Senate Fiscal Agency
P. O. Box 30036
Lansing, Michigan 48909-7536

BILL ANALYSIS

Telephone: (517) 373-5383
Fax: (517) 373-1986

Senate Bills 632 and 633 (as introduced 10-17-17)
Sponsor: Senator Darwin L. Booher
Committee: Banking and Financial Institutions

Date Completed: 5-1-18

**CONTENT**

**Senate Bill 632 would amend the Management and Budget Act to do the following:**

**-- Create the Cybersecurity Council within the Department of Technology, Management, and Budget.**
**-- Require the Council to issue an annual report detailing its activities for improving the infrastructure of the State's cybersecurity operations and accelerating the growth of cybersecurity as an industry in the State.**
**-- Require the Council to meet at least quarterly.**
**-- Exempt certain records and information from disclosure under the Freedom of Information Act.**
**-- Require the Council to create and operate a voluntary program recognizing private and public entities functioning with exemplary cybersecurity practices.**

**Senate Bill 633 would amend the Identity Theft Protection Act to do the following:**

**-- Prohibit a person from failing or neglecting to store in a computerized database in an encrypted form personal identifying information that was collected in the regular course of business in the conduct of trade or commerce.**
**-- Require a person or agency that owned or licensed a database that discovered a security breach to notify each financial institution that issued a credit or debit card that was compromised by the breach.**
**-- Require a notice to include the date, estimated date, or date range of a security breach and, if the person giving notice were the source of the breach, include an offer to provide an affected Michigan resident identity theft prevention for at least 12 months.**
**-- Permit a depository institution whose computerized customer database was subject to a security breach to bring a civil action for actual damages to the institution.**

Senate Bill 633 would take effect 90 days after its enactment. The bills are tie-barred.

## Senate Bill 632

Council Responsibilities

The bill would require the Cybersecurity Council to annually issue a report detailing its activities for the fiscal year. The report would have to include the following:

-- Improving the infrastructure of the State's cybersecurity operations with existing resources and through partnerships between government, business, and institutions of higher education.
-- Examining specific actions to accelerate the growth of cybersecurity as an industry in the State.

By December 1 of each year, the Council would have to submit the report for the immediately preceding fiscal year to all of the following:

-- The Director of the Department of Technology, Management, and Budget (DTMB).
-- The Governor.
-- The Lieutenant Governor.
-- The Senate Majority Leader.
-- The Speaker of the House of Representatives.
-- The Senate and House standing committees with jurisdiction of cybersecurity matters.

The Council would have to create and operate a voluntary program that recognized private and public entities functioning with exemplary cybersecurity practices as determined by the Council. The voluntary program would have to do the following:

-- Establish minimum protections for recognition in the voluntary program.
-- Establish annual review of the minimum protections.

The Cybersecurity Council could request the assistance of State agencies, departments, or offices to carry out its duties.

Council Membership; Terms; Meetings

Members of the Cybersecurity Council would include the following or their designees:

-- The DTMB Director.
-- The Department of Talent and Economic Development Director.
-- The Department of State Police Director.
-- The Department of Military and Veterans Affairs Director.
-- The chief executive officer of the Michigan Economic Development Corporation.

Additionally, the Council would include the following six members appointed by the Governor:

-- One representing the interests of institutions of higher education.
-- One representing the interests of community colleges.
-- Four representing the interests of the business community.

Of the members representing the interests of the business community, one each would have to have knowledge or experience in the following areas: hospital operations, retail operations, finance, or general business.

The members first appointed to the Council would have to be appointed within 90 days after the date the bill took effect.

Council members would have to serve without compensation but could be reimbursed for their actual and necessary expenses incurred in the performance of their official duties as Council members.

Members of the Council would have to serve for four-year terms or until a successor was appointed, whichever was later, except that of the members first appointed by the Governor, two would have to serve for two years, two for three years, and two for four years.

If a vacancy occurred on the Council, the Governor would have to make an appointment for the unexpired term in the same manner as the original appointment.

The Governor could remove a Council member for incompetence, dereliction of duty, malfeasance, misfeasance, or nonfeasance in office, or any other good cause.

The Governor would have to call the first meeting of the Council. At the first meeting, the Council would have to elect from among its members a chairperson and other officers as it considered necessary or appropriate. After the first meeting, the Council would have to meet at least quarterly, or more frequently at the call of the chairperson or if requested by six or more members.

The Council would be subject to the Open Meetings Act.

Record Disclosure Exemptions

The bill would exempt from disclosure under the Freedom of Information Act records or information of measures designed to protect the security or safety of people or property, or the confidentiality, integrity, or availability of information systems, whether public or private, including building, public works, and public water supply designs to the extent that those designs related to the ongoing security measures of a public body, capabilities and plans for responding to a violation of the Michigan Anti-Terrorism Act, emergency response plans, risk-planning documents, threat assessments, and domestic preparedness strategies, and cybersecurity plans, cybersecurity assessments, or cybersecurity vulnerabilities, unless disclosure would not impair a public body's ability to protect the security or safety of people or property or unless the public interest in disclosure outweighed the public interest in nondisclosure in the particular instance.

The bill also would exempt from disclosure information that would identify or provide a means of identifying a person that could, as a result of disclosure of the information, become a victim of a cybersecurity incident that would disclose a person's cybersecurity plans or cybersecurity-related practices, procedures, methods, results, organizational information system infrastructure, hardware, or software.

("Cybersecurity plan" would include, but not be limited to, information about a person's information systems, network security, encryption, network mapping, access control, passwords, authentication practices, computer hardware or software, or response to cybersecurity incidents.

"Cybersecurity assessment" would mean an investigation undertaken by a person, governmental body, or other entity to identify vulnerabilities in cybersecurity plans.

"Cybersecurity vulnerability" would mean a deficiency within computer hardware or software

"Cybersecurity incident" would include, but not be limited to, a computer network intrusion or attempted intrusion; a breach of primary computer network controls; unauthorized access to programs, data, or information contained in a computer system; or actions by a third party that materially affect component performance or, because of impact to component systems, prevent normal computer system activities.)

Storing Personal Identifying information

The Identity Theft Protection Act prohibits a person from conducting certain activities in the conduct of trade or commerce. The bill would include among the prohibited activities, if a person collected personal identifying information in the regular course of business and stored that information in a computerized databased, failing or neglecting to store that information in the database in an encrypted form.

(A violation of this prohibition is a misdemeanor punishable by imprisonment for up to 93 days and/or a maximum fine of $1,000 for a first violation, $2,000 for a second violation, or $3,000 for a third or subsequent violation.)

Security Breach Notice

The Act specifies that unless a person or agency determines that a security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more Michigan residents, a person or agency that owns or licenses data that are included in a database that discovers a security breach, or receives notice of a security breach, must provide a notice of the breach to each resident of the State who meets one or both of the following:

-- That resident's unencrypted and unredacted personal information was accessed and acquired by an unauthorized person.
-- That resident's personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key.

The bill also would require a notice of a security breach to be sent to each financial institution that issued a credit or debit card that was compromised by the breach.

A person or agency that was required to give notice of a security breach to a financial institution would have to provide the notice within three business days after the date the person or agency discovered the breach. Any other notice would have to be provided without reasonable delay.

The Act requires a notice to describe a security breach in general terms, describe the type of personal information that was the subject of the unauthorized access or use, and include other specified information.

Under the bill, a notice also would have to do all of the following:

-- Include one of the following, as applicable, if the information could be determined at the time the notice was provided: 1) the date of the breach; 2) the estimated date of the breach; or 3) the date range within which the breach occurred.
-- Include the date of the notice.
-- State whether notification was delayed as a result of an investigation by a law enforcement agency, if that information could be determined at the time the notice was provided.

In addition, if the person or agency providing the notification were the source of the breach, and were providing the notice to a Michigan resident whose personal information was accessed by an unauthorized person or to the owner or licensor of the information of the security breach, the notice would have to include an offer to provide appropriate identity theft

prevention and mitigation services, if any, at no cost to the affected resident for at least 12 months, and include all information necessary for the resident to accept the offer.

Civil Action

Under the bill, if a person maintained a computerized database that included personal identifying information about a depository institution's customers, and a security breach of the computerized database occurred, the depository institution could bring a civil action against that person for any actual damages to the institution, including its costs incurred in connection with any of the following:

-- Canceling or reissuing any credit or debit cards affected by the security breach.
-- Closing any deposit, transaction, share draft, or other accounts affected by the security breach and any action to stop payments or block transactions with respect to the accounts.
-- Opening or reopening any deposit, transaction, share draft, or other accounts affected by the security breach.
-- Making any refund or credit to a credit or debit cardholder to cover the cost of any unauthorized transaction relating to the security breach.
-- Notifying any customers of the depository institution affected by the security breach.

Proposed MCL 18.1466 (S.B. 632)
MCL 445.71 & 445.72 (S.B. 633)

Legislative Analyst: Stephen Jackson

**FISCAL IMPACT**

**Senate Bill 632**

The bill would have no fiscal impact on State or local government. Departmental annual appropriations should be able to absorb any costs associated with reimbursing Council members for their expenses.

**Senate Bill 633**

The bill would have no fiscal impact on the State and could have a negative fiscal impact on local government. Any increase in misdemeanor arrests and convictions could increase resource demands on law enforcement, court systems, community supervision, and jails. Any associated increase in fine revenue would increase funding to public libraries.

Fiscal Analyst: Ryan Bergan
Joe Carrasco

SAS\S1718\s632sa