Balancing Data Disclosure Requirements and Transparency with the Protection of Confidential Information

Christina V. Bigelow
Scottsdale Regional Compliance and Ethics Conference
April 12, 2019

1

Overview

- Introduction
- Background
- Managing Data Disclosure Expectations/Obligations
- When Disclosure Implicates Confidentiality
- Balancing Confidentiality/Protection And Transparency
- Summary

2

Introduction

[1] BreachIndexLevel.com
[2] Thales, 2018 Thales Data Threat Report
[3] IBM, Cost of a Data Breach Study, 07/2018
[4] Corodata.com

- 14,717,618,286 confidential records stolen since 2013[1]
  - 6,492,212 records are stolen every day
- 67% global mid- to enterprise-level co. breached; 71% U.S. mid- to enterprise-level co. [2]
- Average data breach - $3.86M global; $7.35M U.S.[3]
  - $148/record (global); $225/record (U.S.)
- Security for data at rest is increasing in priority
  - 77% of IT spending globally in 2018; 83% U.S.[4]

3

Introduction (cont'd)

[1] Corodata.com
[2] 2019 Intelligent Information management Report
[3] Shred-it, 2018 State of the Industry, Information Security Report

- $1.1T losses result from paper data/file theft[1]
  - Such disclosures are usually "inadvertent"
- Storage and management of documents occurs through[2]:
  - Email 69%
  - Shared network drives and folders 55%
  - Local storage 54%
  - Document management systems 24%
- 69% of corp. /71% of small business data breaches are in part attributed to employees[3]
  - Human error or accidental loss (47% corp, 42% SBs)
  - Deliberate theft or sabotage (22% corp, 29% SBs)

4

Background

- Confidential information can be defined as:
  - Any and all information of the Company that is not generally available to the public, including any information received by the Company from any Person with any understanding, express or implied, that it will not be disclosed
  - Confidential Information does not include information that enters the public domain, other than through a breach of confidentiality obligations

5

Background (cont'd)

- Federal laws requiring data protection for confidential information
  - Gramm Leach Bliley Act (15 U.S.C. 6802(a) et seq.)
  - Health Information Portability and Accountability Act (29 U.S.C. 1181 et seq.)
  - Federal Trade Commission Act (15 U.S.C. 41 et seq.)
  - Driver's Privacy Protection Act of 1994 (18 U.S.C. 2721 et seq.)
  - Fair Credit Reporting Act, amended by Fair and Accurate Credit Transactions Act (15 U.S.C. 1681)
  - Privacy Act of 1974 (5 U.S.C. 552a)
  - Sarbanes Oxley Act (15 U.S.C. 7241; 18 U.S.C. 1350)
  - Critical Infrastructure Information (CII) Act of 2002 (6 C.F.R. 29 et seq.)
  - Fixing America's Surface Transportation Act of 2015 (16 U.S.C. 8240-1)
  - Atomic Energy Act, Effective 08-08-2005 (42 U.S.C. 2014 et seq.)
- Data protection is generally addressed by sector

6

Background (cont'd)

- States also have data protection, privacy, breach notification laws
- Companies must comply with these requirements while:
  - Meeting regulatory reporting requirements
    - Mandated reporting and information collection examples:
      - Healthcare/Social Work/Education
      - Occupational Safety and Health
      - Securities and Exchange
      - Equal Employment Opportunity/Department of Labor
      - Housing and Urban Development
      - Department of Defense/Veterans Affairs

7

Background (cont'd)

- States also have data protection, privacy, breach notification laws
- Companies must comply with these requirements while:
  - Operating efficiently and effectively
    - Healthcare – Filing with insurers, debt collection, litigation
    - Use of contractors and vendors
      - Software vendors; cloud providers; staff augmentation
  - Industry data exchange

8

Managing Data Disclosure Expectations/ Obligations

- Numerous methods to manage data disclosure obligations
  - 1st – Employees have to know what to protect
    - Information Management/Protection policy/program
    - Classification/Labeling
    - Training
    - Access Control/Authorization/Monitoring
    - Data room or library

9

Managing Data Disclosure Expectations/ Obligations (cont'd)

- Numerous methods to manage data disclosure obligations
  - 2nd – Employees have to understand their obligations
    - Non-Disclosure provisions in employment agreement
    - Confidentiality obligations in employee handbook
    - Company execution of non-disclosure agreements/ provisions
    - Data loss protection and monitoring
    - Data Request and Response Processes
      - Regulatory filings, discovery, third-party requests
    - Exit Interviews/Covenants

10

Managing Data Disclosure Expectations/ Obligations (cont'd)

- Numerous methods to manage data disclosure obligations
  - 3rd – Employees have to understand available protections
    - Vendor non-disclosure provisions/agreements
    - Encryption/Password protection
    - Redaction
    - Secure transmission/On-Site observation

11

When Disclosure Implicates Confidentiality

- Most critical aspect is awareness
  - That the data is confidential
    - Specific classifications – PII, PCII, CEII, export control, etc.
  - Whether disclosure can/should occur
    - Including any regulatory restrictions/constraints
  - The most appropriate protections for disclosure
    - Feasibility of application
  - What is the appropriate disclosure process to follow
    - Process will differ based on the genesis of the request

12

When Disclosure Implicates Confidentiality (cont'd)

- Awareness applicable to native and received data
  - When confidential data is received, employees must be aware of/abide by company obligations
- Established, well-known processes/controls are key
  - Receipt – execution of agreement; communication of obligations; storage; use; etc.
  - Protection/Disclosure –classification; labelling; storage; disclosure processes; available protections
    - Redaction v. NDA

13

Balancing Confidentiality/Protection And Transparency

- Processes should address corporate preferences
  - Need for disclosure
    - Necessary v. advantageous
    - Alternative means to achieve same result
  - Amount/Type of data to be disclosed
    - Redaction v. other protected disclosure
      - Appropriate, applicable protections

14

Balancing Confidentiality/Protection And Transparency (cont'd)

- Processes should address corporate preferences
  - Amount/Type of data to be disclosed
    - Appropriate, applicable protections
      - Number/combination of protections
    - Format and content
      - Hewing closely to request v. relaxed sharing
      - "Actionable" formats v. "Controlled" formats
        - Excel/Word v. PDF

15

Balancing Confidentiality/Protection And Transparency (cont'd)

- Processes should address corporate preferences
  - Reviews/Approvals
    - Mandatory v. optional
  - Disclosure Agreements – company execution
    - Signature authority
    - Communication of execution and obligations
    - Monitoring

16

Balancing Confidentiality/Protection And Transparency (cont'd)

- Processes should address corporate preferences
  - Disclosure Agreements – vendor/other execution
    - Development and accessibility of templates
    - Communication of templates, applicability, expected use, and execution
    - Reinforcement
    - Monitoring

17

Summary

- Managing confidential data = continuous, active process
  - Program management principles should be applied
    - Periodic reviews for effectiveness/changes
    - Triggered reviews to keep current
  - Training and availability of resources essential
    - Periodic reinforcement;
    - Consistent availability
  - Control effectiveness and communication
    - Monitoring, Trending, Lessons learned

18

Questions?

19