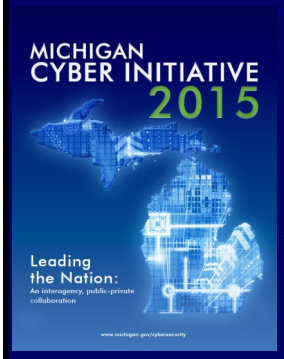
Michigan Cyber Initiative Newsletter

Articles of Interest

Investing in Endpoint Security
A recent survey shows that 85% of the organizations surveyed plan to spend more on endpoint security to improve incident response, detection and mitigate targeted attacks. (Read more here)

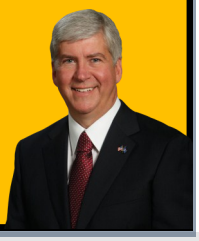
Five Cybersecurity Questions to Consider
Leadership may find it valuable to have these questions answered when determining the organization's legal and cyber risk profile. (Read more here)

Concern Still Lacking after Breaches
In a recent survey, several organizations have stated that while the priority for cybersecurity has increased, there is still a disconnect on the importance and urgency of cybersecurity within the organization. (Read more here)



Michigan's 2015 Cyber Initiative
Continuing the stride 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.



Avoid Becoming a Cyber Crime Victim

The Multi-State Information Sharing and Analysis Center recently released suggestions on protecting yourself from cyber crime.

Configure Your Devices Securely
Use privacy and security settings in software , email systems and web browsers. It is imperative to regularly update your anti -virus software to identify and thwart the newest threats.

Keep Software and Operating Systems Updated
Be sure to install all software updates as soon as they are offered; using the "auto update" setting is the best way to ensure timely updates.

Use Strong Passwords
Never use simple or easy-to-guess passwords like "123456" or "p@$$word". Cybercriminals use automated programs that can try every word in the dictionary within a few minutes.

Be Cautious About Links and Attachments
Be cautious about all communications you receive and the links within them, including those allegedly from friends and family. When in doubt, delete it.

Protect Your Personal Information
Cybercriminals will look at your social networking webpage to find information about you-. Many of the answers to website and bank security questions may be found online, like the color of your car (remember posting that picture of you standing in front of your car?) and your mother's maiden name. Use privacy settings to limit who can see the details of your social network pages, and be smart about what you decide to share online.

Review Your Financial Statements Regularly
Cybercriminals find loopholes and your accounts may get hacked through no fault of your own, so review your financial statements regularly. Contact your financial institution immediately if you see any suspicious looking activity.

Power Grid Security and Reliability is Ongoing Focus

When flipping on a light switch, you expect a room to illuminate. This simple task is made possible by the hard work and dedication of hundreds of utility workers across several disciplines, aided by sophisticated technology that enables them to do their jobs.

As the owner and operator of the high-voltage power grid covering the majority of the Lower Peninsula, cyber security is vital to ITC. We are responsible for delivering electrical energy from power generating plants over our network of power lines to the local distribution system of utilities serving businesses and communities.

Source: IT Holdings Corp.

A range of actions and controls by a wide array of technology enables this energy to be delivered safely and reliably. For example, computer technology is used to maintain power flows, monitor system bottlenecks and keep the cycles at 60 HZ, which keeps your lights bright and consistent.

Along with computer technology comes the threat of cyber-attacks. Threats to the energy sector are no secret. The U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team reported in 2013 that more than half of major brute force attacks targeting industrial control systems were aimed at energy companies. While these threats remain persistent and dangerous, utilities have several defenses in place designed to keep systems safe. These tools, along with vigilant staff, work night and day to monitor activity and respond to threats.

We've seen the damage that can occur when a system is breached, as evidenced by many high-profile companies in recent years across business sectors. While stolen personal information and credit card data poses risks to individuals, any disruption to the energy sector poses major consequences to the everyday flow of society.

To stay ahead of these threats, energy providers in Michigan are talking to each other to learn more about emerging issues and ways to combat them. Over the past year there have been roundtable discussions hosted by the Michigan Public Service Commission, cyber security drills hosted by the Michigan State Police and the Department of Technology, Management and Budget; meetings of the Governor's Cyber Security Task Force; and participation in workshops to help shape legislation designed to aid all businesses to better identify and deal with threats.

Closely related to cyber security is the subject of physical grid security – guarding against deliberate physical attacks to energy infrastructure, and making the grid more robust against severe weather. Our industry is working with the Federal Energy Regulatory Commission and the North American Electric Reliability Corporation to strengthen the nation's grid to better withstand any type of threat, natural or man-made.

Continued investments in secure, modern and robust electric infrastructure – and the skilled workers who bring that energy to us – will keep our lights shining bright.

Author: Ron Hinsley, Chief Information Officer, ITC Holdings Corp.