Diversity™ in Action
MAY/JUNE 2015
ADVANCING STEM PROFESSIONALS AND STUDENTS

Cybersecurity Needs Skilled Pros

A variety of backgrounds can lead to this exciting career

BY ARTHUR SCHURR

James Clapper, U.S. director of national intelligence, has declared cybercrime a greater threat to national security than terrorism, espionage or weapons of mass destruction.

When Clapper testified before the U.S. Senate Intelligence Committee in January 2014, he said, "Many aspects of life have migrated to the Internet and digital networks. These include essential government functions, industry and commerce, health care, social communication and personal information. Foreign threats pose growing risks to these functions as the public continues to increase its use of and trust in digital infrastructures and technologies."

Stephen Ward is East Coast region vice president for Pinkerton, headquartered in Ann Arbor and a subsidiary of security firm Securitas. He agrees with Clapper's assessment but is concerned about the response of U.S. organizations. "Although more American organizations are becoming aware of the importance of cybersecurity, there is still a level of immaturity," he says. " Not every organization feels that they could be a target, and many still need to address the issue of securing their networks."

Vincent Sritapan, cyber security division program manager for the U.S. Department of Homeland Security's Science and Technology Directorate, says, "Technology advancements are outpacing security. The top threats include point-of-sale and web application attacks. We have a lot of intellectual property and growth in those areas, but we have a hard time keeping them secure. Insider and privileged-user misuse and cyber espionage are also big problems.

"The DHS mission is to protect critical systems and infrastructure," Sritapan says. "Technology is vulnerable in areas like the power grid and financial systems, but we're busy creating innovative cybersecurity technology to protect them and move forward."

These concerns have made cybersecurity professionals very hot commodities. The stakes could not be higher, so attracting the best and the brightest talent to cybersecurity is paramount. Fortunately, many gifted, diverse professionals—DHS's Sritapan among them—have answered the call. Sritapan took a direct route, but the others' paths have had more twists and turns.

Mobile Security for DHS

Sritapan oversees mobile security research and development for DHS's cyber security division. The division is part of the Homeland Security Advanced Research Projects Agency under the DHS Science and Technology Directorate. "I engage industry, government and academia around cybersecurity research for mobile security," he explains. "As they push mobile products out, I want to make sure that if we make the effort to create protections for a product, it's worthy of the time and investment."

> "Although more American organizations are becoming aware of the importance of cybersecurity, there is still a level of immaturity."
>
> —STEPHAN WARD, PINKERTON EAST COAST VICE PRESIDENT

Sritapan began his cyber education with a bachelor's in information systems from California State University Northridge in 2007. He went on to earn a master's in national security studies in 2009 and an MBA in information assurance and security management from California State University-San Bernardino in 2011, with support from the National Science Foundation's Cyber Corps Scholarship for Service program. He's now studying at the Naval War College as a U.S. Navy Reserve officer and information professional. He also teaches courses in cyber at Northern Virginia Community College's cyber center.

Sritapan joined the DHS information security architecture and engineering division in 2011. He enjoys the research support at DHS. "In many places, cybersecurity and mobile security can be constrained by budget, time and resources," he says. "But here the sky is the limit and the reach is everywhere."

His minority background has not influenced his career, he says, but his youth has sometimes been a factor. "When I first started in cyber, I worked with people that had work experience

that started before I was born," Sritapan says. "So to overcome that I had to diversify my knowledge set and portfolio."

Sadik Al-Abdulla of CDW

Sadik Al-Abdulla is director of the security solutions practice for technology solutions provider CDW. He manages current business and strategic planning for information risk management, network security and compliance. "Our customers face constantly evolving threats and requirements," he says. "So I ensure that we have the right relationships and offerings to anticipate and meet the needs of our customers and grow our share of the market."

Al-Abdulla began his cyber career at the University of Wisconsin-Madison and the University of Minnesota-Twins Cities. He has top-level technical certifications from Microsoft, Cisco and a dozen other major technology players in the security industry. In 2000, he joined Berbee Information Networks, at the time one of the largest independent IT solution providers in the U.S. CDW acquired Berbee in 2006.

Cybersecurity has always been his passion. "IT is constantly changing, but in cybersecurity everything moves even faster and I love that," Al-Abdulla says. "The threats that we're talking about today are not the threats we were talking about six months ago. That's an enormous catalyst for growth. It's impossible to be bored when everything is fresh and challenging! And because everything moves so quickly, critical thinking and analysis are fundamental skills in this industry."

He notes that the IT industry has not always been a diverse, level playing field. "The industry is making great strides in diversity, but historically, it has struggled, especially at the executive level," Al-Abdulla says. "In 2012, CDW invested in a six-month, one-on-one executive coaching program for me, and I am very grateful for that. The program was a fantastic opportunity. It really helped me develop my leadership skills and grow in my career."

Toyia Rudd directs CDW's diversity and inclusion practices. "CDW makes it a top priority to recruit, retain and develop professionals of color," she says. "I meet regularly with CDW executive committee members to discuss hiring and mobility actions and strategies for diverse coworkers across the company. We're really proud of our efforts to invest in Sadik and other coworkers with strong potential."

L-3's Darrell Lieteau

L-3 cybersecurity solutions architect Darrell Lieteau researches and analyzes computer networks and enterprise infrastructure for cyber vulnerabilities, and develops solutions. His work covers ethical hacking, computer incident handling, solution development, proposal writing and research.

> "Technology is vulnerable in areas like the power grid and financial systems, but we're busy creating innovative cybersecurity technology to protect them and move forward."
>
> —STEPHAN WARD, PINKERTON EAST COAST VICE PRESIDENT

Lieteau got his bachelor's in sociology from Excelsior College in Albany, New York, in 1995. In 2010, he followed that with a master's in administration and information resource management at Central Michigan University. He added an MBA from the University of Maryland, University College in 2014 and has many technical certifications.

He joined L-3, an aerospace systems and national security solutions contractor, in 2012. Before that, he worked at several technical companies, including a previous stint with L-3 and a five-year hitch in the U.S. Navy.

Lieteau believes that takes a certain personality and perspective to succeed in cybersecurity. "It's essential to know how an adversary thinks and how he or she would exploit vulnerable systems," he says. "Understanding the 'hacker' mentality is critical to success in cybersecurity. Adversaries, as well as allies, come from diverse backgrounds. I believe it is important to analyze cyber operations, particularly cybersecurity, from multiple perspectives. Diverse security professionals can provide unique knowledge and experience to organizations that increases overall threat awareness levels."

Lieteau also believes that his status as a minority has been an asset in his field. "It has allowed me to bring a different perspective on security issues, as well as business opportunities for my company," he says. "Being a minority has also helped broaden my view of the people involved in cybersecurity, and I'm seeing increased diversity in the field."

SSA's Agatha Onyewuchi

Agatha Onyewuchi is chief of the security assurance branch of the Office of Information Security in the U.S. Social Security Administration. "I manage an integral part of the agency's information security program by providing the technical framework and security requirements for managing cybersecurity-related risks," she explains. That entails building security capabilities, maintaining agency-wide IT security resilience and providing essential information to senior leaders about risk.

Onyewuchi didn't start her career in cybersecurity. She graduated from the University of Lagos, Nigeria, in 1983 with a degree in English, and worked in finance until she came to the U.S. in 1990. She was hired by OAO Corporation, now part of Lockheed Martin Technology Services, where she was introduced to cybersecurity work.

In 2007, she earned a master's in information assurance from Norwich University in Vermont and became a certified information systems security professional, or CISSP. She received a chief information officer certificate from the Chief Information Officer Institute at Carnegie Mellon University in March 2015.

She worked as a consultant supporting the SSA for two years, then joined full-time in 2009. She credits her education and preparation for her success and love of the field. "This is a dynamic and challenging environment where there are always new threats, risks and solutions. Industry certifications like CISSP are important, but the graduate programs gave me the skills I needed," she says. "The curriculum explores technical theories and methods behind information assurance and also teaches management strategies and leadership. The programs provide both training and practical experience."

Onyewuchi praises the SSA for its efforts in creating an equitable workplace. "The agency promotes workforce diversity, and supports efforts to recruit and retain a diverse workforce," she says. "SSA has given me training and career development opportunities specifically in cybersecurity."

Bill Zielinski, SSA deputy commissioner

for systems and CIO, believes professionals like Onyewuchi exemplify SSA's commitment to utilizing the best talent for its mission. "The Social Security Administration fosters diversity and inclusion awareness for all employees to stimulate effective communication, retain a flexible and agile workforce, and to provide for increased productivity," he says. "We encourage individual talents, experiences and ideas that help us serve our customers."

Jamie Porter, Symantec

Lead incident response investigator Jamie Porter helps technology giant Symantec keep its corporate customers safe. She provides on-site incident response in the form of an arsenal of specialized tools and skills that most companies simply don't have in-house. "One of the biggest challenges we face is when clients try to work the incident themselves before calling for help," she says. "That often results in additional damage and leads to critical pieces of evidence being lost. It is important the security incident is fully understood before any action is taken, and the response must be very measured and precise."

Like many in IT, Porter learned her craft on the job. She has numerous professional security IT certifications, including a CISSP, but no college degree. She finds that certifications, plus her on-the-job training, make her at least as effective as any degreed professional.

Early in her career, Porter designed and supported large corporate networks for several Fortune 50 and 500 companies, gaining a solid IT security foundation. Before Symantec, she worked at IBM for more that 14 years, ending as global security operations manager. A former IBM colleague who had gone to work for Symantec inspired the move to her current position.

Porter believes that calm and composure are the two most important character traits for IT security incident responders; and she has a unique perspective on gender in the field. "In email conversations, it's often assumed that I'm male because of the spelling of my name, Jamie. So, it's always interesting to hear the surprise of the first phone call when someone realizes that I am female," she says. "On occasion I'll notice a distinct and subtle shift in the communication quality after that point. The tone of the conversation becomes subtly patronizing and less direct."

But Porter commends Symantec for its equitable culture. She points to Symantec's Women Action Network, an employee resource group that focuses on career development and networking opportunities for women, as an example f the firm's commitment to fairness.

Porter indulges her yen for excitement by building and racing cars on the LeMons endurance racing circuit. She and her team recently rebuilt a 1982 Mercedes sedan into "five cylinders of turbo-charged diesel fury."

Cynthia Austin of the USAF

Cynthia Austin is the enterprise vulnerability assessments chief for the U.S. Air Force 33rd Network Warfare Squadron. She leads a team tasked with producing and analyzing monthly and on-demand vulnerability reports on Air Force systems and providing cyber-protection solutions. "We also ensure that current network software products are compatible with current systems and standards. And we generate time-compliance network orders to system administrators in the field to remedy new vulnerabilities," she explains.

Austin, a civilian, started her training with a bachelor's in technical management from DeVry University, which she finished in 2011. Before joining the 33rd NWS, Austin resolved IT integration and configuration issues for the 50th Space Communications Squadron at Schriever Air Force Base in Colorado. She was happy to join the 33rd NWS: "I was fortunate enough to find an open position within the 33rd as a government employee, so I could relocate with my active duty spouse."

Austin takes great pride in her work. "The highlight of this job is the satisfaction of safeguarding our nation's defense information," she says. "There is a thrill in protecting systems and data across the USAF against its many cyber attackers."

In her experience, the Air Force and the cyber field itself are egalitarian. "In the cyber career field, we all have one common goal, to protect our network against the adversary," she says. "For me, being in the minority has yet to play any part in the workplace." ■