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 23, 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.

The Governance, Risk and Compliance (GRC) team is part of the overall NDIT cybersecurity team. One of the functions of the GRC team is to assist state agencies with navigating the complexities of federal security requirements, maintaining compliance with information exchange agreements and regulatory compliance frameworks. These requirements are in place to protect citizen data.

GRC also manages audit coordination when federal regulators, such as the IRS and Social Security Administration (SSA), come onsite to verify adherence to requirements. Some of the language contained in this bill could restrict the ability of agencies to comply with these regulatory requirements.

For example: Every state agency that accepts credit card payments must comply with the Payment Card Industry - Data Security Standard (PCI-DSS).

PCI-DSS 3.3.1 states that Sensitive Authentication Data (SAD) “is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.”

According to the regulations, “SAD is very valuable to malicious individuals as it allows them to generate counterfeit payment cards and create fraudulent transactions. Therefore, the storage of SAD upon completion of the authorization process is prohibited.”

PCI rules require stored credit card data to be encrypted prior to processing, which means that email is not an acceptable method for accepting credit card information. While no state agency allows credit card data to be sent by email, some agencies do have paper voucher forms that can be mailed in. Unfortunately, very little can be done to prevent someone from attaching and emailing the information anyway. When this happens, the onus is on the agency to properly dispose of the data.

Another example, from a recent audit of a state agency by the Social Security Administration: The agency has an information exchange agreement with SSA in order to verify benefit eligibility requirements, which is a business process requirement of the agency. During the audit, it was disclosed by the agency that the SSA reports were sent by email, but the emails were deleted within 30 days. The resulting audit finding required remediation to “provide policy and/or configuration evidence of retention period for emails that include the SVES batch files as attachments”.

While it is permissible for the reports to be retained in hard copy or in an approved electronic system, SSA does not allow email to be used as a system for retention due to the risk this presents.

So why does email present such a great risk? According to study completed by Deloitte, 91% of all cyber-attacks begin with a phishing email to an unexpected victim. One of the common methods attackers use, called credential harvesting, starts with a phishing email that contains a link. When clicked, the link takes the victim to a fake sign-in page that often looks identical to an "official" sign-in page. However, when the victim types in a username and password on the fake sign-in page, the information is recorded by the bad guys, who now have all the information they need to access to the victim's email box and all the emails that are contained within.

While retaining emails that contain decisions about day-to day operations of state agencies, for example, prompts openness and transparency in government, retaining emails that may contain sensitive, confidential, or otherwise restricted information pertaining to citizens of North Dakota is risky. The longer emails are required or allowed to be retained, the great the risk.

It is estimated that in one year, a direct client care worker could accumulate emails containing personal health information for as many as 2,000 individuals. Should a data breach occur, the federal Health Information Portability and Accountability Act (HIPPA) allows regulators to levy fines as high as $10,000 per violation of the Act.

Phishing emails also can contain malicious attachments or content. Every day, state employees report phishing emails using the phishing alert button. Those reports go to our cybersecurity team to investigate. Of the thousands that are reported each week, hundreds of emails are found to contain links to credential harvesters or contain other malicious content.

Under the current language of this bill, our security team would not be able to permanently remove those emails from our system, as they do today. While the emails still could be removed from the user's inbox, by remaining in retention, those emails could accidently be provided as part of an open records request, potentially infecting the recipient of the records request.

This bill contains an emergency clause. In order to be properly implemented, additional time may be needed to create necessary policies and procedures, as well as educate agencies on the potential impacts.

I would be happy to work with any members of the Committee or the bill sponsors on some minor amendments to the bill that would address some of the key areas I spoke about today.

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