VIEWS & VISIONS

A publication of Bowles Rice LLP

Summer 2015

Promoting Cyber Hygiene

Jimmy Gianato, Director
West Virginia Division of Homeland Security & Emergency Management

Jimmy Gianato was appointed Director of Homeland Security and Emergency Management for the State of West Virginia by Governor Joe Manchin in September 2005. Mr. Gianato has operational and planning responsibility for the state's response to all emergency and disaster operations and consequence management for incidents involving weapons of mass destruction and terrorism.

In 2010, Governor Earl Ray Tomblin appointed Mr. Gianato as his Homeland Security Advisor, to serve as the primary point of contact with the U.S. Department of Homeland Security. During federally declared disasters, he serves as the State Coordinating Officer and the Governor's authorized representative to the Federal Emergency Management Agency. He also serves as the chairman of the State Emergency Response Commission.

Mr. Gianato has been involved in emergency response for over 35 years. Since 1972, he has served the Kimball Volunteer Fire Department in various capacities, including more than 15 years as Chief, and served as a volunteer and member of the Board of Directors for the McDowell County Emergency Ambulance Authority. He has been a certified Fire, EMS and Law Enforcement instructor for over 20 years and also provides training in Incident Command and the National Incident Management System.

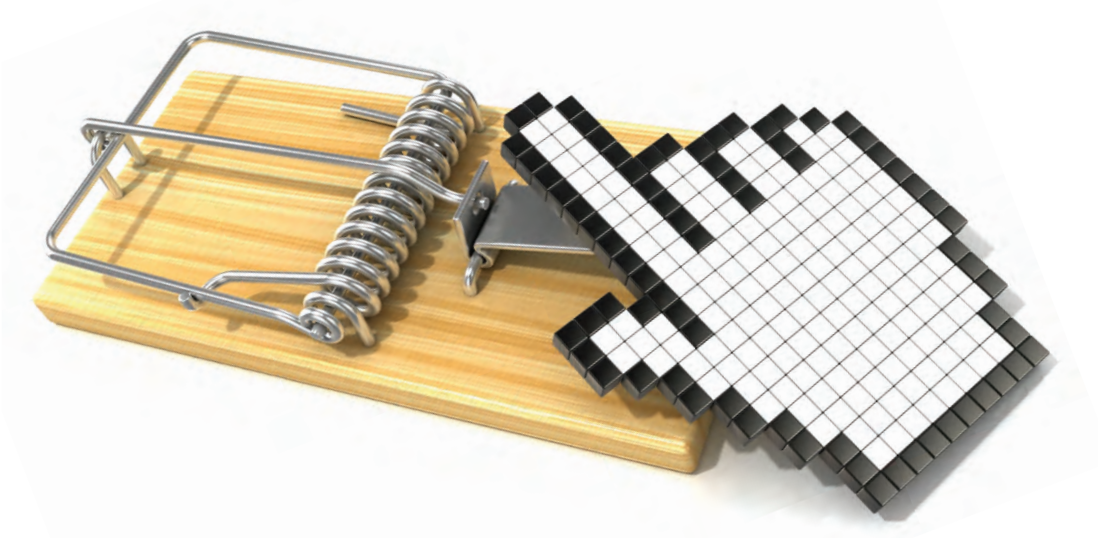
Director Gianato has been selected by his fellow Homeland Security Advisors to serve on the executive committee of the Governor's Homeland Security Advisor's Committee (GHSAC) and chairs the Interoperability Committee.

When we think of security, most of us think in terms of the traditional protections that keep us safe. We think of the physical side of security, how to keep intruders out or how to protect our valuables from being stolen. But in the world today, thieves steal from us in ways that we never dreamed of. They steal our intellectual property, our identities, money from our bank accounts, our medical information, our credit card information and much of our personal information that we always thought was safe. Every year, billions of dollars are spent to repair the damage caused by cyber attacks. Just like every disaster begins at the local level, the prevention of the cyber attack can begin with you. Some simple things that everyone can do can minimize the impact of these events.

Most of us can remember the space race. We remember how the United States lagged behind the Soviet Union and the challenges we faced, as well as the sacrifices that were made until that day in July 1969 when Neil Armstrong descended a ladder and set foot on the moon. The computer equipment that was developed to accomplish that mission filled rooms.

Today, most of us carry a hand-held personal computer that has as much power as its mammoth predecessors. We have progressed from that grainy black-and-white transmission of the moon landing to an ability to video chat with family and friends all over the world. We can access our medical information and fill our prescriptions online, bank online, shop online and read news and weather online. But as we do all these things, we risk exposing that same information. As a result of those advances, we also are presented with the challenges of how to protect our most valuable information and assets, and still have the freedom to use that technology to enhance our lives.

One of the fastest growing trends is social media. Applications like Facebook, Twitter, Instagram and others have enabled us to stay connected like never before. We often post our personal information and even our schedule, but with this connectivity also comes vulnerability. Cyber criminals thrive on the opportunities of social media as consumers have begun to use it as a primary means of communicating. It is estimated that around 10 percent of social media users have received some form of cyber threat.



In addition to the cyber threat, many of us freely place our personal lives in full public view via social media applications. This provides opportunities for those seeking to use the information for fraudulent purposes.

In its efforts to combat cyber crime, the FBI has established the National Cyber Investigative Task Force. This group is comprised of many partners from the intelligence community, Department of Defense, critical infrastructure, industry and international partners. Cyber crime affects us all, and it will take all of us to help reduce its impact.

In West Virginia, the State Police's Crimes Against Children Unit has made substantial progress in investigations and apprehensions of perpetrators who seek to use the internet and new technologies to exploit children. The West Virginia Intelligence Fusion Center and the State Office of Technology have identified numerous cases of individuals using public computers to view child pornography and, working with law enforcement, brought those individuals to justice. The Division of Homeland Security and Emergency Management is working with the private sector to identify ways to enhance the security of networks to better protect those systems from attacks. Additionally, the West Virginia National Guard has developed a cyber response team to help recover from the impacts of these attacks. There are always financial impacts to these breaches, but there are also physical consequences.

In the end, the human factor is critical in preventing the intrusions that cause an incident, event or breach. We can take steps to prevent them, often at virtually no cost. Just as we do things, like brush our teeth for dental hygiene, there are also many things that can be done to promote *cyber* hygiene.

As part of a national campaign, The National Governor's Association, Governor's Homeland Security Advisory Council and the Center for Internet Security have joined to promote cyber hygiene. This campaign is a low-cost program that promotes five key priorities that, once implemented, are proven to dramatically improve an organization's cyber posture by addressing the vast majority of the known cyber threats.

The top priorities for better cyber health are:

Count - know what's connected to and running on your network.

Configure - implement key security settings to help protect your systems.

Control - limit and manage those who have admin privileges to change, bypass or override your security settings.

Patch - regularly update all apps, software and operating systems.

Repeat - regularize the top priorities to form a solid foundation of cyber security for your organization.

Just as homeland security begins with hometown security, cyber security begins with individual security. As we continue to look at all of the emerging technologies that make our lives better, we have to always keep security on our minds.

For more information and to take the cyber hygiene pledge, go to **www.cisecurity.org**.