)
- FTC – Section 5a
  - Do you engage in unfair or deceptive acts or practices?
  - Do you comply with your website's privacy policy?



Breach Examples

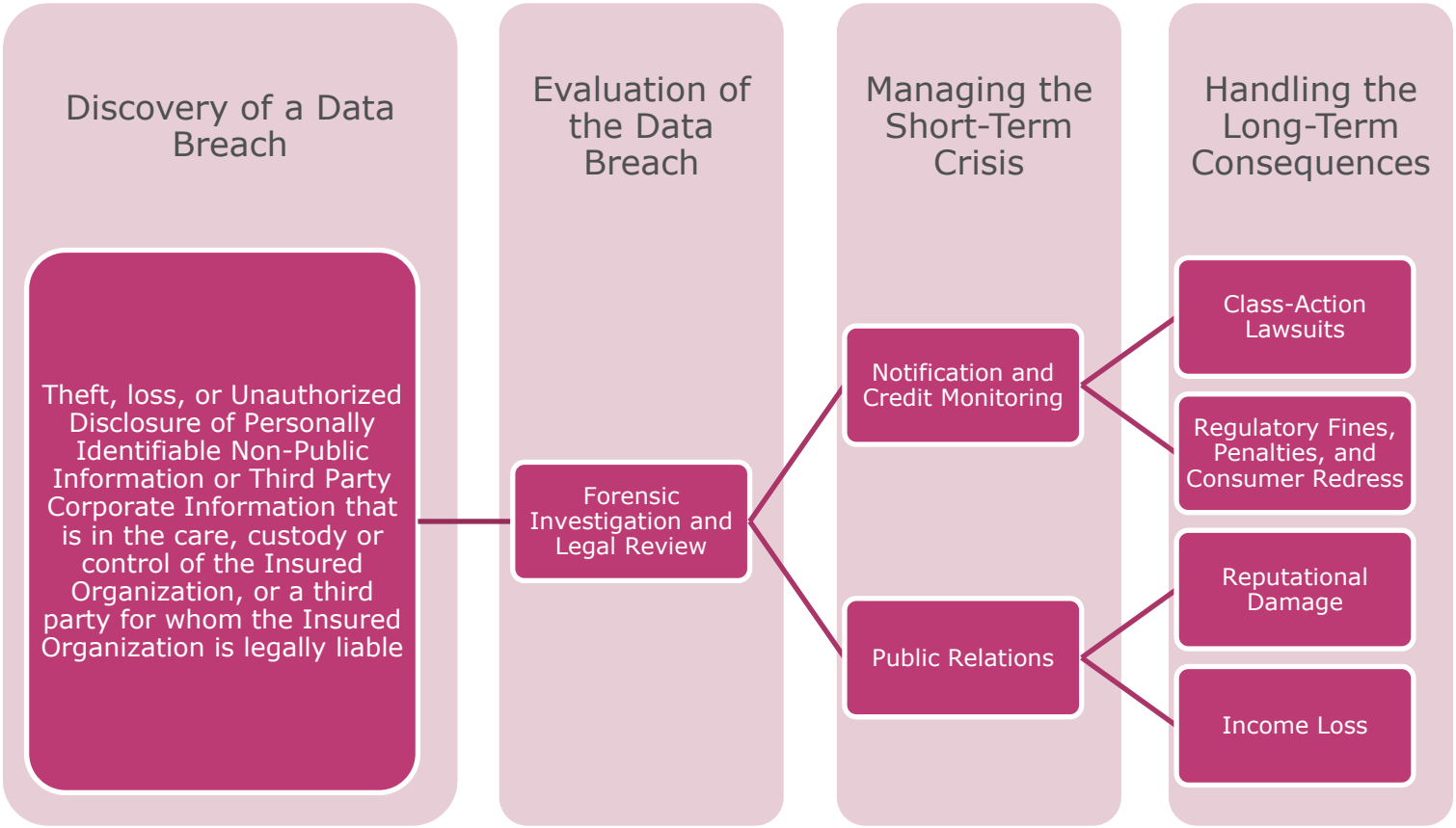
Types of Data Security Breaches

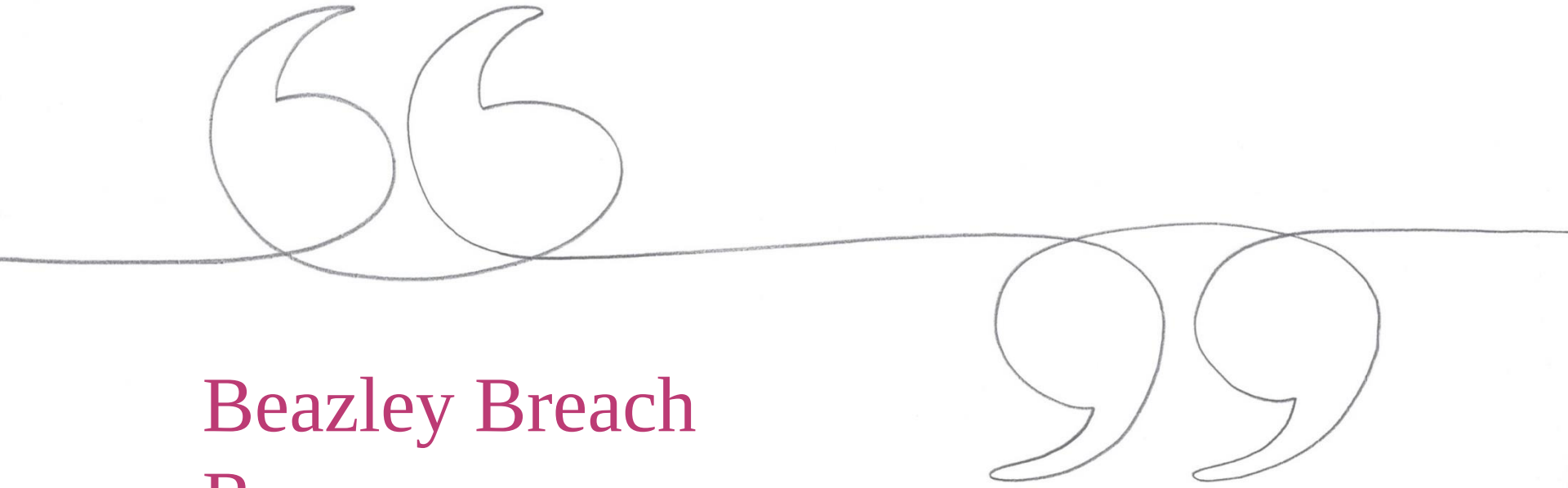
- Improper Disposal of Data
    - Paper
        - Un-shredded Documents
        - File cabinets without checking for contents
    - Electronic assets
        - computers, smart phones, backup tapes, hard drives, servers, copiers, fax machines, scanners, printers
- Phishing/Spear Phishing Attacks
- Network Intrusions or Hackers
- Malware Viruses and Ransomware Viruses
- Lost/Missing/Stolen Electronic Assets
- Mishaps due to Broken Business Practices (human error)
- Rogue Employees
- Third Party Vendors

More Breach Examples:

- Utah Food Bank
- Heritage Foundation
- Easter Seals
- Veterans of Foreign Wars
- Red Barn
- LA Gay and Lesbian Center
- Louisiana and Health Coop
- Folsom State Prison
- And 108 other examples sent to Lauren yesterday…..

A Simplified View of a Data Breach





Beazley Breach Response

What is Beazley Breach Response?

Information Security and Privacy Liability

- Information Security & Privacy liability, Regulatory Defense, Fines and Penalties, Website Content Liability, PCI Fines and Penalties are in the base form.
- Cyber Ext, Business Interruption, Data Protection, Media Liability via end.

+ Privacy Breach Response

- Notifications, Credit and Identity Monitoring and Call Center Services offered on a per person basis. This is outside and in addition to the policy aggregate.
- Legal, Forensic, Crisis Mgmt and PR offered via an additional limit that is outside and in addition to the policy aggregate.

Beazley Breach Response

- Beazley employs the only Breach Response Service team in the industry.
- A comprehensive solution to the risks of security breaches, data loss and unauthorized disclosures including expert hand picked vendors

What Else Makes Beazley Breach Response Different?

- Pre-Breach Education and Services
    - www.beazleybreachsolutions.com
    - Interactive Work shops
    - On-Boarding calls
    - Alex Ricardo
    - IRP reviews
- Dedicated Internal Breach Response Services team
    - Almost 5000 breaches handled since 2009
    - Beazley's *Pay-On-Behalf-Of* versus *saving your receipts*
- MMA Amendatory Endorsement
- Clients are encouraged to activate services when they *think* have a breach, since little breaches turn into big problems if they aren't handled properly. Coverage is triggered by reasonably suspected incidents.
- Services activated with one phone call or email (bbr.claims@beazley.com)

Official Notice

The descriptions contained in this presentation are for preliminary informational purposes only. The exact coverage afforded by the products described herein is subject to and governed by the terms and conditions of each policy issued. The publication and delivery of the information contained herein is not intended as a solicitation for the purchase of insurance on any US risk.

Any Questions