NSCI National Security Cyberspace Institute

CyberPro

June 2010

Keeping Cyberspace Professionals Informed

Senior Leader Perspective: Sandy Bacik

NSCI's Lindsay Trimble recently interviewed Sandy Bacik, principal consultant with EnerNex. Bacik is an author and former CSO who specializes in information security. She has more than 14 years direct development, implementation and management information security experience in the areas of audit management, disaster recovery/business continuity, incident investigation, physical security, privacy, regulatory compliance, standard operating policies/procedures, and data center operations and management. Bacik currently volunteers with NERC, NIST and UCA in assisting in developing interoperability and security standards for the Smart Grid. She is the author of "Building an Effective Security Policy Architecture" and a contributing author to the "Information Security Management Handbook" (2009).

NSCI: Would you give a brief overview of the cyber mission at EnerNex?

BACIK: EnerNex Corporation provides solutions to challenges facing the electric power industry through research, engineering and consulting. The group I'm a part of specializes in security. We provide engineering services, security consulting, software development and customization for energy producers, distributors, consumers and research organizations. Our primary product is information packaged into technical reports, research reports, measurement data, design recommendations or just expert advice.

NSCI: You've written the book "Building an Effective Information Security Policy Architecture." What recommendations do you give information security teams working to secure their organization's network and security architecture?

BACIK: The one thing most security teams forget is to include the business requirements and the business units when developing a network and security architecture. You need to have the business *and* technical requirements before building an architecture or the implementation is going to fail. In order to protect the organization, the organization needs to adopt a defense in depth security architecture for the network. You need to include the business and the technical people, as well as layering that defense.

NSCI: What should companies include in their cyber security policy?

BACIK: The cyber security policy needs to align with the company's mission statement. That mission statement for the enterprise and building it into the cyber security policy needs to fit into the culture of the organization. The cyber security policy needs to state what the company wants to accomplish. For example, "The company will protect all company assets to the level of their importance in the organization." The cyber security policy should also state who's responsible for complying with the asset protection – staff, contractors, partners, consultants, etc. – and who has the authority to enforce.

NSCI: What is your No. 1 tip for companies creating a policy that can keep up with the ever-changing discipline of cyberspace?

BACIK: As you build a policy architecture, your high-level corporate policies need to stand the test of time. They need to be reviewed on an annual basis. Your cyber security enterprise policy needs to be generic without referencing specific technologies, specific positions or staff names. The enterprise should then support that cyber security policy with standards and procedures, which are more of the technical details also reviewed on an annual basis to ensure that those risks and threats are included about how to protect the enterprise assets.

NSCI: How do you recommend organizations balance privacy with accountability when it comes to cyber security?

BACIK: That is a tough one for many enterprises. Most organizations have a corporate statement similar to enterprise assets are for business use only. So employees really should not be doing personal things on the company devices. Again, most enterprises also realize that there's reasonable personal use. The organization needs to have technical controls, such as Internet filtering, monitoring and especially end-user awareness training, to ensure the staff understands how they can use the company assets and what information should be held in confidence versus just blurted out in e-mails or social networking sites.

NSCI: How should employers balance privacy issues and the benefits of social networking sites with the need for security on their networks?

BACIK: Let me kind of step back. When e-mail technology first came out, it was generally viewed like a postcard – do not type anything you don't want everyone to read.

Social networking sites are similar. With social networking sites, there are so many click-through links that take you to other social networking sites and their privacy policies are very different on information sharing. From an organization point of view, the organization needs to have a social networking statement – not necessarily a policy or standard – but a statement to guide the employees. It needs to include regular user awareness training on how staff should be using social networking sites. You know I may be the best and hardest worker a company ever had, but something from my personal life that I posted or someone else has posted might get me terminated. The only way to guide that behavior and to help the employers as well as the employees is user awareness training and making sure the company has taken a stand up front to guide the employees.

NSCI: One of the frequently cited problems with cyber security is the lack of understanding by high-level managers and policy makers as to the extent of the threat. What do you recommend IT professionals do to communicate effectively with their management on the need for security policies and programs?

BACIK: I want to extend that to more than just technology professionals. Technology and security professionals need to remove the term "security" from their vocabulary because there are so many meanings of "security."

If someone comes to me and says "I want you to secure this system."There is physical, logical, and administrative security components. As the security and technology professionals apply that to the business unit, the term "security" freaks them out and scares them. As technology and security professionals, we need to start looking at risk and threat from a business point of view or an organization point of view: "What would happen if we lost X?" Technology and security staff can now start thinking about how this pertains to the business. We can now work with the same concepts. For example, if I say to a business person "What would happen if you lose your laptop that has financial information on it?," a financial person is going to say "Well, I need a back-up." And if a technology person comes in and says "We need to back up all of these laptops," a business person is thinking "I'm not going to be able to use anything." So we need to place it in business terms and risk/threat, so the business person and high-level management understand.

The other misinterpretation is that because you're compliant with the standards and regulations, it also means you're secure. Many high-level managers in the business unit think compliance means security. That's a misconception. Because you're compliant does *not* mean you're secure and because you're secure does *not* mean you're compliant. We need to balance all of those needs.

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

BACIK: As I stated earlier, cyber security teams need to be integrated into the business side, as well as the technology side. Without that balance, you're going to wind up having a gap. Many times, the technology people are going to rush forward and say "You said we needed this technology" and the business side is going to keep saying "Why?"

It's important to make sure that you have the balance of business as well as technology for any security. Even on the Internet, we balance the business with the technical requirements – the compliance, the risk, the threat and the security.