The Nelson A. Rockefeller Center at Dartmouth College
The Center for Public Policy and the Social Sciences

The Class of 1964 Policy Research Shop

—Celebrating 10 Years of Service to New Hampshire and Vermont—

DATA SECURITY IN NEW HAMPSHIRE: IDENTIFYING TARGETS, VULNERABILITIES, AND BEST PRACTICES

Presented to the House Finance Committee

PRS Policy Brief 1617-12
July 11, 2017

Prepared By:

Tara Burchmore
Ashley DuPuis
Jay Raju
Rachel Scholz-Bright
Jeremy Washam

This report was written by undergraduate students at Dartmouth College under the direction of professors in the Rockefeller Center. Policy Research Shop (PRS) students produce non-partisan policy analyses and present their findings in a non-advocacy manner. The PRS is fully endowed by the Dartmouth Class of 1964 through a class gift in celebration of its 50th Anniversary given to the Center. This endowment ensures that the Policy Research Shop will continue to produce high-quality, non-partisan policy research for policymakers in New Hampshire and Vermont. The PRS was previously funded by major grants from the U.S. Department of Education, Fund for the Improvement of Post-Secondary Education (FIPSE) and from the Ford Foundation and by initial seed grants from the Surdna Foundation and the Lintilhac Foundation. Since its inception in 2005, PRS students have invested more than 50,000 hours to produce more than 150 policy briefs for policymakers in New Hampshire and Vermont.

Contact:
Nelson A. Rockefeller Center, 6082 Rockefeller Hall, Dartmouth College, Hanover, NH 03755
http://rockefeller.dartmouth.edu/shop/ • Email: Ronald.G.Shaiko@Dartmouth.edu

TABLE OF CONTENTS

EXECUTIVE SUMMARY

As the world has become increasingly digital, New Hampshire has stored more information online. Many of the New Hampshire state databases contain sensitive information about individuals, businesses, and property within the state. This report seeks to answer the question posed by Representative Neal Kurk of the New Hampshire House Finance Committee: How secure is the data stored by the New Hampshire government? By analyzing the current state of data security nationwide, cataloguing the assets and vulnerabilities of key data-storing state agencies, and engaging in comparative analysis of state data security policy, we aim to understand better the current risks and present viable policy alternatives—if necessary—to mitigate those risks.

1. INTRODUCTION

Globally, the growth in digital data storage has been substantial. Industry estimates predict a 4,300 percent increase in data generation globally by 2020, and expect over one third of this data to live or have passed through the cloud.[1] Simultaneously, the number of breaches has increased sharply. In the United States, the total number of data breaches—affecting both companies and governmental organizations—is growing, with 447 reported data breaches in 2012, 614 in 2013, and 783 in 2014. For state governments, the cost of these breaches is considerable. State governments have lost 111.5 million records of personal information since 2009, and each breach costs about 5.8 million dollars.[2]

The government of New Hampshire and other state governments have taken notice of the issue of data security. According to the National Association of State Chief Information Officers, data security is the first priority for state CIOs. These officers cite several main issues: 77 percent are worried about the increasing sophistication of threats, 64 percent feel that Information Technology (IT) funding is insufficient, 62 percent say there are not enough security professionals available, and 92 percent believe that low salaries are a problem for maintaining IT and data security employees.[3]

Despite these worries, in most states, security budgets have not increased substantially. The New Hampshire Department of Information Technology has an operating budget of 75 million dollars, and spends between one and two percent of this budget on data security. This is comparable to other states, with many Information Technology Departments dedicating only one or two percent of their budgets to security.[4] It remains to be seen whether, beyond some recent increases, New Hampshire will enact additional policies to raise financial outlays, though the state has also taken several other legislative steps to protect state data stores.

2. METHODOLOGY

The world of data security is continually evolving as technology advances and policymakers adapt to new issues. To understand better the data security landscape, we took a multi-method approach to examine what other states have done to address data security, how large-scale breaches have happened and how they can be prevented, and what the state of New Hampshire has done so far.

State by state comparisons were conducted in order to examine the approach to data security undertaken in New Hampshire alongside its peers. These analyses focused on both institutional structures and policy outputs related to data security. For structural assessments, states investigated were selected because they were identified as having well developed data security programs, including both preventative and reactive approaches. All states selected for comparison also have current statutes concerning data security. Information on structural arrangement was gathered from agency websites, reports, and expert interviews. Interviews were conducted with officials from state data security agencies, and addressed the responsibilities, sizes, standards, and roles of the relevant agencies. States selected for comparisons of data security policy were identified as similar to New Hampshire with respect to size, geography, demographics, and state governmental structure and budgets.

Equally important is an understanding of the mechanisms by which attackers gain access to data. The better we can understand the specific threats to data security, the better we can assess the effectiveness of policies and practices to protect it. Accordingly, we also examined state level data breaches and subsequent responses around the nation. First, we examined data on breaches from the Privacy Rights Clearinghouse from 2005-2017, and then systematically searched and examined state media and state government reports of breaches. We then further investigated four specific, large, and high-information cases of state-level breaches. When examining breach legislation, three questions framed the research:

1. How does the state define personal information and/or a breach in relation to information stored by government entities?
2. To which agencies do data security laws apply?
3. Under what circumstances must the state give notice of a breach? And to whom are such notifications given?

In addition to the state by state comparisons, we also examined existing data security practices in New Hampshire. The objective in this section was to determine who is in charge of overseeing data security, who responds to cyber breaches, and what initiatives have already been adopted in the state. The survey of the state was completed using information from agency websites and agency publications, as well as through a series of interviews with high-ranking data security officials in the state, including Commissioner Denis Goulet.

In addition to conducting interviews with government officials, cybersecurity consultants from the private sector were identified and contacted. These interviews were focused on discovering and correcting cybersecurity vulnerabilities. Finally, we examined recently-published data security recommendations from the National Governors Association.

3. BACKGROUND INFORMATION

The first half of this section provides a survey of the different types of data security breach legislation currently in place in New Hampshire, other states, and at the federal level. The second half outlines exactly what happens if a breach occurs and who is responsible.

3.1 Reactive State Data Security Legislation

The most extensive form of state data security legislation is reactive and addresses breaches and breach notifications. Such legislation exists in nearly every state, including New Hampshire. In New Hampshire, a breach of security is defined as "the unlawful and unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of personal information."[5] Breach legislation regulates "any person doing business in New Hampshire who owns or licenses computerized data that includes personal information."[6] In this context, "person" is defined broadly and includes people, corporations, trusts and many other entities. Individual "personal information" includes first and last name, social security number, license to drive, or financial account information.

To determine that a breach has occurred, the entity must confirm that personal information has been accessed without authorization. It must then perform a "risk of harm analysis" to determine that there is reasonable probability of misuse of this data. When encrypted data is stolen, this is a noteworthy case in which risk of harm is not present. Encryption entails transformation "through the use of an algorithmic process into a form for which there is a low probability of assigning meaning."[7] Unless a translation password used to decode the encryption is also stolen in the breach, notification for a breach of encrypted data is not required.

When a breach is confirmed, entities are required to notify affected individuals and government regulators. This notification must be made as quickly as possible, unless a law enforcement or security agency determines that the notification "will impede a criminal investigation or jeopardize national or homeland security."[8] Notifications may be sent electronically, through writing, or by telephone. If the entity in question does not provide notification, individuals whose data may have been compromised have a right to take private legal action against the entity.

These elements of New Hampshire breach notification legislation are common across the country but not universal. Figure 1 below summarizes different elements of notification

legislation in other states. It includes the number of states in which a given law exists and whether New Hampshire is included.[9]

Figure 1. Breach Notification Requirements across States and in New Hampshire[10]

Breach Notification Requirement	Number of States With Requirement	Required in New Hampshire
Trigger Notification by Access	3	No
Require Risk of Harm Analysis	40	Yes
Require Notice to Attorney General or State Agency	28	Yes
Require Notification Within a Time Frame	10	No
Permit Private Cause of Action	17	Yes
Include an Encryption Safe Harbor	45	Yes
Trigger Breach in Electronic and Paper Records	10	No

This data shows that New Hampshire is roughly similar to or slightly ahead of other states in its notification legislation. It has passed every common condition (such as requiring a risk of harm analysis) as well as some of the less prevalent conditions that are only recently gaining prevalence (such as permitting cause of action). While New Hampshire is not at the cutting edge, it is also not lagging behind the nation as a whole in the reactive components of its data security legislation.

3.2 Preventative State Data Security Legislation

New Hampshire data security legislation is entirely reactive, regulating only how entities must respond to a security breach. In several other states, however, preventative legislation has been passed to standardize data security procedures. Two laws, passed in Massachusetts and Nevada, offer especially substantial preventative models.[11]

Passed in January 2010, the Nevada Personal Information Data Privacy Encryption Law was the first piece of state legislation to mandate personal data encryption. Shortly after, in March of 2010, the Massachusetts Data Protection Law became the second, including several additional preventative measures. The law requires that entities storing personal information maintain a "written information security program," or WISP, detailing physical, technical, and administrative procedures.[12] It also regulates the selection of

third-party security providers, limits collection of the data to the minimum required, and stipulates several computer system requirements.[13]

Both of these laws seek to standardize how entities secure personal data, and since their passing, other states have enacted similar laws. Twenty-six states have passed some form of preventative data security legislation, and such legislation is pending in several other states.[14] As of June 2017, however, there is no pending preventative data security legislation in New Hampshire.

3.3 Computer Crime Laws

States have also passed several forms of computer crime laws. This type of legislation addresses a variety of computer crimes including malware, spyware, and phishing, among others. As with preventative and reactive state data security legislation, there are no standardized policies or procedures across states and some states have been slow to adjust to new forms of data attacks.

There are three main types of computer crimes addressed by state policy. "Computer crime" is the most broadly defined term and covers malware, viruses, and other unauthorized attempts to access personal information. "Spyware" means collecting and tracking online activities by users. Finally, "phishing" is fraud by posing as a trustworthy entity to lure the transmission of personal or financial information.[15] There are also several newer types of attacks, such as ransomware, spoofing, and denial of service attacks that are growing in prominence but just beginning to gain legislative attention.

The table below shows how New Hampshire compares to other states in its computer crime laws. It lists the types of computer crimes that are addressed, as well as the number of states in which that legislation has been passed.

Figure 2. Computer Crime Legislation Categories Addressed Across States

Legislative Category	Number of States Addressing Category	Category Addressed in New Hampshire
Computer Crime	50	Yes
Phishing	23	No
Spyware	20	Yes

On this dimension New Hampshire is above average, though there are no pending proposals to address phishing in New Hampshire. It also remains to be seen whether

computer crime law will expand to include other attacks such as denial of service and ransomware.

3.4 Federal Data Security Standards

State agencies are expected to comply with a number of standards related to the management and use of various data sets. These compliance requirements are typically based on statutory or regulatory directives promulgated by a governing body. The State's Department of Information Technology (DoIT, described in section 3.5.1 below) partners with state agencies in regular audits and assessments of the IT infrastructure to support compliance with specific standards.

Standards from the Federal Bureau of Investigation's Criminal Justice Information Services (FBI CJIS) outline the security precautions that must be taken to protect sensitive information like fingerprint and criminal background data gathered by local, state, and federal criminal justice and law enforcement agencies. Standards from the U.S. Department of Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act (HIPPA) require both the protection of individually identifiable personal health information and medical records and the security of personal electronic health information and records. Related, standards from HHS and the Centers for Medicare and Medicaid Services (CMS) under the Minimum Acceptable Risk Standards for Exchanges (MARS-E) of the Patient Protection and Affordable Care Act (ACA) define a risk-based security and privacy framework for use in the design and implementation of health insurance exchange information technology systems for which CMS has oversight responsibility.

Beyond the health and criminal justice contexts, a range of standards also exist for financial information. The Safeguards Program from the Internal Revenue Service (IRS) is responsible for ensuring that agencies receiving federal tax information protect it as if the information remained with the IRS. The Program, which undergoes periodic review, emphasizes the confidentiality of return information, employee awareness, information disposal, secure storage, and computer security. Though non-governmental, standards from the Payment Card Industry Security Standards Council (PCI DSS) encourage common data security measures for all entities involved in payment card processing. The Social Security Administration (SSA) also requires state and local data exchange partners to meet information security safeguards requirements. Finally, Section 508 of the Federal Rehabilitation Act requires that web-based applications be accessible to persons with disabilities.

There are also several federal proposals that would preempt state laws, create uniform breach notification procedures, require encryption and other security requirements, and standardize computer crime law. Most of this legislation has only been proposed in 2015 and 2016, and has not made significant legislative progress. Only one proposal, the Cybersecurity Information Sharing Act of 2015, has passed in the Senate. This law would

modify breach notification procedures in New Hampshire, formally regulating communication between private companies and federal organizations in the event of a breach, but it lacks the scope of some of the other proposals. It is unclear how many, if any, of these additional federal proposals will pass. For now, many data security procedures will continue to be decided at the state level.

3.5 New Hampshire Data Security Structure

To assess the approach to data security undertaken by New Hampshire relative to other states, we describe the status quo in the state below, including descriptions of the primary agencies and actors.

3.5.1 The New Hampshire Department of Information Technology

Unlike large states like Texas, the executive branch of the New Hampshire government has a single information technology department, the Department of Information Technology (DoIT) that "manages and coordinates all technology resources in the executive branch of government."[16] This structure aims to reduce complexity and costs, and to ensure that all IT policies and standards are adhered to by every state agency.

Within the DoIT, day-to-day data security operations are run by the IT Security Group (ITSG). The scope of the agency is broad and it performs a number of crucial data security functions, including information risk management, strategy, incident response management, monitoring, standard-setting, infrastructure guidance, and security awareness outreach.[17]

The ITSG has six staff, in addition to the commissioner of the DoIT, Denis Goulet.[18] It is tasked with protecting crucial networks, systems, and data of the state government and is concerned primarily with data from state residents, including credit card, social security, and healthcare information. As such, it maintains a close relationship with the other departments, especially the Department of Health and Human Services.

3.5.2 The New Hampshire Cybersecurity Integration Center

The New Hampshire Cybersecurity Integration Center (NHCIC) was created in 2016 through an executive order issued by Governor Maggie Hassan.[19] Previously, cybersecurity operations were being run in multiple places and jurisdiction overlapped, and it was unclear when people were supposed to report security breaches or what they should report.[20] From 2016 on, the NHCIC was to be the single cybersecurity operations entity for the government of the state. Any and all cybersecurity incidents are to be reported directly to the agency.[21] Importantly, potential cyber incidents must be reported "immediately and completely."[22]

Once a breach is reported, the NHCIC will "review the incident information reported, engage those necessary to analyze impact, determine next steps based on the nature of the incident, coordinate response activities, and track efforts."[23] The executive order specifies that in the event of a breach, the NHCIC is to work closely with the New Hampshire Information Analysis Center (NHIAC), operated by HSEM and the state police, whose role is to share relevant information with other local, state, or federal institutions. For instance, the NHIAC will inform the FBI if a cyber breach in New Hampshire appears to be a linked to a larger national breach or serious of breaches. Its full role is explained in section 4.4 below.

The NHCIC is located at the Incident Planning and Operations Center (IPOC), which is operated by Homeland Security and Emergency Management. It integrates employees from various agencies, "whose shared responsibilities include the monitoring of networks, sharing of information and situational awareness, and coordination of response, mitigation, and recovery efforts to protect against cyber-attacks and secure private personal information."[24] The executive order also establishes the Executive Oversight Committee (EOC). The role of the EOC is to "oversee the operations of the NHCIC and the implementation of its strategic plan and governance."[25] As such, each agency of the executive branch of government must appoint one representative to the EOC.

3.5.3 Homeland Security and Emergency Management

New Hampshire Homeland Security and Emergency Management (HSEM) is responsible for coordinating state responses to major emergencies. It follows the National Incident Command System (NIMS) model, putting organizational structure into the management of the incident and coordinating conference calls, flow of information, span of control, proper reporting, and documentation.[26]

In the event of a cyber incident (reported to HSEM by the NHCIC), the agency will coordinate activity between the breached agency, the DoIT, and the state police. Generally the DoIT will handle the response to the incident (for instance, protecting data and restoring networks.) while the state police will investigate to determine if a crime has been committed and determine culpability, often with the help of federal agencies such as the FBI. The full role of the state police is explained in section 3.5.5 below.

3.5.4 New Hampshire Information and Analysis Center

The New Hampshire Information and Analysis Center (NHIAC) is "a cooperative effort under the New Hampshire Department of Safety between the New Hampshire State Police and New Hampshire Homeland Security and Emergency Management."[27] The NHIAC is a fusion center, one of 78 such centers that were founded after 9/11 to facilitate multi-jurisdictional information sharing. The Center "gets the right information to right people at the right time, while protecting individuals' privacy and civil liberties."[28]

In the event of a cyber incident, the NHIAC is involved in the "threat piece."[29] It works with agencies such as the FBI to locate the threat and determine who else needs to be notified at the federal, state, or local levels. For instance, a breach in New Hampshire could be part of a larger series of breaches in the country. The NHIAC would then coordinate with federal agencies and other IACs to share what tactics were used in the breach, what responses were most effective, and any other relevant information about the threat.

3.5.5 State Police

The State Police are involved in any criminal part of an investigation. Their role is to investigate the breach and determine who was responsible and what, if any, actions can be taken to address the crime. They maintain a close role with the NHIAC and are also involved in discussions between federal officials and agencies from other states, since breaches in the state can be part of a larger national event or series of events.

3.5.6 Summary of Agency Roles

In the event of a breach, the following agencies each play crucial roles:

Figure 3. Summary of Agency Roles in New Hampshire Data Security Breaches

Agency	Roles
Department of Information Technology	● Day-to-day data security operations (monitoring systems, making back-ups, etc.) ● Coordinating the technological response to the breach (restoring networks, mitigating damage, etc.) ● Providing technological advice to other IT departments (not from the executive branch)
Cybersecurity Integration Center	● Receiving and evaluating the initial report of the cyber incident and contacting relevant parties.
Homeland Security and Emergency Management	● Coordinating the response to a cyber incident (creating planning cells, putting relevant agencies in contact, etc.)
Information and Analysis Center	● Contacting relevant fusion centers in other states and federal authorities (if necessary). ● Staying informed about ongoing threats and other cyber events nationwide.
State Police	● Determining a crime's occurrence and responsible parties

4. STATE BY STATE ANALYSIS

The National Conference of State Legislatures released an analysis of state data security legislation in 2017. The following states were identified as having well developed data security programs: Arizona, Colorado, Idaho, Mississippi, Ohio, Oklahoma, Oregon, South Carolina, Texas, Utah, Virginia, and Washington.

4.1 Structural State Comparisons

These twelve states require by statute that governmental agencies within the state have specific policies or measures to ensure the security of their data.[30] Figure 4 groups these states (as well as New Hampshire) by type of data security structure.

The three primary state data security organizational structures in evidence are states with a single in-state agency with primary responsibility for all data, states with an external non-governmental organization with primary responsibility for all data, and states where each agency has primary responsibility for its own data.

Figure 4. State Data Security Organizational Structures

Type of Structure	States With Structure	Commonalities Across States
An in-state executive agency is in charge of monitoring and protecting all state data	New Hampshire, Colorado, Idaho, Mississippi, Ohio, Oklahoma, Utah, Virginia	Mid to small sized, spread across the country
Non-governmental organization used to regulate government-held data	Arizona, Oregon, Washington	Mid-sized, western, technologically advanced
Each governmental agency and department monitors and controls its own data, often following national regulations	Texas	Larger state in terms of population, land, and budget

4.2 Interviews of State Data Department Representatives

In order to gain additional information about states representing the different structural arrangements noted above, phone interviews were conducted. The following questions were asked of the interviewees:

- What's this office's responsibility? How do you carry it out?
- How large is your office? Is it large enough to carry out what you need to?
- How has and does this office affect Data Security?
- How did you create your standards?
- What data do you prioritize?

Summaries of information gathered from Texas, Arizona, and Washington follow below.

The Texas Department of Information Resources provides data status services and IT help, but its primary service and focus is on cyber security. The department contains 198 individuals, but the representative with whom we spoke stated that they could use "more help to achieve projects." The Department of Information Resources sets data policies on a regular basis. Texas has a federated governmental structure, in which every department has their own information technology department and officer. The Department of Information Resources works to set the policies which these smaller departments follow and implement. They utilize the National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53), a catalogue of US federal information systems developing standards, guidelines, and publications to assist federal agencies in data management.[31]

In Arizona, the relevant agency, Arizona Strategic Enterprise Technology (ASET), was formed in 2011 and focuses on modernizing the way the state's data is stored and protected. Its three goals are: (1) performing cybersecurity exercises with state agencies with state-provided training for government employees, that agency representative Mike Lettman noted as the most important component, as without this crucial training, there is no real sense of data security; (2) modernizing technological infrastructure through working with the State Data Center, which facilitates sharing data; and (3) creating standards and enforcing policies. When looking at these objectives in an actual department within the state, many of them fail to be realized or lack efficacy, underlining a gap between policy and implementation. In the Department of Economic Security, various IT security processes have been established to protect data. The department identified potential weaknesses in its information security program by performing common attack patterns. While this department has been able to take such steps regarding data security, it still lacks an information security program as required by state policy and the ASET office.[32]

In Washington, the relevant agency, Washington Technology Solutions, focuses on data modernization and improved data security as one of many goals of the organization. Its customers include state agencies, counties, cities, tribal governments, and nonprofits, to which it provides network consolidation (bolstering consistency across agencies), creates more accessible data systems for people who need government data, moves more data to the cloud, and builds and develops statewide antivirus, data loss prevention, and firewall services. Despite its ".gov" webhost, this agency is not a direct part of the government of Washington State, and lists the Office of Privacy and Data Protection, the Office of the Chief Information Officer, and the Office of Cybersecurity as its partners.[33]

4.3 Investigation of Comparable States

From the initial state investigation, data security approaches in Idaho, Mississippi, Utah, Nevada, and Maine were identified to be most similar to data security in New Hampshire in size, technological advancement, and structure. Accordingly, we further investigated approaches in these states to compare with New Hampshire.

In July 2015, Idaho Governor Butch Otter signed an Executive Order creating the Idaho Cyber Security Task Force, chaired by Lt. Gov. Brad Little and containing representatives from the Idaho Bureau of Homeland Security, Idaho State Police, Department of Administration, Tax Commission, Idaho Transportation Department, Idaho Department of Health and Welfare, as well as representatives from colleges, universities, and other agencies throughout the state. The task force works with business and industry experts, similar departments in different states, and national cyber security strategists. In January 2017, Governor Otter signed an Executive Order enacting the recommendations of Idaho's Cybersecurity Task Force, performing the following actions to enhance their security. In order to further develop its internal data security programs, New Hampshire may wish to implement some of these actions within the state, such as:

1. Appointing a statewide Director of Information Security to oversee implementation of all cybersecurity policies
2. All state agencies must adhere to NIST Cybersecurity Framework to support risk and cybersecurity management before June 30, 2017
3. Executive branch agencies need to implement the first five CIS Controls before June 30, 2018
4. The State Department of Administration must facilitate annual vulnerability tests and scans and provide them to the Director of Information Security
5. The State Division of Human Resources must expand and review the cybersecurity curriculum for state employee training
6. All executive branch agencies must develop employee education plans
7. All executive branch agencies must require their employees to complete annual cybersecurity training
8. The State Department of Administration and the Director of Information Security must create and maintain a statewide cybersecurity website facilitating intelligence sharing and sharing information about cybersecurity best practices

9. The Director of Information Security must develop a public outreach program for local government, private businesses, and residents to share practices and information.
10. All public state agency websites to include a link to a statewide cybersecurity website, like www.cybersecurity.idaho.gov[34]

Mississippi releases a biennial Strategic Master Plan for Information Technology, most recently published in late 2016 presenting policy for 2017-2019. Its primary goals for 2017-2019 are improving intergovernmental information sharing, employing more flexible technologies, developing the skills of its information technology workforce, and finding solutions to attack the evolving threat of accessed data. Information Technology in Mississippi collaborates across state and governmental agencies to manage and deliver statewide information technology services.[35]

The Chief Information Officer in Utah is mandated to create an executive branch strategic plan addressing the exchange of information between in-state agencies, coordination in information technology systems development and maintenance, and protection of the data of state system users. The present plan covers 2017-2020 and allows government leaders to understand and prioritize the technological innovations they can use to their advantage. The Utah Department of Technology Services establishes specific regulatory compliance objectives for the protection of the public and of agencies. These policies are in conjunction with National Institute of Standards and Technology (NIST) standards. The Department of Technology also works to support a more data-driven government, improving and implementing new data warehouse and business intelligence support.[36]

The primary concern in Nevada in the field of information technology aligns with its present reduced state revenue. Recognizing the importance of having up to date and effective technology, one of its current goals is to use all technology funding as productively as possible in order to maintain a level of technological advancement and invest in upgrades and personal training. With this budget challenge, its priorities include improving productivity and efficiency of agencies and infrastructure while reducing expenses. IT in Nevada is currently quite decentralized, as every agency controls its own information technology environment. Enterprise IT services provides agencies core infrastructure, but agencies are not required to take advantage of these opportunities. Nevada is striving to move toward a state cloud model of information technology service, consolidating services with the goal of increasing security.[37]

Maine possesses a Standing Committee within its Judicial Branch called the Information Technology Governance Committee, whose role consists of assessing information technology projects, deciding which to prioritize, working with the Office of Information Technology to create project management methodology, and ensuring technology meets the needs of the court system.[38]

4.4 State by State Breach Legislation

Figure 5 below presents an overview of legislation in place to respond to data breaches, both of business and state data, in the states that were initially identified above. All legislation mandates that the state or affected non-governmental organization investigate any breach and notify the affected residents.

4.5 Data Breaches and Responses in Other States

In the past decade, almost every state has experienced at least one breach of government data. Some of these breaches have arisen from malicious hacking of and malware installation on government systems and databases, while others have stemmed from loss or theft of physical, data-containing devices. Information about data breaches from the Privacy Rights Clearinghouse, a non-profit data privacy watchdog group, from 2005 through 2017, and from a systematic search of publically available state government reports and media reports on these breaches, yielded information on likely areas of weakness and common causes of state-level breaches.[39]

Figure 5. Breach Legislation in Comparable States

State[40]	Definitions of Key Terms	Groups to Which Law Applies	Notification Logistics
Mississippi	"Breach of security" means "unauthorized acquisition of electronic files, media, databases or computerized data containing personal information of any resident of this state when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable"	Any business or governmental body experiencing a data breach	Affected individuals must be notified after criminal investigation, including of the scope of the incident and identities of the affected individuals. Notice is not required if the investigation proves the breach is not harmful

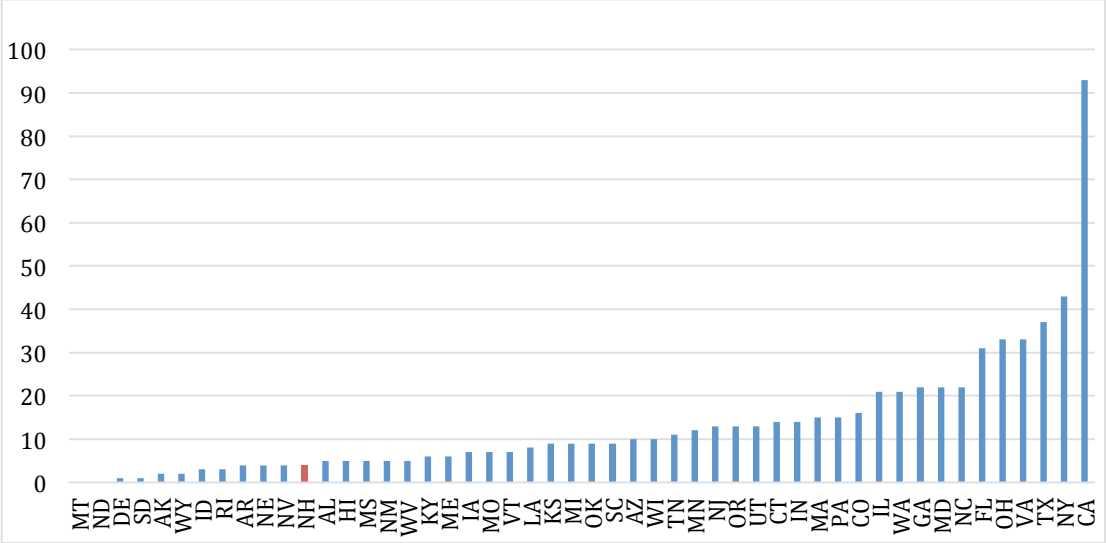
Utah	"Breach" is "an unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal Information"	Any in-state "data maintainer"	After investigating possible compromise, the data maintainer must notify affected residents if there is "reasonable suspicion." Notification must come "without delay," ideally via first class mail or phone. Notification can be delayed if law enforcement deems that notification will impede a criminal investigation.
Nevada	"Personal Information" includes usernames, emails, passwords, security questions, and medical identification number. "Data encryption" is identified as "the protection of data in electronic or optical form"	Any governmental agency, corporation, institution of higher education, or business entity that collects or maintains nonpublic personal information, defined to include names, social security numbers, driver's license numbers, or credit card numbers	When a data collector reasonably believes that unencrypted personal information has been acquired by an unauthorized person or organization, they must notify those affected in "in the most expedient time possible and without unreasonable delay"

Maine	*No relevant definitions*	"Information brokers"	Conduct reasonable and prompt investigations after reasonable suspicion of a breach. If there is reasonable suspicion of unlawful acquisition, they must notify the people immediately following the discovery of data access. Notification can be delayed if law enforcement is enacting a criminal investigation. If the data breach impacts over 1,000 people, consumer reporting agencies must also be notified, as well as state regulators

4.5.1 Overview of Number and Types of Breaches

Since 2005, there have been over 660 breaches of state government data (Figure 6).[41] These breaches have ranged in size from releases of dozens of records to millions of records.[42] The most common cause of these breaches was unintended disclosure, which was the cause of nearly 200 breaches (see Figure 7). Unintended disclosures include sending sensitive data to the wrong party, unintentionally posting it publically online, or other cases where data is mistakenly released through means other than hacking. Unintended disclosures are generally caused by user error or software malfunctions.

Figure 6. Number of Data Breaches in Each State from 2005 to 2017



The next most common cause of breach is loss or theft of portable or stationary, data containing devices, such as USB sticks, computers, hard drives, or tablets, which accounted for nearly 180 breaches.[43] Intentional hacking caused over 100 breaches, and insider misuse, when users with access to data intentionally misuse or breach data, accounted for another 70 breaches.[44] Aside from hacking, a large percentage of these breaches are caused by human error, either through loss of hardware or misuse of software. The following subsections highlight the causes of several major state-level breaches, as well as recommendations and lessons learned in their wake.

4.5.2 California

California produced a comprehensive report examining the causes and effects of data breaches that occurred in the state from 2012 to 2016.[45] The report found that government breaches accounted for five percent of the total breaches, and of those breaches, malware and hacking was the cause of 15 percent, physical breaches for 32 percent, misuse of data by employees for 3 percent, and miscellaneous errors, such as delivery of information to the wrong recipient, insecure data disposal, accidental posting on the web at 50 percent.[46]

Figure 7. Categories of Data Breaches

Breach Type	Description	Examples	Preventative Measures
Unintended Disclosure	Occurs when sensitive information is unintentionally released	• Posting databases online without the necessary security • Sending sensitive records to the wrong recipient • Improper disposal of data or physical records	Implementing clear protocols for release of information to prevent mistakes, ensuring only authorized users have the access necessary to release data
Loss or Theft of Device	Occurs when an information containing device, such as a laptop, hard drive, USB stick, or other device, is either lost or stolen	• When transporting a portable device, the device is lost • An unauthorized person enters an office and steals a computer	Implementing clear security protocols for entry and exit from buildings, and for removing and transporting data containing devices
Intentional Hacking	Occurs when an outside agent gains unauthorized access to sensitive, electronic records	• Phishing schemes in which emails are sent to users claiming to be from a reputable source in an attempt to cause a disclosure of passwords or other information • Viruses and malware • Cracking passwords to gain access to online databases	Deploying cybersecurity measures such as encryption or firewalls, training users to avoid phishing schemes and downloading viruses
Insider Misuse	Occurs when an authorized person uses sensitive records for unintended purposes	• Authorized user steals credit card information or social security numbers • Authorized user intentionally gives access to unauthorized users	Minimizing the number of authorized users and making clear what constitutes misuse of data, creating monitoring processes to ensure that authorized users are not misusing data

The report made several suggestions for how to improve data security in California, including measures targeted at both improving cybersecurity and user-centered improvements. These recommendations fell into two broad categories: user-centered and technology-centered. User based improvements include better training on how to avoid phishing, how to update and use adequately secure passwords, limit user privileges and access to data, and how to train staff and contractors on security measures. Improvements centered on cybersecurity include blocking vulnerable access points, continuously updating and patching software as vulnerabilities become known, and carrying out tests of network and database security.[47]

Figure 8. Recommendations from 2016 California Data Security Report[48]

User Focused	Cybersecurity Focused
• Inventory and monitor location of all devices • Inventory all software • Control who receives administrative privileges • Controlled access based on need to know • Account monitoring and control • Physical security • Security skills training for users • Incident response and management	• Secure configurations for hardware and software on mobile devices, laptops, workstations and servers • Continuously assess vulnerabilities and address them • Email and web browser protection • Malware defenses • Conduct and analyze audits • Data recovery capabilities • Wireless access control • Access monitoring and control • Penetration tests

4.5.3 South Carolina

A recent breach in South Carolina also occurred because of human error, but in combination with malicious hacking. In 2012, the South Carolina state department of revenue was breached due to a phishing attack, which revealed the social security numbers of 3.6 million residents, as well as the credit card information of hundreds of thousands.[49] That breach catalyzed an investigation into how South Carolina's data security could be improved, as well as the implementation of new breach notification and other data security laws.[50] The recommendations resulting from that breach included developing statewide information security practices, increasing collaboration with outside agents with sophisticated cybersecurity capabilities, and developing a statewide data loss prevention program in the case of a future breach (see Figure 9).[51] Some of the recommendations have been implemented, such as clearer breach policy, stricter security measures, hiring specific personnel to oversee information security, conducting regular audits, and mandatory privacy and data security training for employees.[52] However, according to the Department of Revenue Director Rick Reames, "this is a constantly

changing game. The criminals are always changing their tactics and we have to. It would be foolish to predict that there would not be another event."[53]

Figure 9: Deloitte Report Recommendations on South Carolina's 2012 Breach[54]

User Focused	Cybersecurity Focused
• Create a data awareness and training program • Create Chief Operations Officer, Chief Information Security and Chief Privacy Officer positions • Develop a professional development program to attract and retain information security personnel • Create an incident response team • Gather and centralize agency security plans • Establish a security compliance program	• Define security policy • Conduct risk assessments and create risk profiles for agencies • Implement threat monitoring and control • Implement secure network engineering • Develop cyber threat analytics and intelligence • Develop statewide metrics and monitoring • Automate security functions • Develop secure self-healing infrastructure

4.5.4 Texas

One of the largest recent breaches occurred in Texas in 2012, when the Texas Attorney General accidently released the social security numbers of 6.5 million residents to opposing counsel during a case challenging voter identification laws. The Attorney General did not realize that the database contained full social security numbers instead of only the last four digits, and when the mistake was realized, the disks were recalled and the analysts given the information were sworn not to use the data.[55]

Another large-scale breach in Texas occurred in 2011 when tapes containing information on 4.6 million military personnel were stolen from the automobile of a contractor. Both of these breaches occurred because of human error in handling sensitive data, and could easily have been prevented via more comprehensive security and monitoring of how authorized persons handle data.[56]

4.5.5 Utah

A breach of the Utah Department of Health occurred in 2012 and exposed approximately 780,000 records.[57] The breach happened because a Medicaid database was put online without changing the password from the factory default, so hackers were able to easily gain access to sensitive information, including social security numbers and health records. Addressing the effects of the breach cost the state nearly nine million dollars,

including nearly two million dollars on credit monitoring services for affected residents, and 1.2 million dollars on security audits of the state's system.[58] This breach reveals the ease with which security vulnerabilities can be exploited, and highlights the need for standardized procedures for data management. Mistakes that result in breaches are costly to remedy but through smaller investments before a breach occurs, they can also easily be prevented.

Breaches continue to happen across the US, including at least five major breaches since the beginning of 2017.[59] Breaches are likely to continue as hacking techniques become more sophisticated, but it is important to note that the majority of state government data breaches in the public record appear to stem from human errors. These breaches could be prevented through standardizing procedures and training authorized users on how to avoid phishing schemes, password security, and proper storage and transfer of devices containing sensitive information.

4.6 Comparison with New Hampshire

With respect to structure and infrastructure, the data security infrastructure in New Hampshire is similar to that of other small and mid-sized states. It has one agency that performs security operations for the entire government. This ensures consistency: all policies and practices will apply to every governmental agency. This is likely an effective structure for New Hampshire.

The NHCIC is also a unique collaborative initiative. A sub agency of the DoIT, the NHCIC is a collaborative effort between the DoIT and HSEM. Day to day, NHCIC is operated by the DoIT, but in the event of a large breach, HSEM can assume control and deploy the resources and personnel of the NHCIC.

With respect to employee training, according to Commissioner Goulet, it has been mandatory for all New Hampshire government employees for two years. According to HSEM Director Perry Plummer, private contractors have been used and are being used to test the effectiveness of state data security (including the effectiveness of employees). As noted in section 2.4, most breaches occur because of employee mistakes (unintended disclosure, loss of device, or insider misuse), so consistent and standardized employee training is crucial for effective data security.

With respect to best practices, the New Hampshire DoIT website publishes data security best practices. Many other states also do this, with the goal of sharing valuable security information with local governments, private businesses, and individuals. Some states (such as Idaho), have specific outreach programs to enhance this information sharing.

5. NATIONAL GOVERNORS ASSOCIATION RECOMMENDATIONS

For the year of 2016-2017, the National Governors Association (NGA) is completing a full assessment of state data security. The NGA has published a number of reports with information on best practices, recommendations, and other helpful information on state data security. Much of this information may be of use in New Hampshire. Key insights from the NGA reports are outlined in this section.

5.1 Cyber Liability Insurance for States

Even if the best practices for protecting state data are instituted, occasional cyber-attacks are inevitable, and even a misplaced laptop can trigger costly response procedures. To reduce the costs of these incidents, many insurance companies now offer cyber liability insurance. Purchasers pay a regular premium in exchange for a commitment by the insurer to absorb the costs of cyber incidents.[60] These agreements typically have three components:

1. First-party coverage: direct costs such as database recovery, customer notification, and forensic investigation
2. Third-party coverage: indirect costs such as litigation or regulatory fines
3. Exclusions: allowing the insurer to avoid payment in predefined scenarios such as nation-state cyber attacks

For states considering purchasing cyber liability insurance, the NGA makes several recommendations:

- The SERFF Filing Access System provides sample agreements to help states get a better understanding of how the insurance policies are structured and what type of coverage is best for their interests.
- Because cyber threats are dynamic and rapidly changing, "states should negotiate for agreements that account for constant changes in techniques, tactics, and procedures."[61]
- If the insurer awards a policy to the applicant, certain cybersecurity practices will be required and deviance from these standards will void coverage. Therefore, "whatever cybersecurity controls exist as part of the insurance agreement should be integrated into technical, administrative, and organizational security controls throughout all state offices subject to the insurance policy."[62]
- Many security breaches are accidental, so states should negotiate for agreements that cover insider scenarios, including when fraudulent info is used to trick an employee.

5.2 Cybersecurity and Critical Infrastructure

Critical infrastructure facilities, such as transportation networks, telecommunications lines, and power lines, are essential to daily life in modern society. To link widely dispersed facilities and corporate offices and to control equipment remotely, utility

companies have become increasingly reliant on digital technology.[63] This has led to a number of security vulnerabilities.[64]

To respond to this threat, the NGA recommends the following steps for Governors:

- Most infrastructure is privately operated but delivers a public good, so cybersecurity measures are a matter of public policy. Governors should work with other governors and lawmakers to assess the effectiveness of cybersecurity regulation for utility companies.
- Ensure regular contact between homeland security advisors and leaders of state utilities so that cyber events can be properly managed. This is especially difficult since personnel of utility companies often lack security clearances for timely threat intelligence.
- Audit existing rules and practices, as utilities companies lack experience with cyber threats.
- Have a good response plan in place now, as implementing strong security in all utilities will likely take years.
- Include smaller utilities companies in discussions, as they likely cannot dedicate sufficient resources to cybersecurity.

5.3 Building a Cybersecurity Workforce Pipeline

Building, recruiting, and maintaining an effective cybersecurity workforce is one of the main cybersecurity challenges for state governments. The supply of skilled workers is low and the number of qualified teachers is limited, and the demand is extremely high for workers with the skillsets to fill cybersecurity roles effectively. These professionals frequently choose lucrative private sector positions over government jobs.[65] As such, the NGA recommends several steps for improving state cybersecurity workforces:

- Promote education in network analysis, hardware engineering, and general project management rather than simply computer science.
- Identify, establish, and promote mid-career training programs.
- Promote non-traditional conduits (such as coding boot camps) to credential people who lack formal academic degrees.
- Lobby to introduce relevant computer skills earlier in education.

5.4 Cybersecurity in the Education Sector

Educational institutions hold much of the same personal, health, and financial information as in other sectors, the theft of which can lead to "financial ruin, reputational damage, and online abuse for students and faculty."[66] Because academic culture promotes open access to information and schools often encourage students to use mobile devices on school networks, educational institutions often offer an enormous attack surface that can be difficult to secure. The NGA recommends several steps to improve cybersecurity in the education sector:

- Clearly identify how educational institutions fit into the state's current IT plans.

- Educate school executives on relevant cyber threats and how to help counter them, promoting tighter relationships between administrators and school security professionals.
- Separate open, public networks from sensitive ones.

5.5 Small Businesses and Cybersecurity

Small businesses across the United States store financial, health, and personal data on millions of Americans. Unlike large companies, they are usually unable to afford sophisticated cybersecurity solutions, making them a prime target for hackers. For many companies, the costs of these hacks can threaten closure.[67] There are several ongoing challenges to improving security in small business:

- Many small businesses operate without any dedicated IT staff.
- Thin margins make cybersecurity measures a luxury that most small businesses cannot afford.
- Even limited regulatory action or private litigation could drive small businesses into bankruptcy, so they often hesitate to report breaches.
- Regulation of small businesses would increase costs.

Thus, the NGA recommends several steps to governors:

- Design tax or insurance incentives to encourage investment in cybersecurity.
- Consolidate and disseminate training materials and guidance.
- Engage IT, cybersecurity, and legal services that would be willing to offer limited pro bono services to small businesses that need help implementing defenses or responding to attacks.
- Support small business cyber centers.

6. INTERVIEWS WITH CYBERSECURITY INDUSTRY PROFESSIONALS

Cybersecurity consultants from Praetorian, Greycastle, and SecurityScorecard were interviewed with a series of questions about discovering and correcting cybersecurity vulnerabilities. When asked what kinds of data are most vulnerable in systems, the consultants explained that this was an impossible question to answer: The consultant at Praetorian emphasized that system designers are inherently incapable of accurately judging the most vulnerable parts of their system, and that the critical paradigm for cybersecurity was that no countermeasure would completely stop all hackers from breaking in. “Humans can’t tell where vulnerabilities are, especially if they’re the defenders. The only way to find out [where protection is needed] is the aftermath of an attack.”[68]

SecurityScorecard, Praetorian and Greycastle all recommended the use of a penetration test (where a third party attempts to break into the system to outline the key security vulnerabilities that let them do so) to drive cybersecurity policy: “without a penetration test, you have no way of knowing how secure your system is,” explained the consultant at

SecurityScorecard.[69] The expert at Praetorian however, highlighted the problems with mandating tests without requiring further action. "We get many clients that simply take their [penetration] test results, which outline exactly the same vulnerabilities as the results from the year before, and do nothing with them." These policy-mandated tests accomplish nothing if they are not accompanied by changes in behavior, explained the expert at Praetorian.

The expert at Greycastle emphasized the non-digital components of cybersecurity. "Most data leaks are a result of poor employee training and a lack of knowledge about cybersecurity, rather than vulnerabilities in the electronic system," the Greycastle employee explained.[70] The Greycastle employee listed the theft of USB drives, the use of non-secure passwords, and the improper disposal of sensitive papers as vitally important to information security. "Those problems lead to just as many security breaches as the technical stuff," the Greycastle consultant asserted.

Finally, the Greycastle employee outlined three dimensions to data security that are important in determining vulnerabilities: confidentiality, availability and integrity. A piece of data is confidential if it is difficult for it to reach unauthorized people. A piece of data has integrity if it cannot be changed by unauthorized people. Lastly, a piece of data is available if it is protected against data loss either through hardware failure or malicious attack. Though it is difficult to identify vulnerabilities, it may be easier to determine which systems fall short on any of these three areas, explained the Greycastle expert.

7. CONCLUSION

This report analyzes the state of data security in New Hampshire. Interviews with New Hampshire officials responsible for maintaining data security provide information on the current state of the data security systems the state has in place. A state-by-state analysis of data security statutes and systems across the country, a compilation of information on government data breaches, and interviews with private-sector cybersecurity professionals provide potential best practices for the state to undertake.

Data security in New Hampshire primarily falls under the jurisdiction of the Department of Information Technology (DoIT), which manages day-to-day security operations and coordinating technological responses to data breaches. The DoIT's Cybersecurity Integration Center (NHCIC) is responsible for receiving and evaluating initial reports of cyber incidents and notifying relevant parties. Some states of similar size utilize outside organizations to monitor and protect their data. The Cybersecurity Integration Center aims to evaluate threats, develop security strategies, manage incident responses, and provide awareness and standards for security purposes. Similar to the other states investigated, NHCIC regulates when and what to report following a data breach.

Analysis of recent data breaches demonstrates that while cybersecurity is a crucial part of maintaining data security, a major first line of defense is user-based security. Most data

breaches occurred at least in part due to easily preventable human error. Developing trainings, protocols, and oversight mechanisms to monitor users would prevent a great deal of security vulnerabilities.

Recent publications by the National Governors Association also provide a wealth of information on data security best practices. Several of these recommendations are of use to New Hampshire: researching cyber liability insurance, ensuring the safety of state infrastructure, building a workforce pipeline, and improving policies and procedures in the education sector and for small businesses.

Interviews with private-sector cybersecurity professionals shed light on the difficulty in judging the most vulnerable parts of a data system until after an attack. The consultants emphasized the use of penetration tests (in which a third party attempts to break into the system) to reveal key security vulnerabilities.

Overall, while there is no single best solution to state data security issues, a range of specific and potentially-applicable suggestions emerged from our research that may benefit public officials and residents in New Hampshire.

REFERENCES

[1] http://www.marsd.org/cms/lib7/NJ01000603/Centricity/Domain/202/Big%20Data%20Exploding.pdf
[2] National Association of State Chief Information Officers, May 2016 Presentation: http://www.ncsl.org/documents/statefed/NASCIO_Presentation_May2016.pdf
[3] Ibid.
[4] Ibid.
[5] Baker & Hostetler, Data Breach Charts: https://www.bakerlaw.com/files/uploads/documents/data%20breach%20documents/data_breach_charts.pdf
[6] Steptoe & Johnson, Comparison of US State and Federal Security Breach Notification Laws: http://www.steptoe.com/assets/htmldocuments/SteptoeDataBreachNotificationChart.pdf
[7] Ibid.
[8] Ibid.
[9] Baker & Hostetler, Data Breach Charts: https://www.bakerlaw.com/files/uploads/documents/data%20breach%20documents/data_breach_charts.pdf
[10] Steptoe & Johnson, Comparison of US State and Federal Security Breach Notification Laws: http://www.steptoe.com/assets/htmldocuments/SteptoeDataBreachNotificationChart.pdf
[11] CSO Magazine, The security laws, regulations and guidelines directory: http://www.csoonline.com/article/2126072/compliance/the-security-laws--regulations-and-guidelines-directory.html?page=3
[12] Cameron G. Shilling, Privacy and Data Security: New Challenges of the Digital Age: https://www.nhbar.org/uploads/pdf/bj-summer2011-vol52-no2-pg28.pdf
[13] Tenable.com, Understanding The New Massachusetts Data Protection Law: https://www.tenable.com/blog/understanding-the-new-massachusetts-data-protection-law
[14] National Conference of State Legislatures, Trends in State Cybersecurity Laws & Legislation: http://www.ncsl.org/documents/taskforces/StateCybersecurityLawsLegis.pdf
[15] Ibid.
[16] New Hampshire Department of Information Technology. "IT Security Group." https://www.nh.gov/doit/
[17] Commissioner of the Department of Information Technology, Denis Goulet. "Department of Information Technology." Telephone Interview. 12 May 2017
[18] Ibid.
[19] Ibid.
[20] Ibid.
[21] Ibid.
[22] New Hampshire Governor Maggie Hassan (2016). https://www.nh.gov/news/documents/pr-2016-10-28-cybersecurity.pdf
[23] Ibid.
[24] New Hampshire Department of Information Technology. "New Hampshire Cybersecurity Integration Center." https://www.nh.gov/doit/cybersecurity/nh-cic/index.htm
[25] Ibid.
[26] Director of Homeland Security and Emergency Management, Perry Plummer. "Homeland Security and Emergency Management." Telephone Interview. 19 May 2017
[27] Ibid.
[28] Ibid.
[29] Ibid.
[30] http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws-state-government.aspx
[31] Representative of the Texas Department of Information Resources. "Expert Interview." Telephone Interview. 15 May 2017
[32] Representative of Arizona Strategic Enterprise Technology. "Expert Interview." Telephone Interview. 16 May 2017 and https://www.azauditor.gov/sites/default/files/17-104_Report.pdf

[33] Representative of Washington Technology Solutions. "Expert Interview." Telephone Interview. 15 May 2017
[34] http://www.idahostatesman.com/news/politics-government/state-politics/article126819104.html
[35] https://www.its.ms.gov/Documents/master_plan.pdf
[36] http://le.utah.gov/interim/2016/pdf/00002632.pdf
[37] http://it.nv.gov/uploadedFiles/ITnvgov/Content/Governance/dtls/ITAB/About/ITStrategicPlan_Draft.pdf
[38] http://www.courts.maine.gov/maine_courts/committees/tech_comm.html
[39] Privacy Rights Clearinghouse. "Data Breaches" https://www.privacyrights.org/data-breaches
[40] http://law.justia.com/codes/mississippi/2013/title-75/chapter-24/general-provisions/section-75-24-29
http://www.swlaw.com/blog/data-security/2016/03/16/utahs-personal-information-protection-and-data-breach-laws/
http://www.swlaw.com/blog/data-security/2015/04/30/the-nevada-data-breach-law/
http://legislature.maine.gov/statutes/10/title10sec1348.html
[41] Ibid.
[42] Ibid.
[43] Ibid.
[44] Ibid.
[45] State of California Department of Justice Office of the Attorney General. "Breach Report 2016" https://oag.ca.gov/breachreport2016
[46] Ibid.
[47] Ibid.
[48] Ibid.
[49] Constantin, L. (2012, October 29). South Carolina reveals massive data breach of Social Security Numbers, credit cards. Retrieved June 11, 2017, from http://www.infoworld.com/article/2615754/cyber-crime/south-carolina-reveals-massive-data-breach-of-social-security-numbers--credit-cards.html
[50] Deloitte. "State of South Carolina Information Security and Privacy Final Report". http://www.admin.sc.gov/files/InfoSec%20-%20Public%20Final%20Report%20-%201Dec2014.pdf
[51] Ibid.
[52] Smith, Tim. (2016, August 12). The Greenville News. "Four years later, case still open in DOR data breach". http://www.greenvilleonline.com/story/news/crime/2016/08/12/four-years-later-case-still-open-dor-data-breach/88453548/
[53] Ibid.
[54] Deloitte.
[55] Fikac, Peggy. (2012, April 25). Houston Chronicle. "Texas AG releases voters' Social Security numbers in mix-up." http://www.chron.com/news/houston-texas/article/Texas-AG-releases-voters-Social-Security-numbers-3510642.php
[56] Forsyth, Jim. (2011, September 29). Reuters. "Records of 4.9 mln stolen from car in Texas data breach". http://www.reuters.com/article/us-data-breach-texas-idUSTRE78S5JG20110929
[57] Arizona Department of Economic Security. "Performance Audit". (2017, April). https://www.azauditor.gov/sites/default/files/17-104_Report.pdf; Stewart, Kristen. (2013, April 29). "Report: Utah's health data breach was a costly mistake". http://www.sltrib.com/sltrib/news/56210404-78/security-breach-health-data.html.csp
[58] Ibid.
[59] Privacy Rights Clearinghouse. "Data Breaches" https://www.privacyrights.org/data-breaches
[60] National Governor's Association. "Cyber Liability Insurance." https://ci.nga.org/files/live/sites/ci/files/1617/docs/1705CybersecurityInsurance.pdf
[61] Ibid.
[62] Ibid.
[63] Ibid.
[64] National Governor's Association. "Cybersecurity Critical Infrastructure." https://ci.nga.org/files/live/sites/ci/files/1617/docs/1610CybersecurityCriticalInfrastructure.pdf

[65] National Governor's Association. "Cybersecurity Workforce Pipeline." https://ci.nga.org/files/live/sites/ci/files/1617/docs/1610WorkforcePipeline.pdf
[66] Ibid.
[67] National Governor's Association. "Cybersecurity Critical Infrastructure." https://ci.nga.org/files/live/sites/ci/files/1617/docs/1701SmallBusiness.pdf
[68] Cybersecurity Consultant, Christine. "Praetorian Expert Interview." Telephone Interview. 19 May 2017
[69] Cybersecurity Consultant, Geoff. "SecurityScorecard Expert Interview." Telephone Interview. 19 May 2017
[70] Cybersecurity Consultant, John. "GreyCastle Expert Interview." Telephone Interview. 19 May 2017