Michigan Cyber Initiative Newsletter

Articles of Interest

Cybersecurity Tips for City Officials
Local governments are no exception to cyber attacks, and many of the threats could greatly affect citizen services. City officials are urged to invest in training, monitoring and continuity plans. (Read more here)

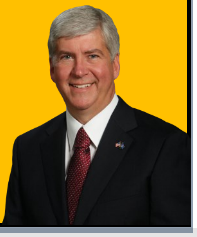
Organizations Face Challenges in Cybersecurity
Results from a new survey reveal that while cybersecurity is a topic during most board meetings, board members feel they lack critical cybersecurity knowledge and trust between cybersecurity professionals among other things. (Read more here)

A Fund for Cybersecurity
Launched last year, a New Jersey investment firms' cybersecurity fund invests in stocks that revolve around cybersecurity. (Read more here)

MICHIGAN
CYBER INITIATIVE
2015
Leading the Nation:
An interagency, public-private collaboration
www.michigan.gov/cybersecurity

Michigan's 2015 Cyber Initiative
Michigan's strategy to protect and defend our most valuable assets through education, economic development and collaboration.

Michigan Cyber Initiative News offers updates on Governor Rick Snyder's cyber initiative as well as knowledge and awareness on cybersecurity issues. This monthly newsletter is produced by the Michigan Department of Technology, Management and Budget , Office of Cybersecurity.



NORTH AMERICAN INTERNATIONAL
CYBER SUMMIT 2015
Experts from across the globe
Best Practices
Emerging Trends
Thought Leaders
REGISTRATION NOW OPEN
COBO CENTER
Detroit, MI
HOSTED BY MICHIGAN GOVERNOR RICK SNYDER
October 25-26
www.michigan.gov/cybersecurity

The Michigan Cyber Corps Needs You!

During the North American International Cyber Summit in October 2013, Governor Rick Snyder announced the formation of a volunteer cyber response team. The Michigan Cyber Civilian Corps (MiC3) is a group of cyber experts capable of assisting the state government in the event of a Governor declared cyber-emergency.

The MiC3 teams are located in various zones across Michigan. Currently, the K-12/ISD multi zone and Alpena zone are in need of additional cyber experts. Members receive training through Merit's Cyber Range and are also given the opportunity to participate in cyber exercises.

For those interested in applying, you can visit www.micybercorps.org for more information and to take the assessment.

Cyber Insurance: Are you Covered?

With cyber-attacks becoming alarmingly common and increasingly severe, the interest in cyber insurance is dramatically rising. Cyber insurance offers protections against losses related to information security breaches, such as data losses, business interruptions caused by network malfunctions or viruses, and fines or lost income due to system stoppages or network intrusions (risks usually excluded from traditional commercial liability coverages). The cyber insurance market is still developing with limited policy standardization or supporting actuarial data for underwriting purposes, so potential buyers should develop a mature information security program before seriously considering this form of coverage. This approach allows prospective consumers to inventory their vulnerabilities and mitigation strategies to ensure they select the right policy unique for their company's needs.

According to Gartner, cyber insurance should not be purchased as a replacement for a weak internal security program. In fact, cyber insurance will not cover all related information security risks and a lacking internal informational security program could hinder a company's ability to obtain coverage altogether. Regardless of industry, the following questions should be answered before purchasing cyber insurance:

- What are the company's most critical intellectual property assets and consumer/customer-based informational assets, and how are they currently being protected?
- Where are these assets stored or located? Internally, at a third-party data center, or in a cloud-based environment?
- What are the company's practices with respect to vetting the cyber security practices of third-party vendors and suppliers that may have access to the company's servers?
- Has the company formally adopted a cyber security standard or practice, such as the National Institute of Standards and Technology (NIST) Cyber Framework, or the International Organization for Standardization's information security management standard, and what mechanism does the company have to document discussions concerning compliance with those standards?
- What can go wrong during, and what could be the gross impact of, a significant data breach or network intrusion?
- Does the company have a mature incident response plan that includes a communication strategy with customers, investors, and law enforcement?
- How, and will, your company's current insurance policies respond to a data breach?

Cyber insurance costs range depending on the size of the company or institution. Additionally, if corporations and institutions can educate their insurer underwriters about the implementation of best practices in security and risk management, they will likely experience more comprehensive coverage and aggressively lower premiums. Companies that do not meet industry standards will, in contrast, see significant retentions, higher prices and exclusions introduced.

Author: Chad Laidlaw is a senior policy and planning analyst at the State of Michigan