ASIS INTERNATIONAL SCHOOL SAFETY AND SECURITY COUNCIL NEWSLETTER

Volume 2 | Issue 4 April 2016

CHAIR MESSAGE

It's hard to believe it's already April, and some of the country is still seeing snow. The council members have been extremely busy over the last month, and it looks like it's going to stay that way based on what I read in my advance copy of the newsletter.

Our newsletter is now translated and posted in Spanish, thanks to Deyanira Murga, providing access to a much larger audience and we have worked extremely hard in sharing and posting information through our social media channels. This month presenter, Ben Gollotti, CPP will discuss using social media as an assessment tool for monitoring social activity that may be a precursor to school related incidents.

Brad Spicer and Mike Fagel will also be presenting over the next couple of months on analyzing a crisis event and how people act, react and respond. Please keep up the great work it will only strengthen our standing within the ASIS International Council Community.

Jason Destin, Council Chair

Council Leadership

Chair - Jason Destin, ABCHS IV
1st Vice Chair – Mark Berger
2nd Vice Chair – Kevin Davis, JD
Council Vice President – Les Cole, CPP
Secretary - Rebecca Bolante, PhD

Newsletter & Social Media

Newsletter Editor - Bernard D. Gollotti, CPP
Newsletter - Tom King, CPP
Newsletter – Tim Wenzel
Newsletter Intl. – Michael L. Johnson, CPP
Social Networking - Bernard D. Gollotti, CPP

SOCIAL NETWORKING UPDATE

The School Safety and Security Council has 3098 followers on Twitter, follow along at @ASISschoolsec, on LinkedIn join the School Safety and Security Group, and LIKE us on Facebook. Be an active supporter by following, liking, sharing and connecting for the latest news, best practices, and trends in providing a safe and secure environments where students, faculty, and staff can excel.

REINVENTING YOUR PHYSICAL SECURITY PERFORMANCE MAY JUST KNOCK THE BAD GUYS OFF THEIR GAME

By: Lawrence J. Fennelly, CHL III, CPOI, CSSI, CSSP-I
By: Marianna Perry, M.S., CPP, CSSP-I
Contributor: Bernard D. Gollotti, CPP

Let's talk about reinventing your physical security performance. Some time ago, we wrote that physical security assessments should be conducted at times of crisis. We have seen terrorist attacks in Paris, San Bernardo, CA, and Brussels. We have also seen the threat levels and security awareness increase in these areas.

Question: "What have you done recently to increase your level of physical security? Assessment? More training? Did you request that additional doors be secured? Have you looked at utilizing social threat assessments as a way to track social media activity? During these times of crisis, it is our recommendation that you also increase your level of protection. As national threat levels go up, so should your threat awareness.

It's during these times of crisis that physical security components get updated, and additional physical security measures often get approved. Conducting annual or monthly security reviews and improving security at your site will fuel overall security performance.

At times, physical security programs need a shot in the arm or a wake-up call. Increase the rounds made by your security officers within your complex to improve security coverage. Set up a schedule to check all alarm sensors and make sure they are working properly. Check also to ensure that all cameras are recording properly. All of your physical security components must be operational and providing you with the best protection possible.

If you haven't done so already, you may want to implement social threat assessments to monitor social media activity that may be a precursor to an incident. The use of social media assessments is growing in popularity since they can utilize technology to track hashtags, monitor social media activity in a defined area, monitor owners account activity and track keyword usage.

The combination of Reinventing Your Physical Security Performance and the addition of Social Media Assessments can be valuable tools in mitigating risk and knock the bad guys off their game.

COUNCIL MEMBERS SHARING EXPERTISE WITH OTHERS

Paul Timm, PSP will discuss "Effective Security Before and After School Hours" at the April 20, 2016, IL School Safety Conference

Rebecca Bolante, PhD, CRC, CTM as been appointed to the Oregon's governor campus safety task-force to review and recommend best practices related to safety. Oregon's Higher Education Coordinating Commission and Oregon State Police Campus Safety Task Force are leading this group. This group has the directive to focus on higher education and will report directly to the governor. This group will help address concerns and characteristics specific to higher education institutions.

Michael Johnson, CPP, will be facilitating the "Managing Risk and Security in International Schools" course for the Principals Training Center July 9-12, 2016, in Miami. Course participants will include Heads of School, Principals and other international school leaders. The Principals' Training Center is an organization that promotes practical and collaborative leadership training for international school leaders. (http://www.theptc.org/btc-106/)

Bernard D. Gollotti, CPP is volunteering his services to assist Bartram's Garden in Philadelphia in conducting a security assessment in prepreation of the Garden's expansion plans connnecting Bartram's Mile and the Schuylkill Banks. The expansion will run along the west bank of the Schuylkill River between Grays Ferry Avenue and 58th Street, on either side of Bartram's Garden.

CHILDREN'S INTERNET PROTECTION ACT PROTECTS STUDENTS IS AN INFORMATIONAL SHEET FOR PUBLIC AND PRIVATE SCHOOLS

By: Dr. Thomas J. Rzemyk, Ed.D., CHPP

The Children's Internet Protection Act protects students from access to obscene or harmful content over the Internet. In today's era, it is imperative for educational institutions across the United States to have internet safety polices and protocols in place in order to protect our children from both internal and external threats and incidents. Not only is it important, it is the law.

Does your academic organization have the proper tools, polices, and procedures in place? What type of firewall does your school have? Is it updated? Is it an older firewall? What specific rules are in place on your firewall? What specific internet traffic shaping rules are in place? Are you using the various network layers to block and permit data? What content is blocked and allowed? Do you have limitations are what content is permitted during certain times of the day? Do you have a primary and secondary internet content filter? Do you need more than one? If you have only one content filter, is it robust enough? What type of reporting features are in place?

Each academic environment is different, and a one size fits all solution will not always work. It is important to develop a customized plan that works for your environment; but also one that meets state and federal law. Through effective and efficient planning, schools can gain the upper hand on those attempting to gain access to secure internal networks.

Children's Internet Protection Act (CIPA) Definition

The Children's Internet Protection Act (CIPA) was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program – a program that makes certain communications services and products more affordable for eligible schools and libraries. In early 2001, the FCC issued rules implementing CIPA and provided updates to those rules in 2011. (FCC, 2015) . As of today, all schools accepting E-rate funding must meet and exceed a specific set of standards.

Internet Safety Policy Purpose

Schools and libraries receiving universal service (USAC) discounts for bandwidth and voice are required to adopt and enforce an Internet safety policy that includes a technology protection measure that protects against access by adults and minors to visual depictions that are obscene, child pornography, or — with respect to use of computers with Internet access by minors — harmful to minors. Has your school obtained funds from USAC and the FCC? If so, have you met the requirements? It is not only important to meet the minimum requirements, but to develop polices and procedures to make sure your educational institution stands apart from others. Can your organization lead the way for others? This is the mentality that each organization should seek when implementing polices and procedures to protect internal networks.

Federal and most state laws require that all institutions with responsibility for administration of the school or library seeking E-rate funding, must provide reasonable public notice and hold at least one public hearing or meeting to address a proposed technology protection measure and Internet safety policy. Also, an open question and answer forum must take place at the end of the presentation. Does you educational institution have a record of this public hearing? If not, it is imperative to have this on file for internal auditing purposes.

The Internet safety policy for K-12 educational institutions should address all of the following issues to include:

- Access by minors to inappropriate matter on the Internet and the World Wide Web (WWW)

- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications
- Unauthorized access including “hacking” and other unlawful activities by minors online
- Unauthorized disclosure, use, and dissemination of personal information regarding minors
- Measures designed to restrict minor’s access to materials harmful to minors

Technology Protection Measures

The Universal Service Administrative Company (USAC, 2015) defines a technology protection measure as a specific technology that blocks or filters Internet access. Educational organizations should enforce the operation of the technology protection measures during the use of its computers with Internet access. It must be understood by all constituents that an administrator, supervisor, or other person authorized by the authority with responsibility for administration of the school or library may disable the technology protection measure during use by an adult to enable access for bona fide research or other lawful purpose.

Example: Network Environment Announcement to Internal & External Stakeholders

> XXXX (Institution name) Internet Service Provider (ISP) is XXXX. The cutover to this specific ISP took place on XX/XX/XXXX (Date of implementation). At that time, the entire internal network went through several improvements to better protect students, staff, and faculty from both internal and external threats. XXXX (Institution name) utilizes a state of the art Unified Threat Management (UTM) firewall from a top tier organization, which is controlled from a central management server. The institutional firewall also has a built in content filter to prevent access to unauthorized materials as described in the CIPA excerpt above. There is also a secondary firewall and content filter built into other systems on the network for an added layer of safety and security. For confidentiality purposes all of the functions of the internal firewall and content filters will not be disseminated in this communication to internal and external stakeholders. Lastly, all students are required to have an Internet Safety Acceptable Use Agreement signed by parents or guardians in order to access network resources on campus. Please note that these polices can change at any time. Parents and guardians will be notified of any and all changes that take place by school administration. Also, all staff, faculty, and other network users are required to affirm and endorse an acceptable use policy as well.

Conclusion

In sum, the protection of our children, teachers, staff, parents, volunteers, and other school personnel is vital. Every protection measure must be put into place to maintain the integrity of an institutions network environment. If you have any questions or concerns about your institutions compliance with CIPA, I encourage you to contact your schools internal administration.

Note: This article is written for educational purposes only. It is not considered legal advice. For specific state and federal law compliance, please seek legal counsel. The author accepts zero liability for the information published in this article.

Contact Information: trzemyk@hotmail.com Cell: 402-213-8300.

SCHOOL SAFETY AND SECURITY SOCIAL NETWORKING ALERT RESOURCES

The use of Social Networking Alerts allows public safety organizations, businesses, and schools a way to provide just-in-time information and directions so that individuals can prepare in the event of an emergency. Social Networking Alerts shouldn't be used to share sensitive information, but to provide timely information to keep people safe and secure. You can learn more by visiting Facebook Safety Check and Twitter Alerts.

VULNERABILITY THROUGH RADICALIZATION

By Brad Spicer, SafePlans, LLC

What scenario could be worse than ISIS terrorists entering the U.S. through its southern border and carrying out an attack on our schools?   Consider the potential for ISIS to convincing people already in the U.S., possibly including students, to do it for them.

The foundation of ISIS ideology is creating chaos through savage attacks. The book "Management of Savagery: The Most Critical Stage Through Which the Islamic Nation Will Pass" by the terror strategist Abu Bakr Naji describes this core component of ISIS ideological training.

Management of Savagery teaches that success is obtained by enacting a vicious campaign of attacks that cause chaos and a decay government authority. This chaos creates the opportunity for ISIS to enact social services that are more stable than the savagery; thereby creating acceptance of their ideology.

Management of Savagery purports that U.S. intervention in the Middle East will lack resolve and can be curtailed though violence. An example states, "If the number of Americans killed is one tenth of the number of Russians killed in Afghanistan and Chechnya, they will flee, heedless of all else." If this doctrine is to be given credibility, an attack on U.S. soil is a plausible ISIS scenario to force the U.S. withdrawal from the Middle East.

The threat of radicalization, ISIS lust for media exposure, and possible ISIS affiliated camps reported near the southern border all highlight the need for improvement in U.S. preparedness efforts. Existing all-hazards plans and training should serve as a platform on which to develop hazard-specific programs. To address the threat posed by radicalization of students, school districts need to expand threat assessment programs to consider ideological-based warning signs.

ISIS is a terrorist organization that is implementing teachings from a book called Management of Savagery (also translated as the Administration of Savagery). It is hard to think of target that is more attractive than a school or college in the U.S.

THE WHYS AND WHY NOTS OF CERTIFICATIONS:

Robin C. Brown, Certification Committee - School Safety and Security Council

Back in the day, when I was a Special Agent for the FBI, they told us that with our Smith & Wesson Model 10 revolver, circa 1950s, and our FBI Credentials, we could get respect, get in just about any door, and get out most jams. Setting the gun aside for the discussion, those credentials did open many doors; got questions answered, and communicated the authority we needed. The Certification Committee was asked to discuss the need, or not, for credentials, certifications, licenses, diplomas, or other post-nominals for the conduct of our business, especially in the school safety and school security arena. Of course, the root of the question is motive for the effort to obtain them. We will set vanity aside, though it does have its place. Some employers require certain milestones for initial employment or job retention. These are situations where others drive the effort for us to improve. Sometimes circumstances such as unemployment or under-employment, will force us back into the classroom or to seek some third party validation of our skills and abilities. Many of the schools and universities with whom we work believe that credentials are important in their world and so expect it from their consultants and advisors. Our objective here is to raise the question about Return on Investment (ROI) of the time and funds to achieve that certification or degree.

Let us break this question into three larger pieces: Education, Certification, and License, each of which is a credential that provides us credibility in our various arenas.

Regarding education, we can find hundreds of quotes extoling its value. However, this statement of Benjamin Franklin is appropriate: “An investment in knowledge pays the best interest.” We get education when we are younger, generally to align ourselves with the expectations of a future employer or to mold a dream we have of our future selves. We seek it when we are older because of a personal interest or we see a need to remain relevant. Relevance is critical in the security industry. Products are removed from the shelves because of relevancy, people are asked to retire or are not hired because of relevancy. Companies close because of relevancy. To be recognized by peers, customers, and those seeking a credible opinion; education, be it formal with terminal degrees, a deep understanding of a new product line, or the beneficiary of personal research, we need to ensure our knowledge is relevant to the market, the threats presented to us, and the various risks created in our environments.

A lack of education can make us personally irrelevant. We should be aware of our education deficits, as they occur and move quickly to remedy them. More than ever before, there are excellent, focused, credible, and affordable graduate degree programs available to us in classroom, blended, or on-line formats. Some are traditional, while many are research based, self-paced, team-modeled, and with other intriguing options. ASIS International compiled a list of education programs offering degrees in the security industry:

https://www.asisonline.org/Membership/Library/Academic-Student-Center/Documents/Academic-Programs-in-Security.pdf - search=security degrees

Results: increased credibility, increased self-esteem and self-confidence; added value to your employer, added ability to market one's self as an subject matter expert, as well as keeping one's mind healthy.

Regarding certifications, there are more than 4,000 credentialing groups, though only 10% have third party validation. Some groups "sell" certifications just like some so-called universities or diploma mills sell degrees. Selecting those that are appropriate for your area of expertise is primary. Considerations might also include the certification's industry respect; does it require continuing education, again to maintain relevancy; has it been deemed appropriate as requisite for employment, for contractual relationships. If the certification is obtained without a significant experience and/or education base, without demonstrated skills by testing or validation by others; but for a healthy purchase price, the industry will likely not accord it the respect necessary for your ROI on the cost. A few ways to select appropriate certifications for yourself in an industry is to ask your customer base what they look for in a consultant or advisor; determine what your competitors have done or achieved; what do your professional associations recommend, or even your insurance underwriters for recommendations. Association with most professional organizations sometimes comes with encouragement to certify with their organization, to obtain the full benefits offered. The continuing education requirements linked to most of the widely-accepted certifications also enhances one's relevance in the industry.

Regarding licenses, we find this sector expanding also. For some jurisdictions, licensing is a funds raiser and way to set a performance standard. For most, it is simply permission to practice in a certain field. The licensure program, as whole, protects the public from unlicensed or disciplined professionals also. We appreciate these in the traditional professional sector jobs like physician, dentist and architect because the consequences of working with an unlicensed person may be huge. If a license is appropriate or even marginally so, strongly consider getting one. Licensure may reduce your professional liability insurance because you are now vetted by a governmental third party. Note too that licensure often requires a performance bond and professional liability insurance. The adage of one being "licensed, bonded and insured" still provides value and comfort to a customer.

Certificates is another growing area of professional development. These include programs taught in a formal education environment but are specialized in a narrower area. Homeland Security is a broad topic that is used to offer academic degrees, certification programs, and certificates. Note that the difference between certification and certificates is important to know. A certificate means that you successfully completed a prescribed program be it education, skill acquisition, or program attendance. There are no later contingencies to the certificate, it does not expire and has no conditions for use. Certification though requires meeting certain entry requirements, often has renewal requirements, sometimes performance requirements, and sometimes industry participation requirements. One that comes to mind is the excellent terrorism program taught by distance learning from the University of St. Andrews http://www.terrorismstudies.com/

There are many excellent certificate programs in Homeland Security listed on the FEMA Emergency Management Institute's site https://training.fema.gov/hiedu/collegelist/dhscertificate/. These certificate programs are generally tuned for current regional and national risk models. FEMA also offers many on-line courses free of charge that are very appropriate to security professionals. ASIS International also offers a broad range of certificate programs noted here: https://www.asisonline.org/Education-Events/Certificate-Programs/Pages/default.aspx

We have all seen the bumper stickers informing all that their kid is an honor student at some school. Initially, that third party validation of a student's achievements made the parents proud, the student embarrassed, and the school richer for the sale of the sticker. They have now morphed to a new collection of stickers ranging from, "I was an Honor Student – I don't know what happened." to "My Kid Beat up your Honor Student." And so the value of the first is diminished by public perception and comment.

The post-nominals we tag after our business names also speak to our customers, employees, peers, and our industry. We also see international trends requiring businesses to have ISO certifications in many of their processes. We can make assumptions too with tags such as Inc. LLC, PC, Co. Ltd., etc. Each of these tells the reader about our company structure and risk assumption.

There are also honorary titles or titles offered in recognition of service in the field, service to country or to ones alma mater. Honorary degrees connote recognition. A post-nominal such as MBE (Member of the British Empire) is honored in many circles. Many professional organizations award Fellowship status to a member based on service and other significant criteria.

Many have contributed to a definition of a credential in Wikipedia leaving this one: "A credential is an attestation of qualification, competence, or authority issued to an individual by a third party with a relevant or de facto authority or assumed competence to do so..."

...And our basic dictionary tells us that credibility means, "The quality, capability, or power to elicit belief: "The scandals posed a crisis of credibility for collegiate athletics" (Taylor Branch). 2. A capacity for belief.

The challenge for all of us on this council, as well as in our various professions, is to remain relevant, credible, and one to whom someone turns for counsel.

CALENDAR OF EVENTS …

April 20, 2016 2016 IL School Safety Conference (Free)

Council Member Presenter Paul Timm, PSP will discuss "Effective Security Before and After School Hours"

Registration: http://www.gbriskcontrol.com/retasecurityregistration/

Future Events

Threat Assessment Training for Campus Teams and their Partners

Registration $395.00

To save your spot, contact rebecca.bolante@chemeketa.edu or 503.409.1385

June 16th and 17th, 2016

Shoreline Community College, Shoreline, Washington

November 9th and 10th, 2016

Umpqua Community College, Roseburg, Oregon

November 21st and 22nd, 2016

Honolulu, Hawaii

ASIS SCHOOL SAFETY AND SECURITY NEWSLETTER – GET PUBLISHED

If you have ever thought about writing and want to give it a try, then now is your chance. Please submit any article on School Safety and Security and the newsletter team will make sure it gets into the newsletter. Being published in the newsletter will generate professional exposure throughout ASIS and allows you to share your expertise with others. We do need your help in putting together a great newsletter. If you have something you are passionate about, please submit an article and the newsletter team will get it published.

For more inforamtion contact Bernard D. Gollotti, CPP at bgollotti@largocs.com