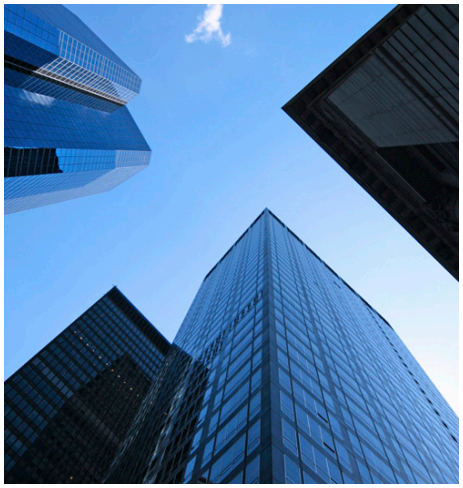
CLYDE&CO
US LLP



2012 Montana Government IT Conference

Cyber/Data Security 101: The Basics, Risks, Best Practices, and Response Procedures

December 6, 2012
Helena, Montana

Presented by Christina N. Terplan, Esq., and Paul G. Nikhinson, Esq., CIPP/US

CLYDE&CO
US LLP

Disclaimers

This presentation represents the presenters' independent opinions and are not to be construed as those of Clyde & Co or our clients

CLYDE&CO
US LLP

Who are we?

- Global law firm with over 1,400 lawyers operating from 30 offices in six continents
- Data Protection & Privacy
- Technology Errors & Omissions Insurance
- Risk Management

CLYDE&CO
US LLP

Overview

- The Risks of Information in the Digital Age
- Personal Information: What is it? Why is it important?
- Breaches of Personal Information: What is a "data breach" and how does one occur?
- Data Breach Examples: The Wall of Shame
- Sources of Liability
- Responding Appropriately to a Data Breach
- Risk Management and Breach Prevention

CLYDE&CO US LLP

What is the Risk?

- Theft, loss, or unauthorized disclosure of personally identifiable information or protected health information.
- State and local government agencies particularly vulnerable given:
  - Large amounts of sensitive data stored on residents and employees;
  - Increasing reliance on portable computing devices;
  - Very misplaced belief that cyber criminals interested only in financial institutions;
  - Relative lack of sophistication in IT systems compared to private sectors with a long history of cyber risk.

CLYDE&CO
US LLP

Identity Theft: The Market for Stolen Personal Information

- In 2005, 5.5% of U.S. households (about 6.4 million households) had at least one member age 12 or older experience identity theft victimization.
- Despite more media and law enforcement attention, by 2010, 7.0% of U.S. households (about 8.6 million households) had at least one member age 12 or older experience identity theft victimization.

See, Bureau of Justice Statistics – http://bjs.ojp.usdoj.gov/index.cfm?ty=pbdetail&iid=2207

- Large and sophisticated black market with shockingly low prices for personal information (supply > demand):
  - Credit card information (name, billing address, card-number, CVV2 code, and expiration date) = $1.50 – $3.00 per file.
  - Social security numbers = $1 – $6 per number, depending on availability of corresponding date of birth and/or mother's maiden name.
  - Online banking log-in details = $50 – $1,000.
  - SpyEye Trojan Kit (top on every aspiring hacker's holiday shopping list): $1,000 – $2,000.

See, RSA Anti-Fraud Command Center, RSA Online Fraud Report, August 20010: www.rsa.com/solutions/consumer_authentication/intelreport/11068_Online_Fraud_report_0810.pdf

General Categories of Personal Information

1. **Protected Health Information** ("**PHI**") – individually identifiable information related to treatment, health condition, or payment for health care services; and
2. **Personally Identifiable Information ("PII")** – Information capable of uniquely identifying an individual
   - Name plus one non-public identifier (e.g., SSN, DL number, date of birth, financial account information)
   - Even without a name, 87% of US citizens individually identifiable with gender, zip code, and date of birth

     (*Computational Disclosure Control, Latanya Sweeny, Ph.D., Carnegie Mellon University, 1997*)

Personal Information Under Montana Law

First name or first initial and last name of an individual **in combination with** any **one or more** of the following **data elements** when the name and the data elements are **not encrypted**:

- Social Security number or tax identification number;
- Driver's license's number, state identification number or similar identification number issued by any state, district or territory;
- an account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to a person's financial account.

Personal Information does not include public information lawfully made available from federal, state, local, or tribal government records.

What is a Data Breach?

- "Data breach" is a term of art and the precise definition depends on the applicable state and federal law(s).

- Data breach notification laws in 46 states, the District of Columbia, Puerto Rico, and the Virgin Islands. Trigger is individual's state of residence.

- Federal sector-specific laws (e.g., HIPAA/HITECH for healthcare and FERPA for student records) may also present separate breach reporting obligations, and apply to types of personal information not explicitly covered by the Montana statute.

When an "Incident" Becomes a Data Breach

The term “breach” has legal significance and the definition varies based upon a multitude of applicate statutes and federal laws. A potential cyber/data information incident should be referred to as an “incident” and not a “breach” until a final determination has been made by the Department of Administration and the state’s commercial insurance carrier.

In Montana, "data breach" means **unauthorized acquisition of data/information** that:

- **materially compromises the security, confidentiality, or integrity of personal information** maintained by a **state agency** or by a third party on behalf of a state agency.
- uniquely identifies an individual and may be of a sensitive nature.
- and **causes or is reasonably believed to cause loss or injury** to a person. Mont. Code Anno., §2-6-1501 through §2-6-1503, MCA. Note: **Risk of Harm** reporting threshold: What "materially compromises the security, confidentiality, or integrity of personal information" is open to interpretation in Montana. Attorney General guidance and court decisions will vary by state.

CLYDE&CO US LLP

Data Breaches: How is Personal Information Compromised

How Do Data Breaches Occur?

- Employee loses an unencrypted portable device (blackberry, laptop, thumb drive, backup tape)
- Property crimes (computers prime targets)
- Inside job (employee steals information, particularly upon separation with agency)
- Stray faxes, emails
- Phishing scams (the “Nigerian prince”), and increasingly, Spear-Phishing (social engineering)
- Malware / virus attacks (especially when working remotely on an unsecured network)
- Advanced Persistent Threats
- Failure to purge/scrub computing devices scheduled for destruction
- Weaknesses in "Cloud" security

Most Common Causes for Data Breaches in the Public Sector

See, Rapid7 Report Analyzing Privacy Rights Clearinghouse Chronology of Data Breaches. Available at: http://www.net-security.org/secworld.php?id=13553

CLYDE&CO
US LLP

The Wall of Shame…

Examples of Publically Reported Data Breaches

- **Department of Defense**: loss of a computer back-up tape by a DoD contractor compromised the protected health information, and social security numbers, of **4.9 million** active military personnel, veterans, and their families.
- **South Carolina Department of Revenue**: phishing attack resulted in theft of approximately **3.6 million** Social Security numbers and information on **387,000 credit and debit card** accounts.
- **California Department of Child Support Services**: Department contracted with IBM and Iron Mountain to conduct a disaster recovery simulation. Department sent the vendors four unencrypted computer backup tapes, containing personal information of **800,000** residents. The vendors returned the tapes via FedEx, but the package was lost in transit between Boulder and Sacramento.
- **Utah Department of Technology Services**: Brute-force attack compromised weak password and resulted in theft of **780,000** files on Utah residents and information related to sensitive healthcare services provided to children.
- **California Department of Social Services**: Department contracted with HP for offsite data management and warehousing. HP sent the State Insurance Fund several unencrypted microfiches via U.S. mail containing payroll data for **701,000** individuals. The package arrived damaged and with contents missing.

CLYDE&CO
US LLP

The Wall of Shame…

Examples of Publically Reported Data Breaches

- **South Carolina Department of Health**. An employee compiled data on more than **228,000** Medicaid recipients, including social security numbers, and emailed this information to his personal Yahoo account. The employee appears to have done so over at least a six-month period, and was only discovered via an internal investigation in connection with his work performance.

- **Northwest Florida State College**: Malware exploited security gap in systems over a period of four months, and extracted information on **279,000** students and employees, including social security numbers, employee direct deposit bank routing and account number information.

- Just the tip of the iceberg: in five out of every six breaches, the infiltration remained undetected for weeks at a time. *See*, "2012 Data Breach Investigations Report," Verizon Communications, at 3 (2012) (http://bit.ly/GFfpdk).

CLYDE&CO US LLP

What is the Exposure?

Direct Data Breach Costs in 2010

- $214 per compromised customer/client record
- $7,200,000 in average total per-incident costs (forensics, legal, notification, credit monitoring)

  (*U.S. Cost of a Data Breach Study, PGP Corporation and Ponemon Institute, 2011*)

Regulatory Investigations & Third-Party Claims

- Notification brings potential for AG regulatory action and provides plaintiffs' bar with tempting lure for putative class actions.
- South Carolina Department of Revenue:
  - Breach discovered October 10, 2012
  - Public notified October 26, 2012
  - First putative class action filed on October 31, 2012

CLYDE&CO US LLP

Step One: Notify RMTD

- Upon discovery or notification of the potential release of personal information, the state agency that maintains the personal information should notify the Risk Management & Tort Defense Division immediately at 406-444-2421.
- The immediate supervisor should assure that the 'Report of Incident' form is accurately completed, signed, and sent to the Risk Management & Tort Defense Division within two business days. http://rmtd.mt.gov/claims/agenciesreportclaims.mcpx
- Do not contact individuals whose information may have been released in the incident.
- In written correspondence, try to refer to the situation as an "incident" and not "a data breach."

CLYDE&CO US LLP

Step Two: RMTD Escalates as Necessary

- Internal investigation and reporting of incident to the State's cyber liability insurance carrier;
- Privacy counsel (attorney-client privilege and work product protections);
- Computer forensics expert;
- Public relations and crisis management consultant;
- Mailing/notification vendor (is your agency equipped to print and mail 5,000 notification letters? How about 50,000? 500,000?);
- Call center vendor;
- Credit monitoring
- **Timing is everything**: Notification (to the affected individuals) must be made **without unreasonable delay**, consistent with the legitimate needs of law enforcement or with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system. Mont. Code Anno., § 2-6-504(1)(b)
- Fixed deadlines in other states

CLYDE&CO
US LLP

Beazley: Cyber Liability Insurance

- Montana participates in a national cyber/information security insurance program underwritten by Certain Underwriters at Lloyd's, Syndicates 623 and 2623 ("Beazley").
- The Beazley policy includes, subject to certain limitations and exclusions, coverage for first-party data breach response costs, and third-party claims arising from the underlying incident.
- $2,000,000 Policy Aggregate Limit (for all coverage combined, including Claims Expenses)
- $500,000 Policy Aggregate Limit for Privacy Notification Costs (subject to a $100,000 per incident Retention); $1,000,000 Policy Aggregate Limit for Beazley Nominated Service Providers.
- Coverage for First Party Data Protection Loss and First Party Network Business Interruption Loss.
- Coverage is nice, but breach prevention should be the collective focus.

CLYDE&CO US LLP

Risk Mitigation & Breach Prevention: Best Practices

ATP (Administrative, Technical, and Physical)

- Administrative:
  - **Written Information Security Policy/Plan ("WISP")**
    - All state agencies and third parties to whom personal information is disclosed by a state agency shall develop and maintain:
      1. an information security policy designed to safeguard personal information;
         - downloads to personal devices?
         - emailing to personal accounts?

         and
      2. breach notification procedures that provide reasonable notice to individuals. Mont. Code Anno., § 2-6-504(4).
  - Regular and documented training of employees regarding information security
  - Access to data on a "need to know" basis
  - Privacy impact assessments for new technology
  - Contractual control over third-party vendors
  - Designated incident response teams

CLYDE&CO
US LLP

Risk Mitigation – Best Practices

- Technical:
  - **Encryption**
  - Limits in storage capacity on portable devices
  - Data loss prevention and detection software
  - NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf
- Physical:
  - Proper **security of facilities and physical hardware** assets
  - Proper purging of physical hardware scheduled for destruction

CLYDE&CO
US LLP

Risk Mitigation – Beazley Educational Materials

Beazley's "No Data Breach" Services

- Newsletter, webinars, sample policies, and other loss prevention information may be found at:
  - https://www.nodatabreach.com/cms/client/(S(tfphxh45hzeix13tcr5w5szc))/BeazleyDataLogin.aspx.
  - On your first visit to this website, click the "Register Now" link on the left side of the screen and enter:
  - First and last name
  - e-mail address
  - Password (create your own new password)
  - Select "Montana"
  - Enter this signup code JR904C10APPT 38
  - Click the arrow to begin
  - Submit your e-mail and password to log in
- Once logged-in, click the "Data Security Updates" link and that will take you to the "Data Security Updates" page where you can sign up for the quarterly newsletter by clicking on the "Subscribe to Our Newsletter" link.

CLYDE&CO
US LLP

Q&A

Questions?