



SENIOR LEADER PERSPECTIVE: BILL PHELPS, ACCENTURE

NSCI recently had the opportunity to interview Bill Phelps, an Executive Director in Accenture's security practice. Bill has spent the past 25 years in technology services. In the past decade, Bill has been a practice leader, company founder, board member and trusted advisor helping organizations with complex management and technology challenges in the areas of information security, data center transformation and technology strategy.



Bill currently leads Accenture's North American Security Practice, where he helps clients address a range of complex Security challenges across industries such as health and public service, financial services, resources, products and communications and high tech. Bill also leads Accenture's global program to help government and private sector organizations address the rapidly increasing cyber security threat. Accenture recognizes the importance of this threat and Bill brings together the full scope of Accenture's global capabilities to help clients respond to it. Key focus areas for Accenture's cyber security initiative include High Performance Security Operations, Information Protection, Mobile Security and Securing the Cloud.

Bill works on Accenture's most complex security engagements. His current client work includes helping a global energy firm transform its overall enterprise security infrastructure, and working with a global financial services institution replatforming its global identity and access management infrastructure. Bill is passionate about the need for organizations to improve their ability to protect sensitive corporate information, and frequently speaks on this topic.

NSCI: Can you tell us a little bit about your role at Accenture and how it relates to improving cyber security?

Phelps: Some of the largest companies and governments in the world hire us to help them understand the cyber security threat, monitor the environment, anticipate potential attacks and remediate situations when incidents occur. We help organizations increase resiliency by embedding security into the fabric of the organization.

My personal role focuses on supporting our clients in our North American business. I work with our clients to help them address complex security challenges, and also spend time with our people, especially on recruiting where we are actively working to grow our team.

NSCI: Vulnerabilities with mobile platforms, including cell phones, seem to be getting a lot of attention these days. What recommendations do you have for improving the security of these devices?



Phelps: Mobility comes with risks that are different from the standard enterprise IT environment. Mobile technologies require a different response from the executives charged with defending their enterprise from cyber attacks and enabling the enterprise to improve operations.

Accenture's experience working with a wide range of companies and public-sector organizations shows that it's worth rethinking security strategy as it applies to mobility. I generally suggest four principles to effectively guide development of a security strategy or initiative for mobile technologies:

- 1. Address four main layers of security: the network, device, application, and back-end system.**
- 2. Build a hard-nosed "culture of security".** Organizations that exhibit a culture of security make responsibilities and accountabilities explicit, by putting in place strong policies and processes. Such organizations tend to view themselves as stewards, not owners, of personal data and take actions to protect data entrusted to them.
- 3. Use carrots, not just sticks, to motivate behavior.** A careful approach to managing employees' expectations and needs will include incentives to promote secure behavior and a willingness to distinguish accidents from malicious intent.
- 4. Know your enemy.** To fully reap the benefits of mobile technologies, companies and government agencies will need to become more aggressive about securing mobile devices and enterprise environments. Focus resources on the areas that are most vulnerable and where the impact of a successful cyber attack will cause the greatest damage.

I have seen a real change in the last 18 months, with more organizations strengthening their policies on mobile device security and increasing the accountability of employees. I think the growth of employee-owned mobile devices is inevitable, and corporate policies need to recognize this.

NSCI: How do you expect threats to evolve in the next few years? What should we be doing now to get ahead of them?

Phelps: I think the threats are only going to get more diverse and sophisticated. I advocate a proactive approach: Anticipate what new threats may challenge the enterprise and mitigate those risks before they can be introduced into an infrastructure or digital asset. Effective cyber-security should be incorporated into processes throughout an enterprise, not just on the perimeter.

Effective cyber-security starts by knowing what data and technology are essential to operations and business continuity. A company or government should develop a detailed plan to protect these assets and capabilities from being compromised, including a robust test of the plan to make sure that it's viable. While organizations typically focus on securing the IT perimeter, it's more effective to secure the data or asset itself, wherever it travels and wherever it lives. Some companies do this internally and some hire companies like Accenture to assist.

Organizations need to pay closer attention to their applications. Many serious breaches result from application-level weaknesses. Most applications were not engineered with security in mind, because developers assumed they would sit behind a secure perimeter. As that assumption is no longer valid,



Keeping Cyberspace Professionals Informed

legacy applications will eventually have to be reengineered, and new applications need to be developed under a new security paradigm.

Identity and access management is another important area for organizations today. Gaining the ability to determine whether customers, citizens, suppliers or employees are who they claim to be when they access enterprise systems and facilities is crucial to enterprise performance. Effective identity and access management programs should create value by embedding pervasive security without sacrificing functionality and ease of use.

NSCI: Many cyber "attacks" are actually criminals seeking to steal intellectual property, and data breaches of one kind or another are in the headlines almost daily. What should individuals and organizations be focused on to prevent losing critical information?

Phelps: I believe the most effective approach to security is the simplest: Concentrate first on stringently protecting what is really important, and then apply measures to the other types of data that are commensurate with their value to the enterprise.

With an information-centric perspective as the foundation, a company can develop and implement the appropriate measures that maximize access to critical information by those who need it while appropriately mitigating the risks to that information throughout its lifecycle. All of this can be done while reducing the overall cost of information protection for the enterprise. I believe there are four key elements to help companies achieve those goals:

- Create an information protection strategy - A company should view its information protection strategy in the broader context of information management. The strategy should include provisions for enabling business opportunities and mitigating critical information risks.
- Locate and classify the information that matters most - While a strategy is absolutely essential to effective protection, it often will fail unless a company knows what it should protect and where that information resides. By locating and classifying the information that matters most, a company can ensure that subsequent efforts are appropriately directed to the information that has the greatest value to the organization—and that could have the greatest negative impact on the company if it were to be compromised.
- Weave information protection into the fabric of the organization - companies should focus considerable attention on ensuring employees understand the importance of protecting information and have the tools to monitor progress over time. As early as possible, a company should assign clear ownership for information and ongoing protection by first defining information protection roles and responsibilities
- Develop capabilities to protect information assets - At the heart of this step in the framework is determining the technologies and processes that optimally support the company's information



Keeping Cyberspace Professionals Informed

protection objectives. In doing so, a company should take a top-down view of how well-suited it is to support those objectives.

NSCI: *Public-Private Partnerships have been mentioned as a key component of improving cyber security. What improvements have you seen in this area over the last few years? What major challenges still exist from your perspective?*

Phelps:

One of the greatest areas for improvement is increased information sharing between government entities and the private sector. Governments often have threat intelligence, but the mechanisms to share it effectively are often not in place. Likewise, the incentives and legal protections to encourage private sector organizations to share information with the government have been lacking as well.

There is also an opportunity and need for more cyber education, and strong technology education more broadly. And the demand for cyber specialists is growing every day.

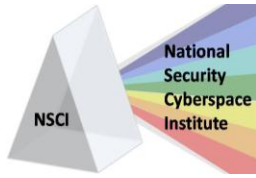
NSCI: *You've sat on a variety of boards and support a range of clients. Can you share a few of the most common mistakes you see regarding the protection of sensitive information?*

Phelps: One of the biggest challenges I see is that security efforts have not always kept pace with the innovations, putting companies at increased risk. One reason companies struggle to respond to threats to their information is a reliance on security standards to set the bar for what is considered sufficient protection. The standards for information security—on which certain industry regulations and security hardware and software products are based—were developed more than 15 years ago and have not been updated appreciably since. Yet during that time, companies have continued to innovate and the environments in which they operate have changed dramatically (think cloud computing, trading partner collaboration and mobility, for instance). Security standards by and large have not necessarily been able to keep up with these important changes.

In addition, companies don't have the appropriate processes in place to distinguish the relative importance of each type of data they generate and store, a determination that is crucial to constructing appropriate security measures.

NSCI: *Regarding cybersecurity, where would you like to see more government involvement? Where would you like to see less?*

Phelps: I would like to see more support for cyber education and improved information sharing.



Keeping Cyberspace Professionals Informed

NSCI: *What are the top 2 or 3 technology challenges you think we need to solve to have a more secure internet?*

Phelps: I actually think this is the wrong question. Very few of the threats I see today are the result of a lack of technology. They result from a lack of adequate resources being applied to cyber security in organizations, and a lack of appropriate and regular measures of effectiveness. Recent Accenture research suggests that only 12% of organizations are 'leaders' as it relates to security.

Where technology is lacking, the problem is often ineffective integration of tools that are already available. One example might be a failure to have an accurate inventory of technology assets so that when a new vulnerability is detected, all affected assets can be quickly and automatically updated.

NSCI: *How do you think we are doing when it comes to international collaboration regarding cybersecurity? How should we move forward?*

Phelps: I think there are more rules in place than is generally recognized but that it's a matter of making sure organizations use them effectively. The recent MegaUpload case was an example of excellent international collaboration.

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

Phelps: For all the valid concern about the magnitude of the cyber threat, I have seen awareness and willingness to act increase tremendously in non-security executives. I am seeing far more CEOs and Boards of Directors actively engaged in understanding the threat to their organization. It is critical that this occur everywhere – cyber security is not a technical or IT challenge, it is something that needs to be addressed across the organization.

NSCI: *Thank you very much for taking the time to visit with us.*

Note: The views expressed in this interview reflect the opinions of the individual and not necessarily the views of Accenture. For more information about Accenture Security, please contact Ana Herrera-Malone at 469-665-6160 or ana.c.herrera-malone@accenture.com.