SENATE BILL REPORT
E2SHB 2375

As Reported by Senate Committee On:
Law & Justice, February 26, 2016

Title: An act relating to cybercrime.

Brief Description: Concerning cybercrime.

Sponsors: House Committee on General Government & Information Technology (originally sponsored by Representatives Magendanz, Orwall, Smith, Tarleton, MacEwen, Muri, Stanford and Wylie).

Brief History: Passed House: 2/16/16, 97-0.
Committee Activity: Law & Justice: 2/23/16, 2/26/16 [DPA].

SENATE COMMITTEE ON LAW & JUSTICE

Majority Report: Do pass as amended.
Signed by Senators Padden, Chair; O'Ban, Vice Chair; Pedersen, Ranking Minority Member; Darneille, Frockt, Pearson and Roach.

Staff: Lindsay Erickson (786-7465)

Background: Cyber Crimes Generally. Cybercrime is a broad term that refers to many different types of high-tech crimes committed through the use of electronic devices, including fraud, scams, theft, extortion, hacking, trespass, identity theft, espionage, terrorism, preying upon the elderly and children, and other crimes. As technology advances, people are storing more information electronically and sharing more information electronically on websites and with businesses, the government, and others. This increased connectivity brings greater risk of theft, fraud, and abuse.

Within the state of Washington, cyber threats are an increasingly unpredictable, dangerous, and proliferating hazard to state, local, and tribal governments, as well as private industry. Local and state governments have reported large, sensitive data breaches, as well as recent cyber heists, some larger than $1,000,000.

Computer Trespass. A person is guilty of computer trespass in the first degree if the person, without authorization, intentionally gains access to a computer system or electronic database of another and: the access is made with the intent to commit another crime; or the violation

---

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.

involves a computer or database maintained by a government agency. Computer trespass in the first degree is a ranked Class C felony with a seriousness level of II.

A person is guilty of computer trespass in the second degree if the person, without authorization, intentionally gains access to a computer system or electronic database of another under circumstances not constituting the offenses in the first degree. Computer trespass in the second degree is a gross misdemeanor.

Criminal Penalties. Class C felonies are punishable by up to five years in a state correctional institution, a fine of up to $10,000, or both confinement and a fine. Gross misdemeanors are punishable by up to 364 days in jail, a fine of up to $5,000, or both jail and a fine.

Summary of Bill (Recommended Amendments): Definitions. The following terms are defined: "access;" "cybercrime;" "data;" "data network;" "data program;" "data services;" "data system;" "malware;" "white hat security research;" and "without authorization." The definition for "computer program" is removed.

Computer Trespass. Computer Trespass in the first degree is modified by specifying that access must be made with the intent to commit another crime in violation of state law that is not a cybercrime.

Electronic Data Interference. The crime of Electronic Data Interference is created. A person commits Electronic Data Interference if the person maliciously and without authorization causes the transmission of data, a data program, or other electronic command that intentionally interrupts or suspends access to or use of a data network or data service. Electronic Data Interference is a ranked class C felony with a seriousness level II.

Electronic Data Theft. The crime of Electronic Data Theft is created. A person commits Electronic Data Theft if he or she intentionally, without authorization, and without reasonable grounds to believe that the person has such authorization, obtains any electronic data with the intent to devise or execute any scheme to defraud, deceive, extort, or commit any other crime in violation of a state law that is not a cybercrime, or wrongfully control, gain access, or obtain money, property, or electronic data. Electronic Data Theft is a ranked class C felony with a seriousness level II.

Electronic Data Tampering. The crimes of Electronic Data Tampering in the first and second degrees are created. A person commits Electronic Data Tampering in the first degree if the person maliciously, without authorization, alters data as it transmits between two data systems over an open or insecure network, or introduces any malware into any electronic data, data system, or data network, and:

- doing so is for the purpose of devising or executing any scheme to defraud, deceive, or extort, or commit any other crime in violation of state law that is not a cybercrime, or of wrongfully controlling, gaining access, or obtaining money, property, or electronic data; or
- the electronic data, data system, or data network is maintained by a governmental agency.

A person commits Electronic Data Tampering in the second degree if he or she maliciously, without authorization, alters data as it transmits between two data systems over an open network under circumstances not constituting the offense in the first degree, or introduces any malware into any electronic data, data system, or data network under circumstances not constituting the offense in the first degree.

Electronic Data Tampering in the first degree is a ranked class C felony with a seriousness level of II, and Electronic Data Tampering in the second degree is a gross misdemeanor.

Spoofing. The crime of Spoofing is created. A person commits Spoofing if the person, without authorization, knowingly initiates the transmission, display, or receipt of the identifying information of another organization or person for the purpose of gaining unauthorized access to electronic data, a data system, or a data network, and with the intent to commit another crime in violation of a state law that is not a cybercrime. Spoofing is a gross misdemeanor.

Prosecution of Other Crimes. A person who, in the commission of a cybercrime, commits any other crime may be punished for that other crime as well as for the cybercrime and may be prosecuted for each crime separately.

EFFECT OF CHANGES MADE BY LAW & JUSTICE COMMITTEE (Recommended Amendments): The definition of "without authorization" is changed to include unauthorized elevation of privileges. The crimes of electronic data tampering in the first and second degrees are changed to include the alteration of data as it transmits between two data systems over an unsecure network, in addition to an open network.

Appropriation: None.

Fiscal Note: Available.

Committee/Commission/Task Force Created: No.

Effective Date: Ninety days after adjournment of session in which bill is passed.

Staff Summary of Public Testimony: PRO: A lot of great changes have been made to this bill since it was last considered by this committee, and this version is a step in the right direction to strengthen our data protection. There are now protections for white hat security efforts, which are acts that strengthen security procedures for our websites. This is an issue that needs to be addressed quickly, considering the recent major breaches of Social Security numbers, health records, and other important privacy information. Ninety-two percent of all hacks now are us hacking ourselves, meaning we get phishing email messages received from what looks like a trusted retailer and valuable personal information is then copromised. These crimes cost retailers and consumers hundreds of millions of dollars each year and are very disruptive.

Persons Testifying: PRO: Representative Magendanz, Prime Sponsor; Joanie Deutsch, WA Retail Assoc.; Alex Alben, WA Office of the Chief Information Officer/WA Technology Solutions.

Persons Signed In To Testify But Not Testifying: No one.