



Governor's Cybersecurity Task Force

**Monday, January 11, 2016
Roughrider Room
State Capitol Building**



Agenda

- November Meeting Highlights
 - *Lt. Gov. Drew Wrigley*
- Overview of Current Cybersecurity Laws
 - *Claire Ness, Office of the Attorney General*
- Overview of Cybersecurity Insurance
 - *Tag Anderson, Director Risk Management Office*
- Review Draft of Cyber Incident Response Plan
 - *Mike Ressler, State Chief Information Officer*
- Status of Current Cybersecurity Activities
 - *Dan Sipes, State Deputy Chief Information Officer*
- Closing Comments
 - *Lt. Gov. Drew Wrigley*



Overview of Current Cybersecurity Laws

Claire Ness
Office of the Attorney General



Overview of Current Cybersecurity Laws

- North Dakota State Law (NDCC 51-30-01) - breaches involving unencrypted personal information
- Health Information Portability and Accountability Act (HIPAA) - breaches involving unencrypted protected health information)
- Gramm-Leach-Bliley Act - breaches of financial institutions' sensitive customer information
- Family Educational Rights and Privacy Act (FERPA)



Overview of Current Cybersecurity Laws

North Dakota State Law (NDCC 51-30-01) - breaches involving unencrypted personal information

- Who must give notice of a breach and to whom?
 - Owners and Licensees of data that include personal information must notify state residents whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
 - If more than 250 individuals are impacted, the owner or licensee must also notify the Office of Attorney General.
 - Persons who maintain data that include personal information data must notify Owners and Licensees of the information if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.



Overview of Current Cybersecurity Laws

North Dakota State Law (NDCC 51-30-01)

- What is the time frame for giving notice?
 - Owners and licensees must give notice “in the most expedient time possible and without unreasonable delay...” Delays due to legitimate law enforcement needs (eg, for a criminal investigation) or necessary to determine the scope of the breach and repair the data system are not unreasonable.
 - Persons who maintain data must notify owners and licensees immediately upon discovery of the breach.



Overview of Current Cybersecurity Laws

North Dakota State Law (NDCC 51-30-01)

- How must notice be given?
 - Notice may be written.
 - Notice may be electronic if the individual to be notified has consented to receive electronic records.
 - If (a) the cost of providing notice would exceed \$250,000, (b) notice would need to reach more than 500,000 individuals, or (c) the notifying entity lacks sufficient contact information for affected individuals, substitute notice is acceptable. Substitute notice: email (to the extent email addresses are available), conspicuous posting on the notifier's website, and notification to major statewide media.



Overview of Current Cybersecurity Laws

North Dakota State Law (NDCC 51-30-01)

- How must notice be given?
 - Certain financial institutions and health care entities are deemed compliant with state law if they follow their industry-specific federal requirements for breach notification.
 - Persons who maintain and use their own notification procedures as part of their information security policies are deemed compliant as long as those procedures are consistent with the timing requirements of this state law.



Overview of Current Cybersecurity Laws

North Dakota State Law (NDCC 51-30-01)

- Who enforces breach notification requirements?
 - The Attorney General
 - Possible enforcement actions include but are not limited to: injunctions, subpoenas, civil penalties (\$5000 per violation), recovery of investigation and enforcement costs,



Overview of Current Cybersecurity Laws

North Dakota State Law (NDCC 51-30-01)

- Key Definitions:
 - Breach: generally defined as an unauthorized acquisition of computerized data when access to person information has not been secured by making it unreadable or unusable.
 - Personal Information: a person's first name or initial and last name in combination with any of several enumerated data elements (when the name and element(s) are not encrypted). Personal information does not include information that is lawfully available to the public.
 - Person: an individual, organization, government, political subdivision, or government agency or instrumentality.



Overview of Current Cybersecurity Laws

Health Information Portability and Accountability Act (HIPAA) - breaches involving unencrypted protected health information)

- Who must give notice of a breach and to whom?
 - Covered entities (and, under Federal Trade Commission rules, certain electronic health record vendors) must notify affected individuals and the Department of Health and Human Services when there is a breach of their unsecured protected health information.
 - If more than 500 individuals in any state or jurisdiction are affected, the covered entity must also notify prominent media outlets in the relevant state or jurisdiction
 - Business associates must notify covered entities of a breach of unsecured protected health information



Overview of Current Cybersecurity Laws

HIPAA - What is the time frame for giving notice?

- Covered entities must notify affected individuals without unreasonable delay and in no case later than 60 days following the discovery of the breach.
- For breaches affecting 500 or more individuals, covered entities must notify the media and Department of Health and Human Services without unreasonable delay and in no case later than 60 days following the discovery of a breach.
- For breaches affecting fewer than 500 individuals, covered entities must notify the Department of Health and Human Services no later than 60 days after the end of the calendar year in which the breach occurred.
- Business associates must notify covered entities without unreasonable delay and in no case later than 60 days following the discovery of the breach.



Overview of Current Cybersecurity Laws

HIPAA - How must notice be given?

- Notice to individuals may be by first class mail.
- Notice to individuals may be electronic if the individuals have consented to receive electronic records.
- Substitute notice must be given to individuals if a covered entity lacks current contact information for 10 or more individuals. Substitute notice in this case is given by posting it on the covered entity's home page for at least 90 days or by providing notice in major print or broadcast media where the affected individuals likely reside.
- Substitute notice may be given to individuals if a covered entity lacks current contact information for fewer than 10 individuals. Substitute notice in this case may be given by some type of alternate written notice, by telephone or "other means".



Overview of Current Cybersecurity Laws

HIPAA

- Who enforces breach notification requirements?
 - The Office of Civil Rights within the Department of Health and Human Services
 - The Office of Civil Rights can refer cases to the Department of Justice when there is a possible criminal violation of HIPAA.



Overview of Current Cybersecurity Laws

HIPAA

- Key Definitions:
 - Covered entities: health care providers who transmit electronic information in connection with certain transactions, health plans (including government plans) and health care clearinghouses
 - Business associate: a person or entity who provides services to a covered entity and creates, receives, maintains, transmits or accesses protected health information. A member of a covered entity's workforce is not considered a business associate of the covered entity.
 - Protected Health Information: generally, individually identifiable health information



Overview of Current Cybersecurity Laws

Gramm-Leach-Bliley Act - breaches of financial institutions' sensitive customer information

- GLBA requires certain financial institutions to develop security measures to protect customer information. The security measures must include response programs to deal with detected or suspected data breaches. Federal interagency guidance says response programs should include breach notification procedures. That guidance applies to financial institutions regulated by the Federal Reserve Board, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency or the Office of Thrift Supervision.



Overview of Current Cybersecurity Laws

Gramm-Leach-Bliley Act

- Who must give notice of a breach and to whom?
 - Financial institutions should notify customers of unauthorized access to and possible misuse of their sensitive customer information
 - Financial institutions should have contractual provisions requiring third-party service providers to have appropriate breach response programs that may include customer notification
 - Financial institutions should notify their “primary federal regulator” of incidents involving unauthorized access to or use of sensitive customer information
 - Financial institutions should notify appropriate law enforcement authorities of any breaches that qualify as “suspicious activities” under their regulations



Overview of Current Cybersecurity Laws

Gramm-Leach-Bliley Act

- What is the time frame for giving notice?
 - When an institution determines there has been unauthorized access to sensitive customer information and the institution determines misuse of the information has occurred or is reasonably possible, the institution should notify the affected customer(s) as soon as possible.
 - Customer notice may be delayed for criminal investigation(s) for as long as notification will interfere with the investigation(s).
 - Financial institutions should notify their primary federal regulator as soon as possible after becoming aware of the breach



Overview of Current Cybersecurity Laws

Gramm-Leach-Bliley Act

- How must notice be given?
 - Financial institutions must notify customers “in any manner designed to ensure that a customer can reasonably be expected to receive it.”
- Key Definitions:
 - Sensitive customer information: customer’s name, address or telephone number in conjunction with one or more of several enumerated data fields - or any combination of data fields that would allow someone to access a customer’s account



Overview of Current Cybersecurity Laws

Family Educational Rights and Privacy Act (FERPA)

- FERPA requires educational agencies and institutions to maintain the privacy and of personally identifiable information in education records but does not those agencies and institutions to undertake proactive breach notifications. Instead, educational agencies and institutions must record unauthorized disclosures of a student's personally identifiable information. The student (or his or her parent) may request an accounting of disclosures and thereby find out whether there has been a breach.
- Educational agencies and institutions must follow any applicable state or other laws requiring breach notification.
- The federal Department of Education issued guidance to educational agencies and institutions on establishing breach notification policies and procedures.



Overview of Cybersecurity Insurance

Tag Anderson
Director, Risk Management Office



Draft of Cyber Incident Response Plan

Mike Ressler
State Chief Information Officer



Draft of Data Disclosure Response Template

Validate the data breach occurred

- Examine the initial information and available logs to confirm that a breach has occurred.
- Agency staff need to identify the type of information disclosed, do not assume that every identified incident is always a breach of Personally Identifiable Information (PII) or Protected Health Information (PHI).
- If possible, try to determine the method of disclosure (internal/external disclosure, malicious attack, or accidental).



Draft of Data Disclosure Response Template

Assign an incident manager (agency employee) to be responsible for the investigation

- If Information Technology Department (ITD) discovers the disclosure, ITD will notify the Director of the agency who is responsible for the data along with their IT coordinator.
- Agency will assign a senior level manager, such as the agency business owner or an individual at an equivalent director level position, to serve as an incident manager to coordinate multiple organizational units and the overall incident response.
- Begin breach response documentation, determine the reporting process and coordinate the flow of information (create a time line of events) about the breach so further communication will be accurate.



Draft of Data Disclosure Response Template

Assemble incident response team

- Include representatives from management, agency public affairs, information technology, legal, risk management, finance, and possibly HR, for internal incidents in the incident response team.
- Contact ITD, if they are not already aware of the incident.
- Contact the Attorney General's Office.
- Contact Risk Management.
- Contact the Governor's Office.
- In concert with executive leadership and legal counsel, designate a single organizational representative (typically the incident manager) authorized to initiate and/or communicate breach details to any party, including the media and/or law enforcement.



Draft of Data Disclosure Response Template

Determine the status of the breach (ITD will assist)

- Immediately determine the status of the breach (is it active or is it post breach.) If the breach is active, take action to prevent further data loss by securing and blocking unauthorized access to systems / data and preserve evidence (computer logs/files) for investigation.
- Document all mitigation efforts for later analysis.



Draft of Data Disclosure Response Template

Determine the scope and composition of the breach

- Identify all affected data, machines, and devices.
- Conduct interviews with key personnel and document facts (if criminal activity is suspected, coordinate these interviews with law enforcement).
- When possible, preserve evidence (backups, images, hardware, etc.) for later forensic examination. Locate, obtain, and preserve (when possible) all written and electronic logs and records applicable to the breach for examination.
- Determine whether in-house resources or an outside service provider will conduct forensics. ITD may contact the Multi-State Information Sharing and Analysis Center (MS-ISAC), for their assistance in the forensics process.



Draft of Data Disclosure Response Template

Determine the scope and composition of the breach

- Work collaboratively with affected parties (ITD or outside hosting vendor) to secure sensitive data, mitigate the damage that may arise from the breach, and determine the root cause(s) of the breach to devise mitigating strategies and prevent future occurrences.
- Seek advice from agency legal counsel on the approved methods for protecting digital evidence, so that you are prepared and are able to properly preserve and document all evidence to ensure it can be used in a court of law, if necessary. This requires detailed recording and following proper collection, handling, storage, custody documentation, and destruction procedures (if applicable).



Draft of Data Disclosure Response Template

Determine whether to notify law enforcement

- If criminal activity is suspected, notify law enforcement and follow any applicable federal, state, or local legal requirements relating to the notification of law enforcement.
- Consult your legal counsel to examine any applicable federal, state, and local breach reporting requirements to determine which additional authorities or entities must be notified in order to satisfy compliance requirements.



Draft of Data Disclosure Response Template

Determine whether notification is appropriate and, if so, when and how to provide such notification

- Determine whether notification is warranted and when it should be made. Executive leadership at the senior technical and/or administrative level, in coordination with legal counsel, is the authority that should generally make this decision.
- Determine proper method to notify affected parties; letters, telephone calls, media, etc.
- Provide notification in a straightforward and honest manner; avoid evasive or incomplete notifications.
- If the breach represents a threat to affected individuals' identity security, consider providing credit repair, credit monitoring or identity theft protection services to mitigate the risk of negative consequences for those affected.



Draft of Data Disclosure Response Template

Determine whether notification is appropriate and, if so, when and how to provide such notification

- Work closely with public affairs or media relations staff to craft the appropriate media notification (mailings, emails, phone calls, etc.).
- Determine the need to notify legislators, board members, and advisory councils.



Draft of Data Disclosure Response Template

Notify the individuals / entities whose data has been disclosed

- Notify affected individuals whose sensitive information, including PII, has been compromised, as required by applicable federal, state, and local laws.
- Reach out to affected parties as soon as possible to notify them about the breach.



Draft of Data Disclosure Response Template

Collect, review, and finalize any breach response documentation and analyses reports

- Assess the data breach to determine the probable cause(s) and minimize the risk of future occurrence.
- Address and/or mitigate the cause(s) of the data breach.
- Solicit feedback from the responders and any affected entities.
- Review breach response activities and feedback from involved parties to determine response effectiveness.
- Make necessary modifications to your breach response strategy to improve the response process.



Draft of Data Disclosure Response Template

Collect, review, and finalize any breach response documentation and analyses reports

- Enhance and modify your information security and training programs, which includes developing countermeasures to mitigate and remediate previous breaches; lessons learned must be integrated so that past breaches do not reoccur.
- Prepare final report.
- Once investigative activities have been completed, safely store, record, and/or destroy (where appropriate) all evidence.
- Consider all alternatives to replacing or clearing compromised resources and machines, including the cost of remediation or rebuilding of the assets to an acceptable security level.



Current Cybersecurity Activities - Application Inventory

Agency	Name or acronym
Division	If applicable within your agency
Business Function	Short description such as Case Management, Unemployment Payments, etc.
Agency Contact	Primary application owner
System Short Name	If applicable; often an acronym
System Full Name	System title; without acronyms
Users	Internal (within agency), External (other agencies/partners), and/or Public
Data	Personally Identifiable Information (PII), Protected Health Information (PHI), Internal Use, and/or Public Use
Access	Internal via STAGEnet and/or external via the public internet
Authentication	None, NDGOV Active Directory, ND Login (LDAP), and/or Other
Developed By	ITD, Agency, and/or Other
Hosted By	ITD, Agency, and/or Other
Cost	Acquisition, Maintenance/Support, and Hosting



Current Cybersecurity Activities - Roles & Responsibilities

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness & Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes & Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies & Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Based on NIST Framework

- 5 Functions
- 22 Categories
- 97 Subcategories

NIST Controls

- 18 Control Families
- 225 Controls
- 669 Control Enhancements



Current Cybersecurity Activities - Roles & Responsibilities

Cybersecurity Roles and Responsibility Matrix

C=Consulted, I=Informed, A=Accountable (Manage/Architect), R=Responsible

Cybersecurity Framework Responsibility Matrix	Priority	ITD	Agency	Other
(PR-AC) PROTECT-ACCESS CONTROL				
PR.AC1 - Identities and credentials are managed for authorized devices and users - Infrastructure and Solution Selection		A R	C	
PR.AC1 - Identities and credentials are managed for authorized devices and users - Individual User ID Management and Monitoring		I	A R	
PR.AC2 - Physical access to resources is managed and secured - Data Center		A R		
PR.AC2 - Physical access to resources is managed and secured - Agency Facilities			A R	
PR.AC3 - Remote access is managed		A R		
PR.AC4 - Access permissions are managed		A	R	
PR.AC5 - Network integrity is protected		A R		
(PR-AT) PROTECT-AWARENESS AND TRAINING				
PR.AT-1 General users are informed and trained		A	R	
PR.AT-2 Privileged users understand roles & responsibilities		A R	R	
PR.AT-3 Third-party stakeholders (suppliers, customers, partners) understand roles & responsibilities		A	R	I
PR.AT-4 Senior executives understand roles & responsibilities		A	R	
PR.AT-5 Physical and information security personnel understand roles & responsibilities		A R	R	
(PR-DS) PROTECT-DATA SECURITY				



Current Cybersecurity Activities - Audits

- ITD SOC2 (Service Organization Controls) Audit
 - Performed by the State Auditor
 - Issued May 6, 2015
 - Will be presented at the LAFRC January 14, 2016
- State Auditor Specialized Security Audit
 - In progress - Began December 2015
 - ManTech is the Security Consultant



Closing Comments



THANK YOU!!!