



[Print Article](#)

[Close Page](#)

Closing the cyber security skills gaps must start in the classroom

<http://www.itworld.com/security/191397/closing-cyber-security-skills-gaps-must-start-classroom>

August 08, 2011, 1:44 PM

By **David Koretz, CEO, Edward Roberts, Director of Marketing**, Mykonos Software, Inc.



[flickr/cdsessums](#)

If you think about Internet security at all, think about this: you've probably been hacked. According to a recent Ponemon Institute study, 73 percent of companies have been successfully attacked through their Web applications in the last 24 months, and those are just the ones willing to admit it.

How did we get to such a precarious place, and what do we do about it?

Security is an industry, and a profession in flux. Once it was the domain of IT and network-centric professionals, but the threat has rapidly shifted to the application layer, and the need for highly-trained software engineers who understand application security from the code-level has gone through the roof. Unfortunately, web application security classes are virtually non-existent in the nation's leading computing programs.

Traditional security education can be summed up as the "fortress" model. Developers create the application with no focus on the security requirements, while the IT department, who has limited knowledge about how the applications actually works is tasked with building a secure perimeter around them. This model may have been moderately successful in the age of client-server applications, but when most applications are being primarily built for the Web and exposed to millions of potential hackers, the rules change. Our systems are largely wide open at port 80 and directly linked to databases, data warehouses, and other critical storage systems that hold enormous amounts of personal and financial data. It is impossible to just "put a wall up" around these Web applications. Worse, the security is complicated by browser security holes, WiFi insecurity and poor coding standards.

What must change

Developers must be taught not only how to build secure code, but more importantly how to foster a security-focused culture throughout their student population. Graduating IT students must not simply understand how to build network infrastructure, but also understand the applications they protect and how they can be exploited by hackers. The separation between computer science programs and their IT counterparts must disappear as they both focus on application security.

Unfortunately, it will take 20 to 30 years to put the changes in place and see results. Curricula must change, students must spend four or five years studying this in school, and graduates must become influential enough inside their organizations to make security a priority. In the meantime, every student must learn about application security, data security, and cloud security whether formally, or informally. They should attend hacker conferences, join [OWASP](#), and play with the same tools that hackers use.

Dated thinking meets forward thinking

It would be easy to blame an organization such as Sony for a breach by claiming their security protocols were deficient and ridicule them for being the victims of such basic hacker attacks. Perhaps another argument is that the people in charge of protecting Sony from breaches did the very best that they were trained to achieve.

Computing schools and the industry can't afford to sit back and wait for Congress to legislate the problem. They must make application and data security a priority for the next generation of IT professionals. The Rochester Institute of Technology (RIT) is taking steps in the right direction. Through a partnership with [Mykonos Software, Inc.](#), the Institute is revamping its security curriculum to encompass more than just infrastructure security by integrating the innovative, proactive security methods that Mykonos uses in its technologies into coursework. RIT students will train on Mykonos' latest Web Application Firewall with Web

Intrusion prevention and use the in-depth data to better understand hacking methods and techniques.

This kind of partnership should be a model for public and private collaboration. Not only will it improve security, but it will also give students the best and most comprehensive skill set needed to compete in the workforce.

About the authors

David Koretz – CEO Mykonos Software

Mr. Koretz is a serial entrepreneur who founded six companies by the age of 30. He is currently CEO of BlueTie and President and CEO of Mykonos Software. Under the leadership of Mr. Koretz, BlueTie has been a three-time recipient of Forbes Magazine "Best of the Web," the Ad-Tech Award for Best B2B Transaction Website, and winner of the AlwaysOn/KPMG Top 100 private companies.

Edward Roberts – Director of Marketing, Mykonos Software

Mr. Roberts is responsible for marketing communications, promotions, lead generation and sales enablement. He has 20 years of experience marketing products to enterprise clients for companies, including WorkforceLogic, InsideTrack, Nelson Family of Companies, Randstad, Harris Interactive and Adecco. He has a BA from Middlesex University, London.

<http://www.itworld.com/security/191397/closing-cyber-security-skills-gaps-must-start-classroom>

© 1994-2011 ITworld. All rights reserved.