February 2013

Holistic Information Security Practitioner Institute

HISPI Program Update

Hello from your HISPI leadership team. This issue of the HISPI newsletter comes to you on the heels of the President's Letter sent to all active HISPI members in December 2012. If you missed the letter from Ralph Johnson, please check your email as it is packed with the latest updates and activities relating to our organization. We are excited about this New Year and we look forward to growing our organization in 2013. This issue is packed with great information. We hope that you find it informative and we welcome your comments.

Renewed Certificates

In the next few weeks we plan to reissue and distribute renewed certificates so if your certificate is expired and you have renewed your certification and remain in good standing you should receive a new certificate in the next month or so.

Membership Dues and CPE Updates

In order to provide an on-going value to our members and to ensure all stay in good standing, please pay membership fees and update CPEs online. Your attention to his matter is greatly appreciated. Notices recently went out regarding outstanding 2011 and 2012 membership fees. Beginning this year reminders will be sent monthly for membership fees due in 2013.

Information on CPEs can be found on our web site under the Certification tab.

In the News

Your HISPI secretary, David Wright, had the honor of interviewing **Taiye Lambo**. Taiye is the founder and current treasurer of HISPI. In this interview, Taiye takes us through the early days of HISPI leading up to current date activities including our sponsorship and Cloud Security Alliance initiatives. You can access this podcast by logging into the HISPI website and selecting on the link **Newsletter interview with Taiye Lambo, Founder HISP and HISP Institute. Click here to listen/download the podcast. Earn 1 CPE for this podcast** under the Downloads area.

Tom Stamulis, HISPI Accreditation Officer will moderate a panel discussion at the upcoming RSA conference. The title of the panel is "Information Security Certifications: Do They Still Provide Industry Value?", please read more information here.

Ralph Johnson will be a panel member at the National Associate of Counties (NACo) Legislative Conference in Washington DC, March 4th. The topic is Cyber and what county officials should know. For more information, please see the NACo announcement.

Taiye Lambo will be speaking at the ISACA Silicon Valley Winter Conference in Santa Clara, California scheduled for March 7-8. HISPI and CloudeAssurance are co-sponsoring as Platinum Sponsors and for members interested in attending, contact Taiye Lambo to utilize one of the complementary passes available to HISPI as a sponsor. Please read more information here.

Herein, you will also find a summary of the **Presidential Executive** order signed on February 12, 2013.

Useful Links

HISPI Home Page

Events

Training

Breach Matrix

HISPI on Facebook

Member Profile

Taiye Lambo

Upcoming Events

Training

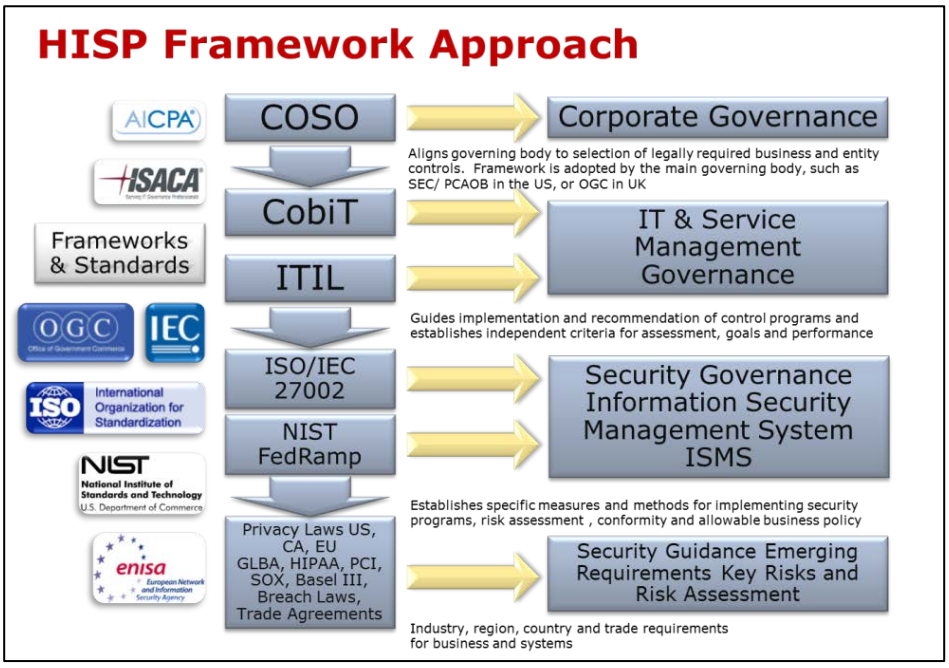
Executive Order – Improving Critical Infrastructure, Cybersecurity

As many of you in information security may already be aware, on Tuesday February 12th President Obama signed an Executive Order that outlines the critical nature of the cyber infrastructure of the United States and sets forth provisions for improving the protections of this infrastructure. In my opinion this has been a long time coming.
One of the provisions in this executive order is section 7 entitled "Baseline Framework for Reducing Cyber Risks to Critical Infrastructure". This provision calls for the creation of a framework designed to reduce such risks. A key portion of this section and one that is of particular interest to HISPI reads:

> *"The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible. The Cybersecurity Framework shall be consistent with voluntary international standards when such international standards will advance the objectives of this order…"*

The development of the framework has been assigned to the Director of the National Institute of Standards and Technology (NIST). The section goes on to say:

> *"The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure."*

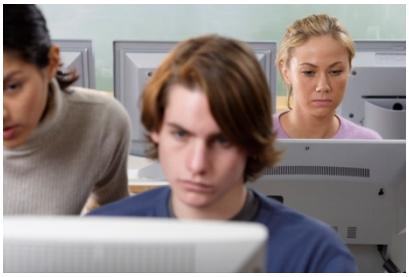


Based on international standards such as ISO 27001, 27002, and 27005, CobiT and ITIL HISPI already has such a framework, which you can see diagrammed to the right. HISPI's years of experience in not only educating Information Security Practitioners on how to implement leading international risk-based standards but also how to integrate these proven standards with legal, contractual and regulatory compliance requirements using an integrated framework approach positions our organization to be at the forefront of this initiative. To that end, Taiye and I are already reaching out to our contacts at United States National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS) to volunteer the services of HISPI in developing the prescribed Cybersecurity framework. This is set to be an exciting and rewarding experience for our membership. We will keep you posted as we move forward.

If you have not already read the executive order and wish to do so it can be found here.

Ralph Johnson, HISPI Governance Board President

Training Update



Online Training Course Availability

The online course is now complete and will be available in two options; one without the printed materials for $245 and one with the full set of printed materials for $495. Current HISP certified members may take the online course as a refresher and receive CPEs. When registering on the site, be sure to enter your certificate number to receive the member discount of $50.

Partnership with New Horizons of Cleveland

In September 2012, HISPI and ASMGi of Cleveland, Ohio formed a partnership with New Horizons of Cleveland. The focus of the relationship was to promote and grow the HISP certification by making it easier for students to register and attend HISP training classes.

New Horizons, the world's largest independent provider of training, will provide the expertise and reach required to promote the class. With over 1,500 sales professionals located in 60 countries around the world and their Online Live™ (OLL) virtual delivery platform, New Horizons will enable an HISP instructor to deliver a live class simultaneously to students from the United States and beyond. "The New Horizons network and OLL provides live access to the best instructors, like Gary Sheehan from ASMGi, to students from multiple geographies at the same time", said Tom Bender, General Manager and Owner of New Horizons of Cleveland. "This provides student access to high quality instruction, with live video and audio, that is not limited by enrollments from a single location. It enables us to reach more students, and run more classes more often."

In addition to running the HISP certification classes, New Horizons and ASMGi will continue to deliver a series of free webinars that promote HISP training and the Institute. Marketed by New Horizons, the HISP Institute and ASMGi, the webinars educate participants about how to build an effective information security management system. These webinars reference the HISP approach and create interest in the class. "New Horizons mission is to educate its customers. The webinars inform attendees about the value of HISP and open a path for students to enroll in the class," said Mr. Bender. Moving forward, New Horizons, HISPI and ASMGi established class dates each quarter for the remainder of 2013. New Horizons will continue to promote the training classes as an important part of their security portfolio. Details of the classes can be found at www.nhgreatlakes.com.

2013 HISP Course Schedule

The following table shows the public classes HISPI is offering in 2013. Encourage your information security professional peers to visit our web site at www.HISPI.org and register for one of these courses.

Course Name	Date	Location	Price
HISP Certification Class - 5 Day	March 19, 22, 26, April 2 and 5 King County Hosted Course	Seattle, WA	$1,495 (USD)
HISP Certification Class - 5 Day	April 15 - 19	San Jose, CA	$2495 (USD)
HISP Certification Class - 3 Day	May 14-16	Cleveland, OH	$2000 (USD)
HISP Certification Class - 5 Day	July 15 - 19	Detroit, MI	$2495 (USD)
HISP Certification Class - 3 Day	August 6-8	Cleveland, OH	$2000 (USD)
HISP Certification Class - 5 Day	September 17, 20, 24, 27, October 1 King County Hosted Course	Seattle, WA	$1,495 (USD)
HISP Certification Class - 5 Day	October 14 - 18	Dallas, TX	$2495 (USD)

Member Profile: Taiye Lambo CISSP, CISA, CISM, HISP, ISO 27001 Auditor

Taiye Lambo is a security subject matter expert in the area of Information Security Governance; with 20+ years IT including 15 years of experience assisting various organizations globally to build robust, comprehensive, effective and sustainable information security programs through the integration of internationally accepted best practices, including ISO 27000, COBIT, COSO, ITIL and NIST. He founded the UK Honeynet project – www.honeynet.org.uk and the Holistic Information Security Practitioner (HISP) Institute – www.hispi.org and also founded the HISP Program, which is the first integrated training and certification for Governance, Risk Management and Compliance (GRC) which he has personally delivered in the following countries **USA, UK, Greece, Jamaica and South Africa**.

He successfully executed critical information security projects for a number of UK & USA government agencies and also serves as an Independent Consultant to the United Nations auditing the ICT Governance and Security Management Programs of various United Nations Missions internationally in various African and Caribbean countries including Monrovia, **Liberia** (UNMIL) and **Haiti**, Caribbean (MINUSTAH), Nairobi, **Kenya** (UNON), Arusha, **Tanzania** (UNICTR) and Abidjan, **Côte d'Ivoire** (UNOCI).

In the commercial sector he has completed Consulting engagements for clients in various verticals including Software, Manufacturing, Financial Services and Healthcare sector.

He was the Director of Information Security for John H. Harland (now Harland Clarke), the leading provider of solutions to the Financial Services industry in the USA, including check and check related products and accessories, direct marketing solutions, and contact center solutions.

He has dual expertise as a hybrid technical and business information security consultant with a pragmatic holistic approach to the management of information security and regulatory compliance, as well as a subject matter expert on Information Security governance and compliance relating to regulatory standards such as HIPAA, Sarbanes-Oxley Act, Gramm-Leach Bliley Act (GLBA), FDIC and others. His presentations at security events include conferences organized by **MISTI, ISSA, InfraGard, ISACA, CPM, SOFE, EDUCAUSE, HITRUST, SECUREWORLD EXPO and KUWAIT INFO SECURITY CONFERENCE & EXHIBITION.** He also served on ISACA COBIT working group for several years during the development of COBIT 3rd and 4th Editions.

Taiye also serves on the Cloud Security Alliance (CSA) Quality Assurance (QA) team on behalf of his organization the HISP Institute (HISPI) for the development of the Cloud Controls Matrix (CCM).

Taiye is President and Founder of eFortresses, Founder of the Holistic Information Security Practitioner (HISP) Institute (HISPI) and Founder of the ***CloudeAssurance*** SaaS platform, the industry's first truly risk-intelligent rating and continuous monitoring system for assurance of cloud service provider's security, governance, risk management and compliance. In the United Kingdom, he founded a successful information security firm CyberCops Europe, gained assignments in the USA for commercial and government agencies where he continued Information security and compliance consulting and became a subject matter expert in several of the current regulations. He has established numerous valuable contacts internationally and has name recognition in the information security/regulatory compliance space globally.

With a Bachelor's degree in Electrical Engineering from the University of Ilorin, Nigeria he also earned a Masters degree in Business Information Systems from the University of East London (United Kingdom).

Please review Taiye's LinkedIn Profile and recommendation's at http://www.linkedin.com/in/taiyelambo

Key Message

Enterprises need to follow a positive security model, identify applications that are required by business, establish policies of approved applications and enforce positive control of traffic.

Member Submitted Article by Arun Warikoo

Enterprise Security – The Way Forward

Traffic on an enterprise network has changed dramatically in the last five years due to the tremendous growth of social networking, mobility and cloud solutions. Enterprises are now employing them as strategic tools for driving business. It is common to see social networking applications like Facebook or twitter, Web 2.0 applications like Webex, and/or Cloud based applications like box.net. The growing need to support an increasingly mobile workforce and the emergence of Cloud solutions has transformed an enterprise network from more private towards a more public.

Need to readdress how security is employed today

Enterprises today follow the Negative Security Model also known as blacklisting. The focus is more on preventing that is known to be bad and not on traffic that is deemed good. With enterprises opening more and more towards the Internet, the threat from external vendors is bound to increase. According to the 2011 Data Breach Investigations Report, hacking and malware were the top two external threats enterprises were facing in 2011. Web applications are the one of the most common threat vectors for propagating malware.

Applications today are capable of operating on non-standard ports. Many applications like IM, peer to peer, file sharing or VoIP are also capable of port hopping. The growth of application based traffic on the network and their ability to port hop or use non-standard ports has rendered a negative security model ineffective. As the focus is to block what is bad, enterprises are playing the catch up game.

Reduce the Attack Surface

There is an urgent need to address how network security is employed today due to the changing traffic patterns on the network. In order to protect the network from changing threat vectors, enterprises need to follow a Positive Security Model that was first evangelized by the Orange Book.

This implies traffic that is explicitly permitted by policy and deemed to be good is allowed and everything else is denied by default- whitelisting

Whitelisting enables the enterprise to reduce the attack vectors and regain full visibility and control of exactly what traffic is allowed into the network. By incorporating a positive control model, security teams can focus on enabling the approved applications, as opposed to constantly trying to stay up to speed with all of the applications that they want to block.

This approach can immediately preclude large numbers of applications from ever touching the network, while dramatically reducing the number of vectors that botnets can use to get in or out of the network.

Conclusion

In order to deal with the changing threat landscape, a negative security model is not going to work. Enterprises need to follow a positive security model, identify applications that are required by business, establish policies of approved applications and enforce positive control of traffic.

About the Author

Arun Warikoo, is a Network Security Architect at Beckman Coulter in greater Los Angeles area.

Holistic Information Security Practitioner Institute

8075 Mall Parkway, Suite 101367
Lithonia, Georgia 30038
United States of America

888.247.4858
720.293.2118
questions@hispi.org

Find us on the Web:
https://www.hispi.org

Holistic Information Security Practitioner Institute