

July 2011 | Holistic Information Security Practitioner Institute |



Holistic Information Security Practitioner Institute

HISPI Program Update

Hello from your HISPI leadership team. This issue of the HISPI newsletter calls to attention some administrative requests for the HISPI members. You all worked hard to achieve this certification so let's cover a few points that are important to keep in good standing.

- Member profile information – Please update your member profile information found online through the HISPI home page. This is important so that the leadership team can reach you with news, program updates, or administrative matters.
- Paying your membership dues – Very important. Certainly understandable that times are hard and all have a tendency to forget, but paying the membership dues is important in keeping basic operations running in the program. The funds are used to promote the program and to facilitate membership activities. Please contact John D. or Taiye if you have questions about your specific situation. Otherwise, we will look forward to receiving outstanding membership dues.
- Submitting your CPEs – Also very important. CPEs tell HISPI that you continue to practice in the data privacy and security space. This also helps you keep up with current trends and how best to apply HISPI principles in your everyday work. If you have questions about what CPEs apply, please reach out to a member of the leadership team.

We hope that this newsletter proves useful, informative, and at times adds just the right amount of humor to bring a smile. Remember, protecting assets is hard work and we all can use some positive tools and support. Here we go...

In the News

HISPI Offers Membership Discounts to CSA Members (Source: CSA)

The Cloud Security Alliance (CSA) and the Holistic Information Security Practitioner Institute (HISPI) are offering a 50% discount on HISPI membership to all CSA LinkedIn group members. Please inform your CSA colleagues of this significant opportunity. Those interested can apply for this offer at: <http://cloudsa.eventbrite.com/>. [Full Story](#)

Cloud Security Alliance Set To Publish Registry for Secure Cloud Computing (Source: CSA)

The Cloud Security Alliance (CSA) is set to publish a public registry in the fall of 2011 meant to serve as a point of reference for securing cloud computing. The "CSA Security, Trust & Assurance Registry" is the result of efforts by CSA to consolidate self-assessments submitted by the many cloud providers on controls they maintain to secure their service. The registry can also be used by customers to assess providers. The initiative will be announced at the upcoming Black Hat conference. [Fully Story](#)

Useful Links

[HISPI Home Page](#)

[Events](#)

[Training](#)

[Breach Matrix](#)

Member Profile

Ralph Johnson

Upcoming Events

[Training](#)

Member quotes: Protecting data is hard work and is not glamorous, but I finally have a sense of being part of a special group of people with a common, important goal. – David Wright

Key Message

Without leadership vision and commitment, yours will be an uphill battle. Gain support from executive leadership through good communication. Your organization brand is not something to take lightly. After all, where would you be if your organization were not a trusted leader with good brand reputation?

Practical Application of HISP by Ralph Johnson

Section 0.7 of the ISO 27002 standard lists a number of critical success factors. Experience has shown me that these are quite accurate and necessary for the success of an information security program. In my opinion the most important one is that of “visible support and commitment from all levels of management”. Without this support for the information security program policies, standards and guidelines will be unenforceable. Specifically the support from the top of the organization is essential. Support from the CEO, Board, and especially IT management (CIO and directors).

Another theme that permeates throughout these critical success factors is that the information security program should support the business objectives and fit within the existing corporate culture. These two concepts are intertwined in that the objectives of the business will also be heavily influenced by the organizations corporate culture and vice versa. Consideration of corporate culture is essential in order to achieve acceptance and cooperation with the information security program. If the program acts contrary to the corporate culture and thus does not support the business objectives the information security team will constantly face an uphill battle and information security is unlikely to achieve any significant degree of success.

A recent experience of one of the students in my last HISP class shows just how the course can be immediately valuable. The student in question is an IT manager representing one of the departments of King County. Shortly after our final class session she was asked by the Director of the department she represents about ISO 38500. After performing some research on what ISO 38500 is (she was not immediately familiar with this standard and honestly was not sure why the Director was aware of it either) she discovered that ISO 38500 is the International Standard for Corporate Governance of IT. She learned that while this is a solid framework, as are all ISO standards, it is not as robust as what she had just learned about CobiT in the class. Using her new found knowledge of CobiT she was able to have a valuable discussion with this Director and guide the Director to a better understanding of IT governance and information security.



Key Message

Security is the responsibility of everyone in an organization, regardless of what role you play.

Member Profile

Ralph Johnson works for King County in Seattle, WA. He began his career at King County in 1989 with a very short stint as an Autopsy Assistant. The next 15 years were spent serving in various IT roles in the Department of Public Health. In 2001/2 he was exposed to the wonders of HIPAA and became directly involved with information security.

Ralph's InfoSec career progressed as follows:

- Earned his CISSP in 2003
- Became the county Security Architect in 2004
- Became the first Information Security and Privacy Officer in 2005
- Earned his CISM in 2006
- Earned CIPP/G in 2007
- Earned the HISP designation in 2008
- Joined the HISPI board as Secretary in 2009
- Became a certified HISPI instructor in 2010

Ralph's true passion for security falls to educating people about risks, their role in reducing those risks and helping find appropriate and acceptable controls to mitigate them. He enjoys the challenge of communicating the importance of information security.

Ralph enjoys eating at nice restraints and watching movies and finds this as a good way to unwind after a long day of protecting his organization.

Ralph's favorite quote is from Bruce Schneier "Security works best when the entity that is in the best position to mitigate the risk is responsible for that risk." This emphasizes to him that information security is not just the responsibility of the governing board, CEO, CIO or even the CISO but every employee of an organization.

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