TESTIMONY OF
Jessica Newby
GOVERNANCE, RISK, AND COMPLIANCE LEAD
NORTH DAKOTA INFORMATION TECHNOLOGY DEPARTMENT
BEFORE THE 68th LEGISLATIVE SESSION
SENATE STATE AND LOCAL GOVERNMENT COMMITTEE
MARCH 30, 2023
NEUTRAL TESTIMONY - HOUSE BILL 1528

Chairman Roers, members of the Senate State and Local Government Committee, my name is Jessica Newby and I am the Governance, Risk and Compliance Lead for the North Dakota Information Technology Department (NDIT). I am here today to provide neutral testimony on House Bill 1528.

When I testified before this committee last week, a few outstanding questions remained regarding the ability to remove emails that contain sensitive/restricted data or malicious content. For the last week, our team has spent a great deal of time working with our vendor to find a solution and has been determined that a feasible solution does not yet exist for an organization of our size.

I bring this to your attention to make you aware of the risk this presents in our environment and to ask you to consider reducing the required retention period to one year, at least until a technical solution can be developed that would allow for the removal of sensitive data.

So how is risk quantified? By looking at the likelihood of an event occurring and the impact it will have, should it occur. If the event was a data breach, for example, the likelihood would be low, since we have security in place to hopefully protect us.

However, when you look at impact….. According to the IBM Security, the per-record cost of a data breach in 2022 was $164. It is estimated that in one year, a client care worker could accumulate emails containing personal health information for as many as 2,000 individuals. In the event a data breach should occur, that represents a potential cost of $328,000 per employee, per year of data retained. More employees plus more records equals more risk. So how do we reduce the risk? Either reduce the number of employees or reduce the number of records.

The technical implementation required for this bill also creates another potential risk related to open records. Agencies use various methods to search for emails and documents but, commonly, employees in question will simply search their own email to look for any records that complies with the request. Once retention is in place, this method will no longer work, because the deleted but retained emails and documents are not visible or accessible by the employee.

In order to enable agencies to conduct open records searches, an individual at each agency will have to be designated, assigned a special role and trained in using eDiscovery tools. This role is particularly sensitive, because the assigned individual will be able to search for and potentially read any email sent or received by anyone within their agency.

Thank you and I would be happy to stand for questions.