



The 5 Keys to Compliance Leadership

Security PS is the Midwest's Leading Independent Application and Network Security Consulting Firm.

We offer services in the following areas:

- Web Application Security Assessments
- Network Security Assessments
- Source Code Security Reviews
- Password Compliance and Analysis
- Training
- Vulnerability Testing and Management
- Security Compliance
- And much more...

New compliance issues have cropped up for businesses in the last few years due to the emergence of the different regulatory and industry standards such as Sarbanes-Oxley, GLBA, HIPAA and PCI. These regulations have brought attention to the importance and challenge of managing security efforts. Some organizations have addressed this challenge by creating a new role within the organization: the compliance leader.

The compliance leader's title varies by organization. These titles include: Chief Security Officer (CSO), Chief Information Security Officer (CISO), Information Security Officer (ISO), Risk Manager, Director of Audit and Compliance, and many others. While the title may vary, the role does not. These individuals must lead their company down a path of compliance and due diligence. So how do you lead to compliance? Follow these

five steps and you'll be well on your way.

1. Balance the Needs of the Business

This job is not without its challenges. One of the difficult aspects the compliance leader faces is balancing the business needs and objectives against the compliance requirements. Security is often seen as a balance between what is safe, or secure, and what is convenient. If something isn't seen as convenient it can often be perceived as impacting the business in some way. Achieving compliance most certainly is NOT convenient and will impact multiple groups within the organization. As a compliance leader, you must not lose sight of the fact that compliance is not only achieved for compliance's sake, but also to significantly reduce risk to the organization as a whole. Compliance

ultimately provides a solid base for protecting the company assets and reputation. Communication of this important point is important at all levels within the organization.

2. Multi-level, Multi-path Communication

In order to effectively and efficiently reach your compliance goals you must develop relationships across the various business units. These relationships are pivotal to deploying a smooth compliance plan. Meeting with the leaders of the various business units is certainly a great way to develop these relationships. By meeting one-on-one with other leaders you will begin to understand their unique challenges. You will also be able to understand how compliance might impact and even improve their busi-

(Continued on page 3)

Busy at Work, Busy at Home, Bill Witbrod

Inside this issue:

- The Keys to Compliance Leadership 1
- Busy at Work, Busy at Home, Bill Witbrod 1
- FFIEC Responds To Growing Threats 2
- Upcoming Seminars and Roundtables 3
- Upcoming Trainings 4

This past March, Security PS welcomed a new director to their growing team. Bill Witbrod joins us as the Security Compliance Director. Bill has several goals he would like to accomplish while working as a team member; his desires are to develop a compliance practice, build new business and strengthen the company's core offerings. Recently, Bill spearheaded efforts for Security PS to obtain PCI Certification. Bill has already facilitated two roundtables, bringing clients together to address industry issues.

With 14 years of experience, Security PS is thrilled to have Bill on their team. "Bill brings us a wealth of experience in security

A Security PS Team Member Profile



Bill Witbrod, CISM, CISSP

compliance and is extremely passionate about what he does. His knowledge and ex-

perience provide a great fit within the rest of the team," said Steve Rodgers, President and CEO.

One of Bill's prior life experiences includes serving for 8 years for the US Army National Guard Signal Core. He currently is serving as the Vice President of the Kansas City's ISACA chapter and holds a number of technology certifications including: CISA, CISM and CISSP. Bill also has some vendor certifications from Microsoft, Checkpoint and CISCO.

(Continued on page 2)

FFIEC Responds to Growing Threats



Bruce Marshall, CISM, MCSE

“Both the FFIEC guidelines and the current criminal threat require financial institutions to do more than invest in two-factor authentication.”

Retail and commercial banking customers face increasingly sophisticated criminal attacks that seek to steal money or private information used for identity theft. Last year the Federal Financial Institutions Examination Council (FFIEC) responded to these growing threats by updating their security guidance to financial institutions. The FFIEC is a government body responsible for establishing uniform principles and standards with which financial institutions must comply. One area of their oversight is the protection of online banking customers.

The FFIEC guidelines now require financial institutions to conduct a risk assessment of their online authentication controls. A risk assessment identifies the greatest criminal threats to the organization and its customers. The assessment findings are then used to plan corrective security changes in the environment. Financial institutions must complete a risk assessment by the end of the year to comply with FFIEC guidance.

While the FFIEC established the requirement for conducting a risk assessment, they did not provide organizations with the details necessary to complete this work. “Some organizations have narrowly interpreted the guidance from the FFIEC to indicate they must invest in two-factor authentication solutions,” said Bruce K. Marshall, Security PS Director of Network Security.

“However, both the FFIEC guidelines and the current criminal threats require financial institutions to do more. Our risk assessments identify the areas of actual need, which can save our clients money.”

Responding to this need, Security PS created the FFIEC Authentication Risk Assessment consulting service. This service offering aimed at helping banks and other financial institutions identify and eliminate high risk threats to their Internet services. Both current and new clients will benefit by first consulting with Security PS about their plans.

“Our FFIEC Authentication Risk Assessment service helps financial institutions meet these requirements in an efficient and timely manner,” said Steve Rodgers, president of Security PS. “We combine our financial industry experience with our application security expertise to quickly guide organizations through an easy and low cost risk assessment process.” The final result of a FFIEC Authentication Risk Assessment is a summary of the current findings alongside a clear plan to correct the greatest security problems.

Security PS will host an upcoming web seminar for financial institutions interested in learning more about the FFIEC guidance and completing their own risk assessment. Sign up for this free seminar, or learn more about this service, by emailing Security PS at info@securityps.com or call (913) 888-2111.

Busy at Work, Busy at Home, Bill Witbrod Cont.

Bill has been married to his wife of Susan for six years. Together Bill and Susan keep active at home changing diapers and keeping peace with their three sons, all under the age of four years. Some of his hobbies are spending time with his family, hanging out with friends and running. Bill loves to run and the proof is 4 marathons that he has under his belt. He is currently training for the

Chicago Marathon in an effort to qualify for the prestigious 2007 Boston Marathon. Under the age of four years. Some of his hobbies are spending time with his family, hanging out with friends and running. Bill loves to run and the proof is 4 marathons that he has under his belt. He is currently training for the Chicago Marathon in an effort to qualify for the prestigious 2007 Alaska.

The 5 Keys to Compliance Leadership Cont.

ness units.

Have you ever met with the sales and marketing departments to understand how compliance and communication of a strong security posture might actually improve revenue? Over the course of the last several years, security has begun to shift from a burden to a benefit. Customers, partners, and vendors want to work with companies who demonstrate a strong commitment to the protection of personal and confidential information. If you can work with your sales and marketing team to figure out how to communicate this you will positively impact your businesses growth and the bottom line.

3. Understand Risk Levels and Priorities

Speaking of sales and marketing, make sure you understand the risk levels in your organization and how that might be related to where revenue is generated and what confidential information is being protected. Identifying the highest revenue streams will lead you to the most important applications, networks, and systems within the organization. Once these have been identified, match that up with information that needs to be protected and you have a clear picture of what is most important to the organization. If you can create a few scenarios demonstrating what may happen if information is compromised you will capture the attention of the upper-level executives. Now you have a priority list of areas to focus on as well as the attention of the executives.

4. Network with Peers

Compliance leaders should also look outside their organization to take advantage of the experiences of other people managing compliance efforts. Attending professional organization meeting such as ISSA, ISACA, and HTCIA is a great way to network with other peers. Since many of the compliance challenges across indus-

tries are similar, it is important to understand how others have addressed and resolved issues. These networking events also provide a great opportunity to stay on top of the continually changing regulatory environment.

5. Read Leadership Books

A good leader is continually learning throughout their lifetime. Consider reading books on various leadership topics in order to learn more about effectively communicating and leading your organization to compliance. Here are several suggested books to consider:

- [Monday Morning Leadership](#) by David Cottrell
- [The 21 Irrefutable Laws of Leadership](#) by John C. Maxwell
- [The Five Dysfunctions of a Team](#) by Patrick M. Lencioni
- [Execution: The Discipline of Getting Things Done](#) by Larry Bossidy

If you're finding it hard to establish an effective compliance leadership role in your organization consider joining the InfoSec Leadership Roundtable mentioned in the events section of this issue. Also, feel free to give Bill Witbrod a call at (913) 888-2111. He would be happy to share more insight and advice on how you can lead your organization to compliance and make you successful in your role.

Security PS Events

Upcoming Seminars and Roundtables:

InfoSec Leadership Roundtable Roundtable **September 21**

Web Security Seminar 1/2 Day **September 27**

InfoSec Leadership Roundtable

In this new roundtable series we address the challenges of leading and managing your information security team. While we cover topics related to today's every changing landscape of information security, participants will also learn from experts and their peers how to successfully lead teams in an effective and efficient manner.

Web Security Seminar — 1/2 Day

Our experts cover the fundamentals of web security risks with live demos and examples in this half-day seminar that will blow you away. You will learn how insecure and vulnerable web enabled applications and services can be. The presentation and demos are conducted by real-world ethical hackers with extensive experience identifying application security risk.



SECURITY PS

STRATEGIC INFORMATION SECURITY

Prefer a hardcopy of the InfoSec Advisor?

If you would like to receive this newsletter in hardcopy, please email us a quick note along with your mailing address to: info@securityps.com

Visit our Web site at www.securityps.com

Security PS

7300 College Blvd, Suite 175
Overland Park, Kansas 66210
USA

Phone: +1 (913) 888-2111
Toll Free +1 (877) 9 SPS INC
Fax: +1 (913) 888-2120

Coming Next...

In an upcoming issue of *InfoSec Advisor*, the Security PS newsletter, we'll share our insight on Wireless Security and a discussion on how the ISO1779 standard should be used in an assessment.



Security PS Training



Upcoming Training:

In-Depth Web Application Security	October 10
Hands-on WebInspect™ Training & Certification	October 11 & 12
Securing Windows and Active Directory	November 7 & 8
Attacking & Defending Web Applications	November 14 & 15
Information Security Foundations	December 5 & 6

For further information on classes and locations, please visit our Web site: <http://www.securityps.com/training>

Introducing our newest training—Attacking and Defending Web Applications Security PS has been educating application developers, architects, QA personnel, and security professionals about the risks, security principles, and security best practices of application security for years. Now, with an extended two-day hands-on course, Security PS is offering the opportunity to not only learn these concepts from top industry experts, but also to participate in live application hacking exercises and challenges to attain a new level of understanding of this critical security area.

In-Depth Web Applications Security provides the attacks, demonstrations, principles and best practices of web application security by the experts in the industry. Up-to-date and designed to impact the security of your on-line applications for the long term, managers, developers and security staff will benefit from this course.

Hands-on WebInspect™ Training & Certification teaches manual and automated assessment techniques using SPI Dynamics' WebInspect™ product.

Information Security Foundations is a survey course aimed at system administrators and others charged with supporting IT security. The course addresses both hardware and software issues and potential threats both physical and electronic in nature.

Securing Windows & Active Directory. Attendees will discover how hackers can profile, extract information from, and attack computers running Windows. They will learn how to close security gaps using techniques and Windows security features demonstrated during the training.

For more information on all Security PS Training offerings, visit our Web site at www.securityps.com.

Register now!