Cyber Liability and Data Compromise; The New Risk Management Frontier

Today's Agenda

- What is a Data Breach?
- Data Breach Concerns
- Data Breach Causes
- Data Breach Risk Management

North Dakota's Breach Notification Law

- NDCC Chapter 51-30
  - Any person owning computerized data that includes personal information shall disclose any breach of the system following discovery of the breach to any resident of the state whose unencrypted information was, or is reasonably believed to have been, acquired by an unauthorized person.
  - Also must notify Attorney General if breach exceeds 250 individuals.

North Dakota's Breach Notification Law (cont.)

- Notification:
  - Written notice;
  - Certain electronic notice options;
  - Or, substitute notice if the cost will exceed $250,000 or there are over 500,000 affected persons
    - Email, Website Posting, and Media Notification

Notification Laws

- 48 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands require notification of security breaches involving personal information

What is a Data Breach?

- NDCC Chapter 51-30-01 defines “Breach of the Security System”
  - “…unauthorized acquisition of computerized data when access to **personal information** has not been secured by encryption or by any other method or technology that renders the electronic files, media, or databases unreadable or unusable.”

What is a Data Breach? (cont.)

- NDCC 51-30-01 defines "Personal information" broadly.

"…**an individual's first name or first initial and last name in combination with any of the following** data elements, when the name and the data elements are not encrypted:

(1) The individual's **social security number**;
(2) The **operator's license number**;
(3) A nondriver color photo **identification card number**;
(4) The individual's **financial institution account number**, **credit card number**, or **debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial accounts;**
(5) The **individual's date of birth**;
(6) The **maiden name of the individual's mother**;
(7) **Medical information**;
(8) **Health insurance information**;
(9) **An identification number assigned to the individual by the individual's employer**; or
(10) The individual's **digitized or other electronic signature**.

What is a Data Breach? (cont.)

- "Personal Information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

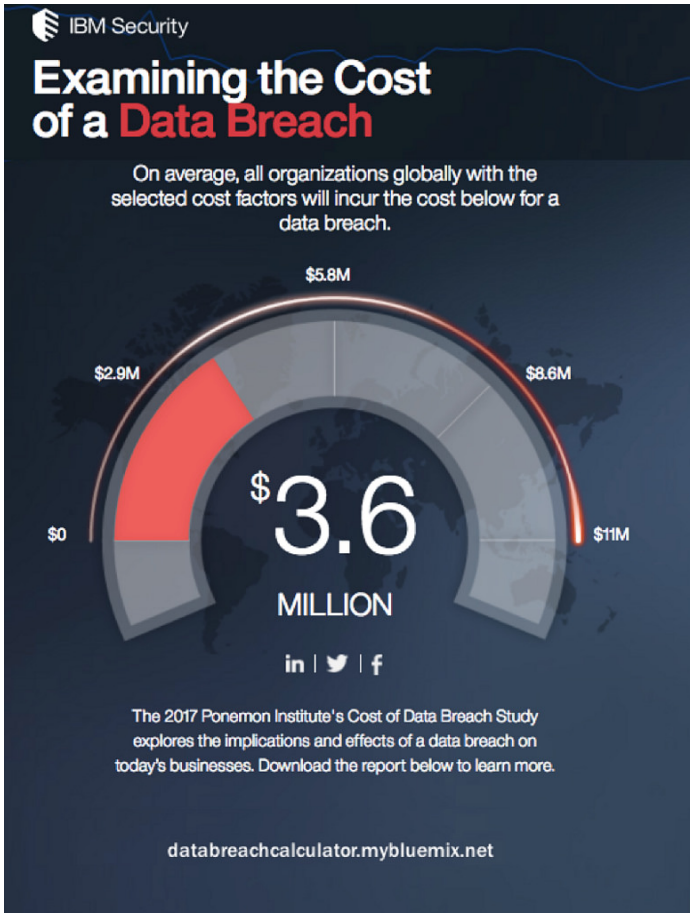
Cost of a Breach

- Breach Expenses (IDT 911, LLC)
  - Legal Costs ($300-$600 per hour)
  - Forensics ($250-$600 per hour)
  - Notification ($1-$3 per record)
  - Call Handling ($7-$25 per call)
  - Credit and Fraud Monitoring ($8-$75 per record)
  - Identity Theft Resolution ($400 per case)

Cost of a Breach (cont.)

Records	Average Cost
100	$18,000 - $36,000
1,000	$52,000 - $87,000
10,0000	$143,000 - $223,000
100,0000	$367,000 - $615,000
1,000,0000	$892,000 - $1,775,000

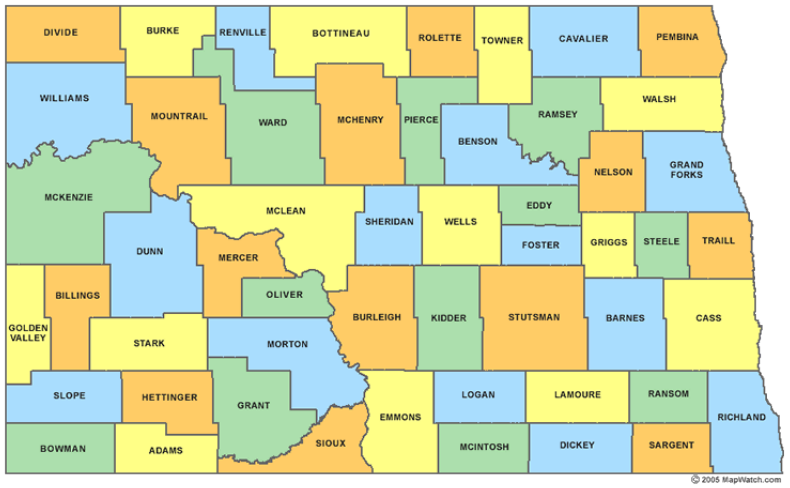
Cost of a Breach (cont.)



- True Cost Varies
  - Type of Data
  - Type of Breach
  - Legal or IT Assistance
  - Vendor Costs will Vary
  - Breach Fall-Out

Are we at Risk?

- Employee Information
- Payment Information
- Medical Records
- Any other record containing personal information



Data Breach Causes

Employee Error

- Know who has access to data
  - Limit access as much as possible
- Educate and train employees
  - Culture Change
  - Employee Awareness
- Stolen passwords
  - Use strong, unique passwords
  - Avoid password reset questions with answers easily found online

Insider and Privilege Misuse

- Know what data you have, where it is and who has access to it
- Only gather data you need
- Know where you need additional auditing and fraud-detection

Crimeware

- Patch anti-virus software (keep up to date)
  - 99.9% of successful exploitations used vulnerabilities for which software update patch fixes were available for more than a year
- Use two-factor authentication
  - eg: a bank card and a PIN; smartphone and a fingerprint
- **Educate and train employees**
  - **Avoid opening and responding to anything suspicious**

Physical Theft and Loss

- Encrypt your devices and sensitive data
- Run regular backups to prevent loss and downtime
- Allow for the wiping of device
- Make it easy for employees to report lost or stolen devices to mitigate the potential damage

Points to Ponder

- A data breach is not always a disaster, mishandling it is!
- 23% of recipients opened phishing messages and 11% clicked on attachments.
- On average, it's just 82 seconds before a phishing campaign gets its first click.
- Be vigilant!

We Think We Had a Breach, Now What?

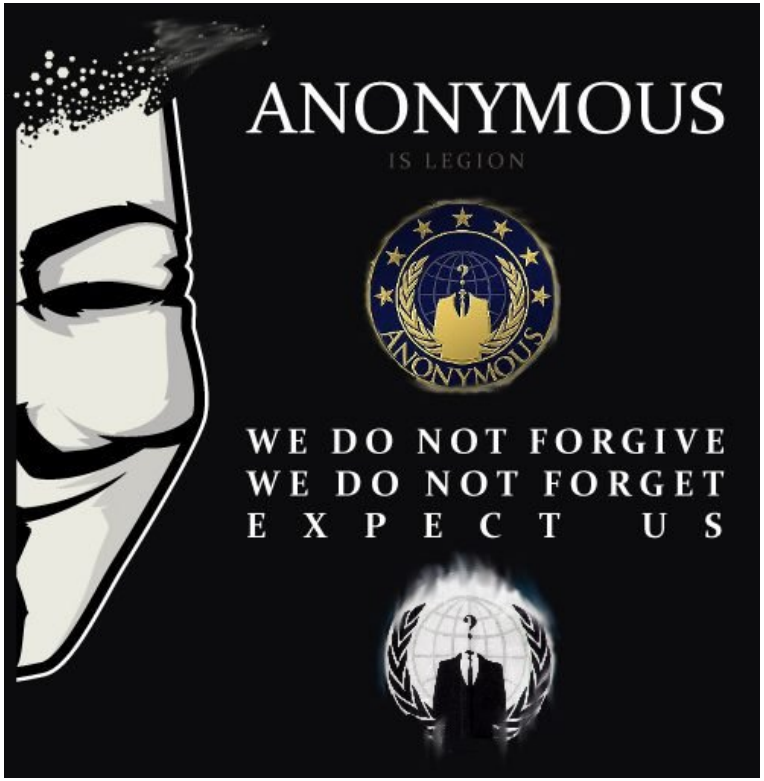
- First and foremost, do not panic
  - However, time is critical
- Investigate the potential breach
  - IT Forensics
- If a breach did occur, consult legal counsel regarding obligations
- Document, document, document

So where do we go from here?

Analyze Your Risk

- What kind of information do you collect and retain?
- How long do you retain personal information?
- Where is the information stored?
- Who has access to the information?
- Is the information located on a computer system?
- Do you have a data security policy?

Avoid/Eliminate



- Don't collect data, unless it is necessary
- Remove data as soon as you are able
- Restrict access to data to only those who need it
  - Data has become an asset **and a liability.**

Reduce/Prevent

- **Educate and Train Employees**
  - **78% of breaches could have been avoided with better practices and training (IDT 911, LLC)**
  - Email practices
  - Password practices
  - Eliminate work-arounds
  - Improve awareness

Reduce/Prevent (cont.)

- Be vigilant
  - Be on the look-out for odd activity
- Patch anti-virus software
- Encrypt sensitive data
  - Helps reduce/prevent breach costs
  - Not useful, if stolen
- **Run regular back-ups**
- Evaluate data disposal procedures

Transfer

- Effective 8/1/16, the NDIRF began including coverage for first and third-party data breach costs within its Liability Memorandum of Coverage
- $250,000 annual aggregate limit
- Option to purchase higher limits with additional underwriting
- Pricing is included in the annual Liability contribution

Multi-State Information Sharing and Analysis Center (MS-ISAC)

- **Free** cybersecurity resource for all local governmental entities

https://www.cisecurity.org/ms-isac

- Services include:
  - Incident response
  - Vulnerability assessments
  - Cyber threat intelligence
  - Suspicious email analysis

Questions/Comments/Concerns?

- Brennan Quintus
  - 701-751-9105
  - Brennan.Quintus@NDIRF.com