November 2011

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 Cyber Security Month. On October 3, President Barack Obama officially proclaimed October as National Cybersecurity Awareness Month. In this proclamation, the President states, "Every American has a stake in securing our networks and personal information, and we are working across the public and private sectors to ensure coordinated and planned responses to cyber incidents, as we do with natural disasters." As members of HISPI, we can feel proud that our efforts and the mission of HISPI play a key part in protecting information, assets, and people not just in the United States, but globally. Although we may stop and celebrate our accomplishments, there is still much to do as we continue this journey….

In the News

FITSI (Federal IT Security Institute) Offers for HISPI Members:

- 25% off of courseware purchased until end of 2012 (available 3 qtr 2011). Enter promo code HISPI2012.
- One free exam voucher good until the end of 2012 for any HISPI member that becomes a FITSI member between now and the end of the year. Enter promo code HISPI2012.

On a related note FITSI and HISPI have a strategic partnership with recognition that each offers "value added" certifications. The partnership maintains a shared goal, which is to develop a common set of certification criteria. In addition, HISPI offered discounts off membership to FITSI certification holders and as a result gained 6 new members in just the last two days. For those interested in learning more, please read the Full Story.

Major Cloud Providers Will Participate in CSA's Security, Trust & Assurance Registry

On November 16, the Cloud Security Alliance (CSA) announced that Google, Microsoft, Verizon, Intel and McAfee are set to publish reports to the public registry. This registry was established 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 compare cloud service providers. Full Story

In support of this effort for transparency, the HISPI is launching the Cloud Assurance Assessor Program (CAAP). Once a self-assessment is completed by the Cloud Service Provider, an HISPI Qualified CAAP independent assessor can be contracted to validate the self-assessment provisional rating and associated evidence along with any internal requirements.

CAAP Assessed companies and their Assessors must meet a set of minimum requirements. For more information please e-mail questions@hispi.org.

Useful Links

HISPI Home Page

Events

Training

Breach Matrix

HISPI on Facebook

HISPI LinkedIn Group

Member Profile

John B. Sapp Jr.

Upcoming Events

Training

Cloud Assurance CAAP Assessor Program

Practical Application of HISP by John B. Sapp Jr.

In the ISO 27002 Code of Practice, Section 12 outlines security requirements for Information systems acquisition, development and maintenance and in summary states that information security must be taken into account in the SDLC processes for specifying, building/acquiring, testing, implementing and maintaining IT systems.

In my experience, this section seems to be routinely overlooked in its entirety or highly under-utilized by organizations when they procure off-the-shelf software, (OTSS replaces COTS due to the increasing amount of open-source software on the market today), and more importantly outsourced development of software applications for information systems. Subsection 12.1 clearly states you should have security requirements of information systems, which should be interpreted as the need for minimum set of functional security requirements. Most software developers and surprisingly many information security professionals follow the philosophical approach of security requirements being "non-functional" requirements, however I would argue that they are "functional" requirements on the merit of the fundamental expectation of the information system to protect the confidentiality, integrity and availability of the data and the information system itself as a feature and function of the information system.

I believe that subsection 12.2 supports my argument as it requires "correct processing in application systems", and identifies the obvious when it states that "purchased software should be formally tested for security, and any issues risk-assessed." As the code of practice continues, it highlights cryptographic controls (12.3), security of system files (12.4), security in development and support processes (12.5) and last but certainly not the least, technical vulnerability management (12.6). Many organizations utilize application security scanning tools to identify security flaws and vulnerabilities, however not all software vendors have a process by which you can report these flaws nor do they issue security bulletins to address these proactively. This is where I can say that Microsoft got it right when they launched the Trustworthy Computing effort in 2002.

My most recent experience and practical application of HISP occurred within the past 12 months when I launched an effort to develop a software security assurance program and associated policy. Consider the fact that our organization has a "growth by acquisition strategy" for the healthcare IT segment and is quite federated in its operations when it comes to developing healthcare technology solutions, which made this an even more daunting task.

The HISP approach to information security played a major part in the vision and strategy. I leveraged the mapping of ISO 27002 Section 12 and NIST 800-53 as the foundation of this initiative and it proved to be my saving grace when I presented the approach and value proposition to senior executives. We were able to further map this with CMMi to incorporate security into our software development process across the enterprise as part of a holistic approach to information security within the products that we deliver to the healthcare market with the protection of sensitive patient information in mind. Our executives also learned that we could become more efficient and consistent in our responses to information security questionnaires that are increasingly becoming part of the procurement and contract negotiation process with customers from both the public and private healthcare sectors.

As I enter into my new role of transforming and productizing information security to drive innovation within the healthcare industry, it is the principles of a holistic approach to information security that will anchor the vision and strategy.

Key Message

Ask and answer three questions when it comes to information security:

1) What?
2) So what?
3) Now what?

Member Profile - John B. Sapp Jr. – CISSP, HISP, CRISC, CGEIT

John B. Sapp Jr. is employed by McKesson Corporation in the Office of the CISO and matrixed to the Office of the CTO, where he is based in the metro Atlanta area. His affiliation with McKesson began in 2001 when he spent two years as a consultant who developed business solutions for their warehouse management and supply chain systems. After a contractor reduction he spent time with Birkenstock Footprint Sandals and Cost Plus World Market before being contacted by McKesson to return as a full-time employee as a Senior IT Project Manager in 2005. Although it was not exactly a role that John envisioned himself transitioning into, it turned out to be the beginning of his career transformation from software development into Information Security and IT Risk Management.
John's Information Security and IT Risk Management career path included:

- Becoming McKesson – US Pharma Business Unit Security Leader in 2007
- Earning CISSP certification in 2008
- Obtaining CGEIT certification in 2008
- Promotion to Director, Product Development Standards – Security & Risk
- Achieving HISP certification in 2010
- Joining the HISPI Advisory Board in 2010
- Gaining CRISC certification in 2011
- Becoming a HISPI certified instructor in 2011
- Founding ASSURE Technologies, LLC to develop security risk intelligence solutions
- Becoming Senior Director, Information Security Product Management & Innovation

John is at his best when given the creative freedom to develop a vision and strategy for information security as evidenced by an award winning risk management program dubbed PRiME (Product Risk Management for the Enterprise), which he developed to delivered a center of excellence approach for managing the risks associated with software product development at McKesson. He has an insatiable passion for sensitive data protection with a particular interest in healthcare as the industry evolves from its legacy environment into the cyber-era.

John is an avid sports fan who has coached youth football for 10 years and high school football for five years and also enjoys watching movies (A Few Good Men is his favorite… "You can't handle the truth") and is definitely a foodie who enjoys a variety of cuisines. He spent 12 years in the San Francisco Bay area where he had the opportunity to experience the Napa and Sonoma Valley wine region on a regular basis.

John's favorite quote is "A Fool with a Tool… is STILL a Fool", which can be applied to numerous scenarios within the IT world, however he finds this especially true when organizations attempt to convert software developers into security professionals by simply giving them tools to use for the purpose of identifying security flaws in their applications without the benefit of a secure development process that includes security awareness, education and training. Additionally, tools generate an inordinate amount of technical data that must be converted into business risk context in order to provide security risk intelligence for executives to make risk-based decisions and understand the value proposition of information security as an enabler to business operational success. John believes in the philosophy of answering three questions when it comes to information security:
1) What? 2) So what? 3) Now what?

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