Cyber/Data Information Security (FAQs)

Department of Administration

Risk Management & Tort Defense Division

October 10, 2023

Q: What is a cyber/data information security breach?

A: The laws vary by state, and federal laws may also apply. In general, under Montana law, "data breach" means the unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by a state agency or by a third party and causes, or is reasonably believed to cause, loss or injury (§2-6-501(1) MCA). The term 'breach' may be easily misconstrued and implies that the state was negligent; therefore, a cyber/information security situation should be referred to as an 'incident' and reported to the Risk Management & Tort Defense Division (RMTD) in accordance with the instructions found at https://rmtd.mt.gov/claims/agenciesreportclaims. RMTD will work with the state's insurance carriers to determine whether or not a 'breach' has occurred.

Q: What is personal information?

A: The laws vary by state but, in general, personal information means:

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 (i.e. SSN, DL number, date of birth, financial account information).
3) Under Montana law, "personal information" means the first name or first initial and last name 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 payer identification number; or
    - Driver's license number, identification card number issued pursuant to §61-12-501 MCA, a tribal identification number or enrollment number, or similar identification number issued by any state, district, or territory; or
    - An account number, 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; or
        - medical record information as defined in §33-19-104 MCA, or
        - an identity protection personal identification number issued by the United States internal revenue service.
    - Personal information does not include public information lawfully made available from federal, state, local, or tribal government records.

Q: What are the risks?

A: 1) It is estimated that 7% of U.S. households experience identity theft victimization of personal information annually.

2) There is a large and sophisticated black market with shockingly low prices for personal information such as:
    - Credit card information.
    - Social security numbers.
    - Online banking login details.

3) State and local agencies are particularly vulnerable given that they have:
    - Large amounts of sensitive data stored on residents and employees.
    - Increasing reliance on portable computing devices.

Q: What are some examples of federal and state government cyber/data information security breaches?

A: Federal offices and state agencies have experienced many breaches. To name a few:

- **Department of Defense**: loss of a computer back-up tape by a Department of Defense 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.

Q: What are some common causes of breaches?

A: Breaches most commonly arise from these activities:

- Loss of unencrypted portable device (blackberry, laptop, thumb drive, backup tape).
- Property crimes (computers prime targets).
- Inside job (employee steals information, particularly upon separation with firm).
- Stray faxes and emails.
- Phishing scams (i.e. “Nigerian prince”) and spear-phishing (i.e. 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.

Q: Does the state purchase or maintain cyber/data information security insurance?

A: The answer is ‘yes’. A brief summary of the state’s insurance coverage is hereby provided:

- Montana state government and the university system participate in a national cyber/data information security insurance program through a Lloyd's of London syndicate (i.e. "Beazley").
- The policy includes coverage for data breach response costs such as forensic investigation of the breach, mail notification, credit monitoring, regulatory fines and penalties, business interruption, and cyber extortion.
- The policy also provides coverage for damage to the state and university system’s digital assets as well as third-party claims arising from the underlying incident.
- Coverage is subject to a $12,000,000 annual aggregate limit but various limitations and exclusions apply; therefore, breach prevention should be the collective focus!
- For a more detailed summary of insurance coverage provided under the state cyber/data information security insurance policy, please visit the Risk Management & Tort Defense Division’s website at http://rmtd.mt.gov/insurance/cyberdatasecurityinsurance. Call us at (406)444-2421 if you have questions.

Q: How can breaches be prevented?
A: Breaches can be prevented through administrative, technical, and physical controls:

- Written information security plans
- Regular and ongoing information security training
- Access to data on a "need to know" basis
- Privacy impact assessments for new technology
- Contractual control over third-party vendors
- Encryption of desktops, laptops, and portable devices
- Limits in storage capacity on portable devices
- Data loss prevention and detection software
- Proper security of facilities and physical hardware assets
- Proper purging of physical hardware scheduled for destruction

Q: Does the state's insurance carrier provide any loss prevention resources?
A: Many resources are provided by state agency's and university system's technology staff. However, additional services are available through the state's insurance carrier, Beazley. Newsletter, webinars, sample policies, and other loss prevention information may be found at https://wwwbeazleybreachsolutions.com. On your first visit to this website, click "Register", use the activation code OpMxeQ, and follow the instructions.

To learn more about cyber/data information security laws, risks, insurance coverage, best practices, and incident response, you may view a video posted on the Risk Management & Tort Defense Division's website at http://rmtd.mt.gov/training/client.html. Please contact the division at (406)444-2421 if you have additional questions.