West Texas Cyber Security Consortium

Cyber Security Depends on Education

by Marisa Viveros | 3:00 PM June 24, 2013

We're facing an eyebrow-raising talent shortfall in cyber security. Consider the findings of a recent inquiry by the UK's National Audit Office. Its report stressed not only that the current pool of security-educated graduates and practitioners falls far short of demand, but also that "it could take up to 20 years to address the skills gap."

This is a challenge my team at IBM is addressing, largely by connecting with the proliferating academic programs on cybersecurity and encouraging higher levels of collaboration among them, industry, and government. (See our recent report here: *Cybersecurity Education for the Next Generation*.) We're particularly concerned to see that the heavy demand from employers for people capable of fighting off today's waves of cyber attacks is pulling talent out of the ranks of professionals who would otherwise be educating the next generation, and doing the critical research to advance the state of the art. Especially given the rapid and continuous evolution of threats, it's critical that academic cybersecurity programs share best practices and curriculum updates.

But it's just as important for enterprises — from startup businesses to large corporations, and from small nonprofits to vast government agencies — to do their part. They have the means as well as the critical need to enhance their employees' cyber security knowledge.

Start with the many IT professionals on their staffs that were never educated in the security aspects of systems. One important way to achieve enhanced security is to design it from the start, in new application development, in how data is managed, and in the construction of IT infrastructure. Employers should invest in IT employees' training, encouraging and supporting the pursuit of related certificates and degrees from graduate schools and other outside programs. The financial investment need not be large. Coursera, Udacity, and other free, online resources offer security-related courses, and there are numerous online Webinars and YouTube videos to which employees can be directed.

Even those employees who did arrive with security knowledge have more to learn. The field of cyber security is constantly expanding, with more domains to secure and more ways to attack. Intrusions are harder to detect; attackers are stealthier and more evasive. Academic programs that did emphasize cryptography and countering sniffing and denial-of-service attacks now cover areas like cyber-physical attacks, the protection of heterogeneous systems, and real-time security data analysis.

Better yet, hiring enterprises can find ways to join forces with academic programs. Among the hundreds of programs we follow, many focus strongly on business. These tend to have industry advisory boards or sponsors. Their best

business partners are deeply engaged, funding research and design competitions, providing fellowships and scholarships, contributing to curriculum design, and sending their own employees to the institution for training and advanced degrees.

Your education mission doesn't end at the door of the IT department. All the rest of your employees also need to know more about protecting themselves and the company. In a recent Ponemon Institute survey, 73 percent of respondents reported that an employee's security misstep had caused financial loss and/or brand damage to their organization. The sad truth is that many employees do not even know when they are engaging in risky behavior that could cause a major security breach. That widespread naivete can take a heavy toll in an era of Bring Your Own Devices (BYOD) and social media. A slipup can happen to anyone, regardless of their position in the organization.

The best defense is to provide comprehensive education programs for employees. You don't have to turn every employee into a cyber security expert to improve your defenses collectively. IBM, for example, requires all employees to complete digital training each year, which covers matters from secure handling of client data to appropriate sharing on social media sites. Employees can easily learn how to spot and avoid the most frequent types of threats, such as phishing attacks in emails.

Whether taught in a university setting or carried out in an enterprise, cyber security is a holistic problem and needs a holistic solution. Just as educational institutions are beginning to develop interdisciplinary approaches (such as joint programs between computer science and business, medical, law, economics, public policy, criminology, and even journalism schools), organizations should ensure that their approach to security reaches the people responsible for infrastructure, human resources, data, applications, ethics assurance, management policy, and legal compliance.

There have been technological advancements within the last few years to help Chief Information Security Officers (CISOs) secure corporate networks against unintentional, or intentional, risky behavior by employees. But while such technical controls, and the establishment of sound policies, are essential components of effective security, educating employees in IT and cyber security is one of the best investments a company can make — and a rational recognition that it will take all of us to create a more secure future.

MARISA VIVEROS

Marisa Viveros is a Vice President at IBM Corporation, leading its Cyber Security Innovation initiative globally. She is responsible for creating education and research programs that foster stronger collaborations among academic institutions, government organizations, and IBM to develop cyber and information security knowledge and talent.

http://blogs.hbr.org/2013/06/cyber-security-depends-on-educ/