

CYBERSECURITY: OPPORTUNITIES FOR MICHIGAN

THE THREAT

On January 26, 2011, the State of Michigan website was hacked. The domain was posted for sale on the Internet for \$55 and the purchaser would have received important administrative access if the hack had not been discovered.

On April 20, 2011, Sony experienced a breach of its PlayStation Network that exposed customer accounts, including credit card information, for up to 77 million users.

These incidents demonstrate the increased risk of cyber-attacks that accompanies our growing reliance on technology in both the public and private sectors. Not only are individuals vulnerable to scams and malicious programs, but they must also be attentive to the security of the organizations that they provide personal information to when making online purchases. This includes government entities that hold significant amounts of personal information about their constituents online. Governments are reliant on physical

infrastructure that is also threatened by cyber-attacks on utilities, health care, finance, education, and communication and transportation systems. A utility incident could lead to massive blackouts and a breach of patient health records could lead to mistreatment of and even death.

FEDERAL CYBERSECURITY OBJECTIVES

- Clarify roles and empower actors with policy, legal structures and coordination;
- Educate the public about the risks to increase the value put on security;
- Invest in workforce development to continue to lead the world in science and technology innovation related to cybersecurity;
- Further develop public-private collaborations to mitigate vulnerabilities and respond to incidents;
- Incentivize the private sector to develop more secure products.

**The focus has to be on prevention.
That is the way you offer
maximum protection to
consumers.
- Attorney General Eric Holder**

OPPORTUNITIES FOR MICHIGAN

State governments have more direct interaction with constituents than the federal government does so they are in a better position to provide education about cybersecurity. While the private sector is best-equipped to develop innovative cybersecurity technology and state governments cannot force this development, they can encourage it through collaborative partnerships. There are many groups in federal, state, local, tribal and territory governments and the private sector working on these efforts. Some collaboration already exists between these groups but there is room for growth in this area. These collaborations are most effective when governments have expertise to be able to offer value to the private sector so Michigan must continue to develop its knowledge base in the field. Encouraging the development of companies in this sector will not only fit the with State's goals to "stop the brain drain" and foster jobs but it also aligns with the federal goal to lead in cybersecurity innovation.