Session of 2018

Substitute for HOUSE BILL No. 2359

By Committee on Government, Technology and Security

2-15

AN ACT concerning information systems and communications; creating the Kansas cybersecurity act; establishing the Kansas information security office; relating to executive branch agencies.

Be it enacted by the Legislature of the State of Kansas:

Section 1. Sections 1 through 8, and amendments thereto, shall be known and may be cited as the Kansas cybersecurity act.

Sec. 2. As used in sections 1 through 8, and amendments thereto:

(a) "Act" means the Kansas cybersecurity act.

(b) "Breach" or "breach of security" means unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of an executive branch agency does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

(c) "CISO" means the executive branch chief information security officer.

(d) "Cybersecurity" is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

(e) "Cybersecurity positions" do not include information technology positions within executive branch agencies.

(f) "Data in electronic form" means any data stored electronically or digitally on any computer system or other database and includes recordable tapes and other mass storage devices.

(g) "Executive branch agency" means any agency in the executive branch of the state of Kansas, but does not include elected office agencies, the Kansas public employees retirement system, regents' institutions, or the board of regents.

(h) "KISO" means the Kansas information security office.

(i) (1) "Personal information" means:

(A) An individual's first name or first initial and last name, in combination with at least one of the following data elements for that individual:

(i) Social security number;

(ii) driver's license or identification card number, passport number,

military identification number or other similar number issued on a government document used to verify identity;

(iii) financial account number or credit or debit card number, in combination with any security code, access code or password that is necessary to permit access to an individual's financial account;

(iv) any information regarding an individual's medical history, mental or physical condition or medical treatment or diagnosis by a healthcare professional; or

(v) an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual; or

(B) a user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(2) "Personal information" does not include information:

(A) About an individual that has been made publicly available by a federal agency, state agency or municipality; or

(B) that is encrypted, secured or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

Sec. 3. (a) There is hereby established the position of executive branch chief information security officer. The CISO shall be in the unclassified service under the Kansas civil service act, shall be appointed by the governor and shall receive compensation in an amount fixed by the governor.

(b) The CISO shall:

(1) Report to the executive branch chief information technology officer;

(2) serve as the state's CISO;

(3) serve as the executive branch chief cybersecurity strategist and authority on policies, compliance, procedures, guidance and technologies impacting executive branch cybersecurity programs;

(4) ensure Kansas information security office resources assigned or provided to executive branch agencies are in compliance with applicable laws and rules and regulations;

(5) coordinate cybersecurity efforts between executive branch agencies;

(6) provide guidance to executive branch agencies when compromise of personal information or computer resources has occurred or is likely to occur as the result of an identified high-risk vulnerability or threat; and

(7) perform such other functions and duties as provided by law and as directed by the executive chief information technology officer.

Sec. 4. (a) There is hereby established the Kansas information

security office. The Kansas information security office shall be administered by the CISO and be staffed appropriately to effect the provisions of the Kansas cybersecurity act.

(b) For the purpose of preparing the governor's budget report and related legislative measures submitted to the legislature, the Kansas information security office, established in this section, shall be considered a separate state agency and shall be titled for such purpose as the "Kansas information security office." The budget estimates and requests of such office shall be presented as from a state agency separate from the department of administration, and such separation shall be maintained in the budget documents and reports prepared by the director of the budget and the governor, or either of them, including all related legislative reports and measures submitted to the legislature.

(c) Under direction of the CISO, the KISO shall:

(1) Administer the Kansas cybersecurity act;

(2) assist the executive branch in developing, implementing and monitoring strategic and comprehensive information security risk-management programs;

(3) facilitate executive branch information security governance, including the consistent application of information security programs, plans and procedures;

(4) using standards adopted by the information technology executive council, create and manage a unified and flexible control framework to integrate and normalize requirements resulting from applicable state and federal laws, and rules and regulations;

(5) facilitate a metrics, logging and reporting framework to measure the efficiency and effectiveness of state information security programs;

(6) provide the executive branch strategic risk guidance for information technology projects, including the evaluation and recommendation of technical controls;

(7) assist in the development of executive branch agency cybersecurity programs that are in compliance with applicable state and federal laws and rules and regulations and standards adopted by the information technology executive council;

(8) coordinate the use of external resources involved in information security programs, including, but not limited to, interviewing and negotiating contracts and fees;

(9) liaise with external agencies, such as law enforcement and other advisory bodies as necessary, to ensure a strong security posture;

(10) assist in the development of plans and procedures to manage and recover business-critical services in the event of a cyberattack or other disaster;

(11) assist executive branch agencies to create a framework for roles

and responsibilities relating to information ownership, classification, accountability and protection;

(12) ensure a cybersecurity training program is provided to executive branch agencies;

(13) provide cybersecurity threat briefings to the information technology executive council;

(14) provide an annual status report of executive branch cybersecurity programs of executive branch agencies to the joint committee on information technology and the house committee on government, technology and security; and

(15) perform such other functions and duties as provided by law and as directed by the CISO.

Sec. 5. The executive branch agency heads shall:

(a) Be solely responsible for security of all data and information technology resources under such agency's purview, irrespective of the location of the data or resources. Locations of data may include: (1) Agency sites; (2) agency real property; (3) infrastructure in state data centers; (4) third-party locations; and (5) in transit between locations;

(b) ensure that an agency-wide information security program is in place;

(c) designate an information security officer to administer the agency's information security program that reports directly to executive leadership;

(d) participate in CISO-sponsored statewide cybersecurity program initiatives and services;

(e) implement policies and standards to ensure that all the agency's data and information technology resources are maintained in compliance with applicable state and federal laws and rules and regulations;

(f) implement appropriate cost-effective safeguards to reduce, eliminate or recover from identified threats to data and information technology resources;

(g) include all appropriate cybersecurity requirements in the agency's request for proposal specifications for procuring data and information technology systems and services;

(h) (1) submit a cybersecurity assessment report to the CISO by October 16 of each even-numbered year, including an executive summary of the findings, that assesses the extent to which a computer, a computer program, a computer network, a computer system, a printer, an interface to a computer system, including mobile and peripheral devices, computer software, or the data processing of the agency or of a contractor of the agency is vulnerable to unauthorized access or harm, including the extent to which the agency's or contractor's electronically stored information is vulnerable to alteration, damage, erasure or inappropriate use;

(2) ensure that the agency conducts annual internal assessments of its security program. Internal assessment results shall be considered confidential and shall not be subject to discovery by or release to any person or agency outside of the KISO or CISO. This provision regarding confidentiality shall expire on July 1, 2023, unless the legislature reviews and reenacts such provision pursuant to K.S.A. 45-229, and amendments thereto, prior to July 1, 2023; and

(3) prepare or have prepared a summary of the cybersecurity assessment report required in paragraph (1), excluding information that might put the data or information resources of the agency or its contractors at risk. Such report shall be made available to the public upon request;

(i) participate in annual agency leadership training to ensure understanding of: (1) The information and information systems that support the operations and assets of the agency; (2) the potential impact of common types of cyberattacks and data breaches on the agency's operations and assets; (3) how cyberattacks and data breaches on the agency's operations and assets could impact the operations and assets of other governmental entities on the state enterprise network; (4) how cyberattacks and data breaches occur; (5) steps to be undertaken by the executive director or agency head and agency employees to protect their information and information systems; and (6) the annual reporting requirements required of the executive director or agency head; and

(j) ensure that if an agency owns, licenses or maintains computerized data that includes personal information, confidential information or information, the disclosure of which is regulated by law, such agency shall, in the event of a breach or suspected breach of system security or an unauthorized exposure of that information:

(1) Comply with the notification requirements set out in K.S.A. 2017 Supp. 50-7a01 et seq., and amendments thereto, and applicable federal laws and rules and regulations, to the same extent as a person who conducts business in this state; and

(2) not later than 48 hours after the discovery of the breach, suspected breach or unauthorized exposure, notify: (A) The CISO; and (B) if the breach, suspected breach or unauthorized exposure involves election data, the secretary of state.

Sec. 6. (a) An executive branch agency head, with input from the CISO, may require employees or contractors of executive branch agencies, whose duties include collection, maintenance or access to personal information, to be fingerprinted and to submit to a state and national criminal history record check at least every five years.

(b) The fingerprints shall be used to identify the employee and to determine whether the employee or other such person has a record of criminal history in this state or another jurisdiction. The executive director

or agency head shall submit the fingerprints to the Kansas bureau of investigation and the federal bureau of investigation for a state and national criminal history record check. The executive director or agency head may use the information obtained from fingerprinting and the criminal history record check for purposes of verifying the identity of the employee or other such person and in the official determination of the qualifications and fitness of the employee or other such person to work in the position with access to personal information.

(c) Local and state law enforcement officers and agencies shall assist the executive director or agency head in the taking and processing of fingerprints of employees or other such persons. Local law enforcement officers and agencies may charge a fee as reimbursement for expenses incurred in taking and processing fingerprints under this section, to be paid by the executive branch agency employing or contracting the individual required to submit to fingerprinting and a criminal history record check.

Sec. 7. Information collected to effectuate this act shall be considered confidential by the executive branch agency and KISO unless all data elements or information that specifically identifies a target, vulnerability or weakness that would place the organization at risk have been redacted, including: (a) System information logs; (b) vulnerability reports; (c) risk assessment reports; (d) system security plans; (e) detailed system design plans; (f) network or system diagrams; and (g) audit reports. The provisions of this section shall expire on July 1, 2023, unless the legislature reviews and reenacts this provision pursuant to K.S.A. 45-229, and amendments thereto, prior to July 1, 2023.

Sec. 8. Executive branch agencies may pay for cybersecurity services from existing budgets, from grants or other revenues, or through a special assessment to offset costs. Any executive branch agency's increase in fees or charges related to this act shall be used only for cybersecurity and no other purpose. Service or transactions with an applied cybersecurity cost recovery fee may indicate the portion of the fee dedicated to cybersecurity on all receipts and transaction records.

Sec. 9. This act shall take effect and be in force from and after its publication in the statute book.