General Assembly of the Commonwealth of Pennsylvania
Joint State Government Commission
Room 108 Finance Building, 613 North Street
Harrisburg, PA 17120
717-787-4397

Released: September 22, 2015

Summary of the Staff Study in Response to House Resolution No. 778 of 2014

Cybersecurity in Pennsylvania

On December 19, 2013 national retail chain Target revealed that it had suffered a cyberattack that resulted in the unauthorized access to payment card data of customers making credit and debit card purchases in its U.S. stores. Initially, Target estimated that approximately 40 million credit and debit card accounts may have been impacted between November 27 and December 15, 2013. Upon further investigation, Target discovered that names, mailing addresses, phone numbers, or email addresses for up to 70 million individuals were also stolen.

The Target incident is just one of several recent high-profile instances of personal data theft. It should come as no surprise, then, that cybersecurity is becoming a growing concern for governments, which possess personal information about their citizens, as well as sensitive government data. As a result, the Pennsylvania House of Representatives adopted 2014 House Resolution 778, directing the Joint State Government Commission (JSGC) to conduct a comprehensive study of the Commonwealth's cybersecurity efforts and protocols to protect private information of its citizens.

Specific information about networks and security measures cannot be published in order to protect the systems in place and to avoid revealing vulnerabilities. In fact, Pennsylvania's Right-to-Know Law provides a specific exception for records that, if released, could endanger the safety of computer security. Therefore, this report, the result of JSGC's comprehensive study, provides only an overview of the cybersecurity policies in place throughout the Commonwealth government.

Although Pennsylvania has not yet suffered a major breach, state offices and agencies are under constant threat. The question is not *whether* a breach will occur, but *when* a breach will occur. Ultimately, JSGC staff formulated two recommendations.

First, centralization of cybersecurity efforts will enhance cybersecurity efforts. Each branch of Pennsylvania's government addresses cybersecurity separately. All branches of the Commonwealth government implement cybersecurity efforts and protocols directed at safeguarding the personal information of residents of the Commonwealth. However, Pennsylvania's cybersecurity standards and protocols differ between the branches of government, and to an extent, within branches of the government. The Governor's Office of Administration has set a good example for centralized cybersecurity, and would be a good model for the legislature and the courts to follow. Greater cooperation between the branches will also enhance cybersecurity efforts.

The second recommendation is modernization of Pennsylvania's security breach notification law, the act of December 22, 2005, (P.L.474, No.94). This act has not been amended in the 10 years since its enactment, despite the fact that technology has rapidly changed, often in ways that could not have been foreseen, and continues to do so. This report includes suggested amendments.

The full report is available on our website, http://jsg.legis.state.pa.us/