

THE CYBERSECURITY DOWNLOAD

Issue 1 - news, tips, and trends in cybersecurity - October 2011



Maryland is Poised to Become the “Epicenter” of Cybersecurity

Governor Martin O’Malley, in a 2009 interview with the Federal News Radio, stated that, “Maryland has the potential to become the Silicon Valley of cybersecurity.” Maryland is in a unique position to be at the forefront of an emerging industry that is projected to create new stable employment opportunities for many years to come. The emerging industry is cybersecurity and there are many factors that lead Governor O’Malley to make such an optimistic statement.



The reason Maryland is in a position to become the Silicon Valley of cybersecurity has a lot to do with the geographic location of the state as well as a variety of other factors. As identified in the Cyber Maryland Report, some of the most distinguishing factors are that Maryland is home to 50 federal agencies and research facilities, several of the nation’s top

academic research institutions, and an information technology (IT) industry cluster that is estimated to include 9,500 private sector businesses. This critical mass of organizations that possess expertise and capacity for action places Maryland in a leadership position in developing solutions to defend the nation against the growing threats in cyberspace.

To download the complete Cyber Maryland Report and access additional information about why Maryland is at the forefront of cybersecurity go to www.choosemaryland.org/industry/InfoTech/default.aspx.

Local Businesses Looking for Cybersecurity Workers

Local businesses operating in the cybersecurity arena are currently hiring qualified cybersecurity and information technology (IT) workers. However, there is a gap between the type of employees businesses need to hire, and the skills and qualifications that job seekers possess. This reality is causing local businesses like Superior Technology Solutions Corporation (STSC) to temper their growth because they are unable to find qualified workers to bid on new contracts.

STSC delivers quality IT support services to government agencies; however, in order to be awarded new contracts they must hire employees with clean backgrounds, industry certifications, and other qualifications. After learning about the qualified job seekers participating in the Pathways to Cybersecurity Careers program, STSC was able to hire two participants to fill immediate vacancies. David G. Williamson, president of STSC said, “MOED was instrumental in assisting with the hiring of two help desk technicians. These positions were difficult to fill because it required candidates to hold security clearances [and specific industry certifications]. We appreciated the diligence and hard work of Rosemary Woren and Michael Volk [of MOED] for assisting us with this endeavor.”

To learn how the Pathways to Cybersecurity Careers program may benefit your business, or how it may help you upgrade your skills, visit: www.aawdc.org/cyber.



Publication prepared by:
Michael Volk
MOED Cybersecurity Navigator
Phone: 410-396-1430
E-mail: wvolk@oedworks.com

FREE TRAINING: that could change your life!

Did you know you may be eligible to receive funding for training and industry certifications that will help you break into the emerging field of cybersecurity? If you have a background in information technology (IT), information assurance (IA), computer science, engineering, or another technical area you may be eligible to receive free training and industry certifications.

Certifications include: A +, CompTIA Network +, CompTIA Security +, Cisco Networking, Windows Server, Certified Ethical Hacker, Certified Computer Examiner, and others.

But funding is only available for a limited time so you must act fast! Hundreds of Maryland residents have already taken advantage of this opportunity.

For additional details about the Pathways to Cybersecurity Careers training program please go to: www.aawdc.org/cyber.

THE CYBERSECURITY DOWNLOAD

CSI 2.0: Computer Forensics

Every second 14 people become victims of cyber crimes. This is according to an eye opening study conducted by Norton in 2011 that examined cybercrime in 24 countries around the world. Cyber crime impacted a total of 431 million adults and cost a total of \$388 billion in 2011. (The complete report can be found here: http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/.)

Cybercrime is a significant threat that will continue to grow as use of technology increases. With the rise of cyber crime, computer forensics experts will be in demand.



Computer forensics experts play an integral role in investigating and prosecuting cyber crimes. Computer forensics professionals typically work in a lab supporting law enforcement organizations as well as legal teams charged with prosecuting and defending cases. A computer forensics expert will examine computers and other electronic devices involved in alleged crimes. Examinations are conducted to first determine if a crime has occurred, and secondly gather evidence used for prosecution and defense. Computer forensics is an exciting career field but it requires a specific combination of training, experience, and education in order to be qualified.

If you are interested in learning more about what you can do to become a computer forensics expert check out the article titled “So you want to be a computer forensics expert” by Deb Shinder. The full article can be found here: www.techrepublic.com/blog/security/so-you-want-to-be-a-computer-forensics-expert/4866?tag=mantle_skin;content.

Tips to Keep You Safe Online

Individual users of technology play a major role in preventing the proliferation of cyber crime. However, basic knowledge about how technology can be used safely is required. Below are some real world warnings that the Department of Homeland Security published to help you stay safe online:

- **Don't trust candy from strangers** - Finding something on the Internet does not guarantee that it is true.
- **If it sounds too good to be true, it probably is** - Beware of grand promises; they are most likely spam, hoaxes, or phishing schemes.
- **Don't advertise that you are away from home** - Be careful when setting automated email responses when you are away from home or the office. You do not want to let potential attackers know that you are not home, or worse, give specific details about your location or itinerary.
- **Lock up your valuables** - Take steps to protect personal or sensitive information by following good security practices.
- **Have a backup plan** - Since digital information can be easily lost or compromised, make regular backups of your information so that you still have clean, complete copies.



The full article and additional tips from DHS can be found here: www.us-cert.gov/cas/tips/.

What is Cybersecurity Anyway?

The National Security Agency (NSA) defines cybersecurity as “measures that protect and defend information and information systems by ensuring their availability, integrity, authenticity, and non-repudiation.”



Contacting Your Local One-Stop Career Center

To find out if you are eligible to participate in the Pathways to Cybersecurity training program, or to learn about other training programs focusing on areas such as BRAC, green construction, and green manufacturing, contact your local Baltimore one-stop career center.



Northwest One-Stop Career Center:
2401 Liberty Heights Avenue
Mondawmin Mall—Suite 302
Baltimore, MD 21215
Phone: 410-523-1060

Eastside One-Stop Career Center:
3001 E. Madison Street
Baltimore, MD 21205
Phone: 410-396-9030

Baltimore Works One-Stop Career Center:
1100 N. Eutaw Street
Baltimore, MD 21201
Phone: 410-767-2148

The Career Center Network is a service of the Baltimore Workforce Investment Board, the Mayor's Office of Employment Development and multiple workforce partners.

For more information visit www.oedworks.com