



### SENIOR LEADER PERSPECTIVE: JODY WESTBY

NSCI's Lindsay Trimble recently interviewed Jody Westby, CEO of Global Cyber Risk LLC. With more than 20 years of technical, legal, policy and business experience, Westby provides consulting and legal services to public and private sector clients around the world in the areas of privacy, security, cybercrime, breach management, forensic investigations and e-discovery. She also serves as Adjunct Distinguished Fellow for Carnegie Mellon CyLab. Earlier in her career, Westby practiced law with two top-tier New York firms and spent 10 years in the computer industry, specializing in database management systems. She speaks globally and is the author of numerous articles and books.



**NSCI: How does the Global Cyber Risk team help leaders understand the technical aspects of cyberspace, so that they can make decisions regarding reliable defense and cybersecurity? What advice do you give to organization leaders to effectively communicate with their IT staff?**

WESTBY: There are two problems: (1) IT staff do not know how to effectively communicate with senior management. They get too technical and do not relate their needs to operational and bottom line issues that executives care about. And, (2) executives and boards think that because the organization has hired IT technical people, they do not need to focus on cyber security or defense issues.

We work with senior executives and boards as well as IT staff to help them understand their roles and responsibilities in protecting digital assets and responding to cybercrime. If they understand that, the cyber security program will start falling into place and defense of data, networks and applications becomes an enterprise issue that is shared. We also help IT staff shape their messages to get funding and attention for priority issues. We primarily rely upon the [governance materials](#) that I developed for Carnegie Mellon University in helping both executives and IT staff understand how to communicate with each other, and my book, "[Roadmap to an Enterprise Security Program](#)." The focus is really upon roles and responsibilities because everyone basically wants to do their job.

**NSCI: In your consulting work, what are the top tips or "best practices" you give regarding risk assessment and prioritization of cyber defense efforts?**

WESTBY: The two most important best practices are up-to-date inventories of applications and data and cross-organizational teams that meet regularly to discuss privacy and security issues and work out enterprise approaches.

An effective inventory is the single most important cornerstone of any security program. It can be developed rather inexpensively and will be the key to managing compliance with privacy laws and security best practices and standards. If done right, it can also be used to facilitate e-discovery. My team



## *Keeping Cyberspace Professionals Informed*

has unparalleled experience in developing inventories, and we have seen the benefits with both public and private sector clients.

Cross-organizational teams need to have senior level representation and meet regularly. There is often some resistance to establishing yet one more group to meet about yet one more topic. An effective approach is for the IT staff to invite the desired personnel for a lunch meeting and present issues that matter to the invitees, such as privacy and security issues that impact their operations, compliance, customer relations, reputation, etc. Then ask at the end of the meeting if people think it would be a good idea to meet again. If the presentation has been effective, the answer is almost always, YES!

***NSCI: Do you think the lack of cyberspace identification and attribution inhibits law enforcement efforts? How do you balance this with privacy concerns?***

WESTBY: The lack of attribution in tracking and tracing cyber criminal activities is not as big a problem as the lack of a harmonized global framework on cybercrime – both substantive provisions and procedural provisions about how to conduct search and seizure, cooperate, etc. There are 233 countries and territories connected to the Internet, but many of these countries do not have cybercrime laws, 24/7 points of contact and trained personnel, including judges and lawyers.

I chair the American Bar Association's Privacy & Computer Crime Committee and we developed the [ITU Toolkit for Cybercrime Legislation](#), with participation from around the world. This document consists of sample language for cybercrime laws – both substantive and procedural – that all countries can use to help move toward a globally-harmonized approach to cybercrime. There are some technical issues associated with attribution, but the issues are overwhelmingly legal and policy issues. Good cybercrime laws contain due process and privacy protections to help balance the needs of law enforcement with civil liberties and individual rights guaranteed under U.S. and international law.

***NSCI: What do you think it will take for prosecutors to effectively communicate the technical complexities of cyberspace to a judge and jury?***

WESTBY: Prosecutors cannot effectively communicate if (1) they do not have the information to present to the judge and jury that comes from effective investigative assistance, proper search and seizure, and documentation regarding chain of custody of the evidence, and (2) trained judges and attorneys in cybercrime legal and evidentiary issues. It is going to take having a harmonized global approach in legal frameworks and cooperation across public and private sector participants in cybercrime investigations.

***NSCI: From an international perspective, there seems to be a proliferation of differing privacy and data protection laws and regulations. This often complicates private industry efforts to develop effective solutions that meet the rules of multiple countries. Any ideas on how this could be improved?***

WESTBY: Yes, there is an extremely complicated framework of privacy laws globally. The United States has one of the most complex legal frameworks, and our state breach laws have added to this. Now, foreign countries are passing breach laws.



## Keeping Cyberspace Professionals Informed

It is almost impossible for multinational companies to manage cross-border data flows and compliance with the various laws. If they don't have a good inventory of data that helps track cross-border data flows, they will be unable to manage their compliance obligations and risks. My company helps large multinationals understand their compliance obligations – privacy, security and breach – and develop policies, procedures and security programs that facilitate compliance. The laws have developed faster than most companies are able to keep pace and companies need to understand that their risk posture has changed significantly. Companies can no longer think they can just join the U.S. Safe Harbor program and not worry about compliance.

How to improve? Again, begin with an effective inventory and do not fall into the trap of thinking that a software tool will do all the work for the organization. These are serious compliance issues with legal, technical, operational and managerial considerations that have to be managed according to an organization's risk plan.

### **NSCI: Is there anything else you'd like to add?**

WESTBY: Beyond the lack of good inventories and cross-organizational teams, the other big gap I see is a lack of attention to planning for cybercrime. Many multinationals do not have any idea what the cybercrime laws are (or if they exist) in the jurisdictions in which they do business; who to contact in the event of an incident; what treaties or protocols exist between the United States and those countries; what providers to interact with; etc. Privacy is viewed as a policy issue, security is viewed as a technical issue and cybercrime is something that is dealt with when it happens. It is really a huge gap in security programs.

MIS TRAINING INSTITUTE'S  
**INFOSEC WORLD 2010**  
 April 17-23 • Orlando • Disney's Coronado Springs Resort  
**► CONFERENCE & EXPO**

Over 70 Practitioner-Led Sessions Covering All Areas of Information Security  
 ► [www.misti.com/infosecworld](http://www.misti.com/infosecworld)

Co-Located Summits  
 The CISO Executive Summit April 18  
 IT Audit Management Summit April 21-23  
 Summit On Secure Virtualization and Cloud Computing April 22

Earn up to 61 CPEs!

PLATINUM SPONSORS: ORACLE, RSA, QUALYS  
 CISO SUMMIT SPONSORS: BT, Aveksa, Q Labs  
 VIRTUALIZATION & CLOUD SUMMIT SPONSOR: TREND MICRO  
 GLOBAL EDUCATION SPONSOR: (ISC)<sup>2</sup>  
 ASSOCIATION SPONSORS: ISSA, WITIE  
 PREMIER MEDIA SPONSOR: SC

110 Royal Aberdeen • Smithfield, VA 23430 • ph. (757) 871-3578