

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. The results could be deadly; a utility incident could lead to massive blackouts and a breach of health records could lead to mistreatment or death of patients.

HUMAN RESOURCES

The threat of incidents most often comes from external sources like governments and cyber-criminals, but it can also come from internal sources as well. It can be intentional in the case of a disgruntled employee, as in the recent WikiLeaks incidents, but it can also be unintentional. This highlights the importance of internal security measures and employee education.

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

CYBERSECURITY: OPPORTUNITIES FOR MICHIGAN

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.

MICHIGAN'S STRENGTHS

Michigan is uniquely positioned to be a leader in this area. As a result of the IT consolidation under the Engler administration, Michigan has a very centralized system. This structure enables the technology department to more closely monitor cybersecurity by maintaining only two trusted internet connections for 20 state agencies. Because of this configuration, the State of Michigan was chosen as a pilot for the federal government's Einstein program. While funding was not renewed for this program, it is likely that this IT structure will enable Michigan to secure further grant funding or pilot programs.

COLLABORATION

Michigan also has a strong talent base in this field. Strong university programs train a new generation of professionals for this field each year. The headquarters of Internet2, an advanced networking consortium led by the research and education community, is in Ann Arbor. The National Guard's Cyber Unit, state and local government collective pilots like Albert, MS-ISAC and AT&T, and other private sector initiatives offer a variety of opportunities for collaboration.

**For more information contact:
The Michigan Cyber Security Action
Team**