Training Tomorrow's Cyber Soldiers

Eller and Engineering team up to launch online master's in cybersecurity.

Berkeley, California, 1986: It was just a small thing – a 75-cent error in a University of California laboratory's computer user records. Still, UA alum Clifford Stoll (PhD Astronomy '80) was asked to investigate. What Stoll found was no minor accounting error. A hacker had penetrated the Lawrence Berkeley National Laboratory's network as a pathway into military and industrial networks around the world.

It took 10 months of cyber-sleuthing – largely on his own time – but Stoll followed the digital tracks to Hanover, West Germany, where the criminals were ultimately arrested. What had motivated them? Money. The Soviet KGB had paid them $54,000

for stolen secrets – paltry even in today's dollars: $119,280, adjusting for inflation.

Stoll wasn't trained in digital sleuthing. He was an astronomer turned systems admin who'd earned his PhD from the UA's Lunar and Planetary Laboratory. But purely by accident, he had become what may be the UA's first cybersecurity expert alumnus.

"A cyber-secure America requires a full pipeline of emerging talent ready to support our nation's most complex challenges."

– Cheryl Whitis, Raytheon Missile Systems Vice President of Information Technology

Fast-forward to 2017, when hacker-caused headaches are much bigger than they were in the mid-1980s. It's fair to say that the world's civilian and military networks are now under constant attack. The consequences can be devastating, and they aren't just monetary. They can be life threatening.

Case in point: June's Petya ransomware attack that targeted computer systems throughout Europe and the United States. Public works in Ukraine – including those focused on the Chernobyl nuclear power site – were especially hard hit. The hazard-site plant didn't experience leaks as a result, but staff were forced to measure dangerous radiation levels manually. The month before, ransomware attacks in nearly 100 countries locked patient records at numerous hospitals.

For thousands of organizations around the world, the threat of digital catastrophe has never been so clear, and as a result, the demand for computer crime fighters is so strong that job openings are predicted to triple over the next five years. As they do, the University of Arizona will be there to answer the call.

Together, the Eller College of Management and College of Engineering recently launched a fully online Master of Science in Cybersecurity degree. The 33-credit program combines expertise from Eller's MIS department with that from Engineering's departments of electrical and computer engineering and systems and industrial engineering, and is the first of a series of programs that Eller will launch to prepare professionals for the world's fastest-growing technical business fields.

"Cyber-crime costs are expected to jump to $3 trillion by 2021," Eller Dean Paulo Goes said. "Companies are scrambling to find qualified candidates who can excel at providing cyber defenses. Those graduating from the UA's new master's program will learn not just theory, but also hands-on approaches to the critical components of cybersecurity, including business intelligence, data mining, information security, risk management, systems security management, penetration testing, network security, system cybersecurity engineering and cyber warfare."

Unlike other national programs, the UA MS in Cybersecurity is designed for working professionals, offering flexible scheduling, with six admission dates throughout the year. It offers two tracks – Information Systems, focused on software, data and people, and Physical Systems, emphasizing security of computers, email, medical devices and the Internet of Things – and already has earned the stamp of approval from industry leaders.

"A cyber-secure America requires a full pipeline of emerging talent ready to support our nation's most complex challenges," said Cheryl Whitis, Raytheon Missile Systems vice president of information technology and member of the UA's MIS Advisory Council. "Our company, along with its business and technology partners, will need successive generations of cybersecurity talent to help us secure customer environments as well as address new business opportunities." – *Martha Retallick*

Program Core and Tracks

Common Core
12 UNITS

Courses include Information Security in Public and Private Sectors, Data Mining, Computer Networks and Systems Cyber Security Engineering

Information Systems Track
21 UNITS

Courses include Information Security Risk Management, Cyber Threat Intelligence and Cyber Warfare Capstone

Physical Systems Track
21 UNITS

Courses include Systems Engineering Process, Digital Communication and Cyber Security: Concept, Theory and Practice

Learn more about the new MS in Cybersecurity at cybersecurity.arizona.edu.

SHUTTERSTOCK PHOTO