Newsletter Sep 2014
Edition 3

School Preparedness Now

Safer Schools For a Better Tomorrow *Initiative*

The goal is to increase district-level preparedness to improve continuity of learning for PreK-12 schools and minimize impact of school-related disruptions and emergencies.

PHONE:
(609) 631-4531

FAX:
(609) 631-4926

E-MAIL:
ssbt@doe.state.nj.us

We're on the Web!
See us at:

www.state.nj.us/education/schools/security/task/

Individual Highlights:

School Preparedness Now *is a newsletter that provides New Jersey school districts with relevant, up-to-date, and practical information on safety & preparedness for schools and local communities.*

For more information contact the **K-12 *School Security Task Force*** *at* ***ssbt@doe.state.nj.us.***

NJ In the News: Cyber Security Awareness Month

Gen Tech, Gen Wii, Net Gen, Gen Next, Post Gen. Are any of these phrases familiar? These are the terms used to describe Generation Z, our current K-12 school community. This generation (1995 - present) was born into and living in an era whereby the main communication is the internet. Everyone's life, young and old, is now connected and impacted by the World Wide Web (the Internet).

The Internet is integral to our way of life, economy, and safety and risks. Being "connected" helps us immensely in our day-to-day productivity yet it can pose great threat and risk. These threats and risks can affect an individual, an institution, or an entire society. It is fundamental all persons have a basic knowledge of computers and cyber security to go forward in the 21st century.

President Obama has designated October ***National Cyber Security Awareness Month*** (NCSAM). The objective is to get information, resources and tips to help internet users take some common sense steps to stay alert of the dangers on the web and enjoy using computers safely.

A few useful sites to visit during NCSAM Month are:

- New Jersey Info Secure
- Cyber(smart:)
- Stop.Think.Connect

Share other valuable links and resources to schoolsecurity@doe.state.nj.us.

Hot Topics: The New Wave of Drilling

Schools have been conducting security drills for over three years since the Drill Law went into effect in November 2010. Most schools have attained a benchmark level of readiness for locking down and evacuation, the two primary responses in New Jersey applicable to various emergencies. Anecdotal reports from drill observations indicate some concern for "drill fatigue"; staff and students exhibit a decrease sense of urgency during drills that result from complacency and/or exercise monotony. As threats to schools evolve, drill exercises should too. More and more schools are installing swipe cards or using key fobs to access the facility, iPads for online attendance and/or accountability, smartboards for instruction, remote security cameras and other internet-reliant systems. As schools advance technologically, it is timely to begin considering how to plan to respond to cyber-related threats. Once plans have been developed they should be exercised. It is critical schools' cyber readiness does not lag; schools must work with key partners to ensure risks for cyber threats are considered and assessed.

Here are some useful tips:

- ✓ Include the district and/or school's IT manager on the school security planning committee.
- ✓ Integrate "cyber-smart" practices. Chat with students about being online.

It ain't what you don't know that gets you into trouble. It's what you know for sure that just ain't so.

— Mark Twain

Hot Topics (…cont'd)

- ✓ Request a Cyber Safety and Cyber Bullying Presentation.
- ✓ Visit NJDOE's Core Curriculum Content Standard – Technology Page.
- ✓ Know the law – The High Technology Crimes and Interactive Services Protection Act.
- ✓ Be sure your district and/or school has a policy on internet use (Tip: Consult with your County Prosecutor's Office). Communicate this policy to staff, parents, and students.

Promising Practices: Cyber Tabletop Exercise

A **tabletop** is a drill exercise that a group of people can do in a controlled setting to plan how to respond to an emergency. Tabletops are useful especially when planning for the unknown, like a cyber threat. Below is a tabletop scenario that can be used to assess how your district/school will handle the threat.

TABLETOP SCENARIO

Incident Thursday, June 6, 2014 2:00 a.m.
Recipient: Superintendent
District Size: 8,600 students, Pre-K to 12

Event Information
The superintendent receives an email from the NJ Office of Information Technology with an alert stating that a potential security breach was found in systems running Microsoft Windows XP with Service Pack 3 (SP3) and Microsoft Office 2003. Microsoft ended support for these systems on April 8, 2014 and these products have not received a security patch since. As the district still has computers running the Windows XP system the superintendent forwards the email to the district's IT designee. They start scanning the system/network when a breach is detected. At this time it is unknown the extent of the breach; however, it is thought that records, tests, and personal information on both current and former students and staff has been stolen.

Notes
This tests the flow of communication throughout the school district and community (parents, administrators, staff, police, etc.).

Things to consider:

- Does your district monitor network activity? Is there a process in place to address suspicious activity?
- Do you keep contact information on former students and staff members? For how long?
- Who is in charge of doing system updates and scans? In-house personnel, consultant, other?
- Are you running out of date operating systems and products? Do you have a process in place to upgrade these as they are phased-out?
- Who is in charge of doing system updates and scans? In-house personnel, consultant, other?

Questions for players

- ➢ What would be done with this information?
- ➢ Who would you contact with this information? When?
- ➢ How would you share this information with the community?
- ➢ Who decides what information to release?

A Special Message from the Director of the New Jersey Office of Homeland Security and Preparedness, Chris Rodriguez

Hello. My name is Chris Rodriguez. I am the new director of the New Jersey Office of Homeland Security and Preparedness (NJ OHSP). Prior to joining OHSP, I served for more than a decade in the Central Intelligence Agency (CIA), where I held a variety of analytical and management positions. In these roles, I closely collaborated with U.S. Intelligence Community partners at the federal, state, and local levels to identify and counter persistent threats to the United States and its allies. During my time at the CIA, I also oversaw an analytic unit that handled global economic and energy security, as well as related counterintelligence and cyber threats. In 2011 and 2012, I served as a policy advisor on Governor Christie's staff, overseeing OHSP, the Department of Law and Public Safety, the Department of Military and Veterans' Affairs, and the Department of Transportation. I bring the experience of working closely with the public and private sectors to coordinate and collaborate for a common good as an asset to this position.

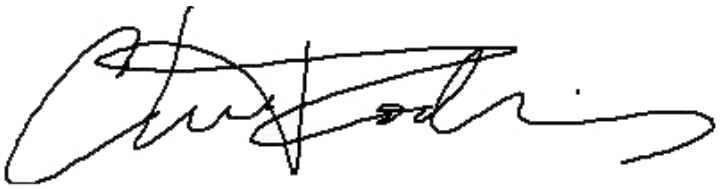
I was born and raised in Morris County, which makes this position that much more significant to me. I have a vested interest in service to all the people of New Jersey. I am excited to engage in this new role. As director, I intend to continue the tremendous work of my predecessors and identify new areas that are of significance to the continued security and preparedness of our great state. Specifically, the mission of OHSP is to protect the people of New Jersey by leading the state's counterterrorism and preparedness efforts and by coordinating emergency response across the state. It is my responsibility to assure that our intelligence and preparedness efforts are closely aligned with evolving risks and threats.

Chris Rodriguez, Director of New Jersey Office of Homeland Security and Preparedness.

The focus on Cyber Security in this edition of "School Preparedness Now" aligns well with a growing focus of this office. The cyber threat crosses all geopolitical, economic and demographic boundaries, including our schools. It is important that all of us in the school environment do everything we can to adopt strong cyber security strategies for our school networks and IT infrastructure, as well as, instruct our youth on how to safely navigate the Internet.

To this end, the Multi-State Information Sharing & Analysis Center (MS-ISAC) is conducting a national K-12 Computer Safety Poster Contest to encourage young people to use the Internet safely and to craft messages that will best resonate with their peers across the country. The contest will launch this fall and is open to all public, private and home-schooled students. I invite and strongly encourage all of our schools to get involved! Winning entries of this national contest will be included in the MS-ISAC 2016 Calendar, which is distributed to every state as part of the MS-ISAC Cyber Security Awareness Toolkit. For more information, contact Michael Vance at michael.vance@ohsp.state.nj.us.

Throughout my professional career, two things have stood out to me as key pillars of success in any organization – Service and Trust. For me, this office is the state's representation of these two pillars. I am confident the service we provide to our partners stem from trusted sources that are only concerned with the best interests of all New Jersey residents. I look forward to OHSP's continued commitment and partnership to ensure *Safer Schools for a Better Tomorrow*.



Significant Incidents that Make an Impact on NJ School Policies

January 17, 2014

Multi-Threat School Incident

On January 17, 2014, 'a bomb threat and a person with a gun' was called in to police causing a multi-agency response to a private school in Holmdel, NJ. The incident is one of several hoaxes police have received. The intention of these calls is to send tactical teams to respond to an emergency.

February 17, 2014

Swatting Incident

On February 12, 2014, a Swat team swarmed an unsuspecting home in Hamilton, NJ based on a call to 9-1-1 claiming there was critical incident involving hostages and a bomb. It turned out to be a prank that resulted from a dispute over a Twitter handle. For more on this story, click here.

*Note: *Although these incidents consume and waste resources, they serve as a reminder that schools must continue to prepare for the inevitable and build relationships with first responders to be ready for when a critical incident happens*.

AT-A-GLANCE: What is Swatting?

In simple terms, 'Swatting' is a phone prank intended to send the SWAT (Special Weapons and Tactics) or other tactical police units to an unsuspecting person's home.

Swatting is the tricking of any emergency service into dispatching an emergency response based on the false report of an on-going critical incident. Episodes range from large to small. Typically the fabricated police reporting stems from a prank, personal vendetta or to discredit someone (e.g. online gaming). Swatting can cause massive disruption in a community, school, or other place of business. This type of hoax, which deploys police, ambulances, fire and other emergency responders to a fabricated incident misuses valuable resources.

Did You Know? NJ Facts

1 – The Office of Homeland Security and Preparedness launched New Jersey as the first state to become a member of the Stop.Think.Connect coalition.

16 – In accordance with the US Department of Homeland Security designations, NJ OHSP has 16 critical infrastructure key resource (CIKR) sectors. The government sector includes public and private K-12 facilities as a subsector.

10 – The number of years since the inception of September as National Preparedness Month.

41 – The number of tropical cyclones (hurricanes) that have affected New Jersey in the month of September (1815 – present). Historically, the majority of storms have hit New Jersey during this month.

3+ – The number of years New Jersey's K-12 school community has been practicing security drills.

***Academic success cannot be achieved if students do not have a safe learning environment. Research has proven students who are fearful do not learn well*.**

For this reason, New Jersey is one of the most aggressive states when it comes to protecting our nation's most vulnerable population – **OUR CHILDREN.** New Jersey is serious about providing a top-notch education for all children in all communities *regardless of zip code.*

Prepárate Ahora: ¿Como Se Dice?

During summer 2011, NJ DOE hosted an 8-week course for state stakeholders on **Spanish as a Second Language** as part of the Planning for the Next Pandemic grant received to look at ways continuity of education could occur during emergencies. New Jersey recognizes the importance of linguistic and cultural competence in planning and implementing resources, as well as communicating and delivering messages across various mediums. In response to this growing need to better communicate across diverse populations, NJ is targeting key stakeholders that are integral during emergency planning, including state officials, law enforcement, administrators, and education personnel to enhance our state's linguistic competency. In this spirit, this newsletter will feature a Spanish Language Vocabulary Section.

Ataque Cibernético
-- Cyber Attack

Ciber
--Cyber

Conciente
--Awareness

Contraseña
--Password

Digital
--Digital

En Línea
--Online

Internet
--Internet

Privacidad
--Privacy

Respeto
--Respect

Responsabilidad
--Responsibility

Tecnología
--Technology

Generación Zeta
--Generation Z

Your District in the Spotlight: Red Bank Regional High School

Many of us may not readily understand the pros and cons behinds the 1's and 0's that surf the cyber world daily and are the foundation of what *makes our world go' round*, but that is one lesson the students at Red Bank Regional High School (RBRHS) did not miss. RBRHS houses the Academy of Information Technology (AOIT). AOIT, led by Mandy Galante and Jeremy Milonas, have developed a robust curriculum that "educates students with secure habits for their digital lifetime". Students in the AOIT are challenged throughout a 4 year high school course schedule that includes: Intro to Computers (9th Grade), Networking – how to build and fix computers (10th Grade), Cybersecurity - How to Stop Hackers (11th Grade), and Forensic – Finding Criminal Evidence on a Computer (12th Grade).

Ms. Galante shares, "it is important students not only know how to use computers but comprehend the basic workings of the digital system". This culture requires students to have a positive attitude toward technology and a responsible approach to understanding and navigating through the World Wide Web. In fact, parts of the curriculum have been extended to all of RBRHS's students. The Digital Literacy Course teaches core computing concepts every child should know including: effectively and safely accessing online information, netiquette, privacy, and ethical use of digital content. Keeping up with youth trends, the course is adding a component to address security issues specific to mobile devices since teenagers use their phones as their primary computing device.

The results of this program have exceeded all expectations. Aside from students being hands-on with the digital world, the Cyber security course was accepted by Syracuse University into their Project Advance Program; students at RBRHS receive college credit from Syracuse setting them up to be ahead of the academic curve in college! **We applaud Ms. Galante, Mr. Milonas, and the students of RBRHS's AOIT for creating a digital print for the next generation that will help us all be more safe and secure.**

Over 100 years of Academic Excellence

NEXT ISSUE

Highlights

Want to be featured in our next issue? Have a topic you want us to address?

Send us comments, promising practices, featured school districts, or an incident you have dealt with to:

ssbt@doe.state.nj.us

Welcome Ben Castillo, the state's new Director of School Preparedness and Emergency Planning.

Ben has provided extensive service to New Jersey through his experience in law enforcement for over 25 years. Most recently he has used this experience in the classroom setting as an educator at Ocean County College. Ben brings knowledge and training experience in establishing security measures for various state and entities to this new role in school security.

- ✓ **K-12 School Security Task Force Update**
- ✓ **Next Steps of *Safer Schools for a Better Tomorrow* Intiative**

About… The K-12 School Security Task Force

Established in 2006, the mission of The Governor's K-12 School Security Task Force is to further enhance the safety and security of New Jersey's public and nonpublic school students and, to the extent possible, develop standard benchmarks for education and law enforcement officials to help maintain consistency in school security protocols across a wide variety of safety and security challenges.