SPONSORED REPORT



MIAMI DADE COLLEGE COMBATS CRITICAL SHORTAGE IN CYBERSECURITY

Who hasn't received that dreaded warning notification in their inbox telling them to change their password? It's a far-too-common message as security breaches and hacks increasingly threaten the safety of users' personal information. Hackers are breaking into servers and databases all over the world every minute of every day, and there aren't nearly enough professionals with advanced training to combat them.

It's estimated that the global cybersecurity workforce will have more than 1.5 million unfilled positions by 2020, according to the Center for Cyber Safety and Education.

To address this critical shortage, Miami Dade College has launched specialized cybersecurity programs, boot camps and courses that, in tandem with MDC's state-of-the-art training facility, the **Cybersecurity Center of the Americas,** provide students with unprecedented hands-on experience.

GUIDANCE FROM EXPERTS

In addition to providing the latest technology for training, including an ever-evolving Cyber Range, or virtual training platform created by worldwide security leader CyberBit, the center has a board of advisors made up of experts in the field.

"With the expertise of chief information security officers, security analysts and national advisors, we are able to incorporate the knowledge, skills and abilities that industry needs into our programs and training options," said Antonio Delgado, dean of MDC's School of Engineering, Technology and Design. "Having a direct line to industry leaders also creates a pathway for our students to work for their companies as interns and mentees before they even graduate, and the organizations benefit by having access to our resources such as the Cyber Range."

LEARNING OPTIONS FOR EVERYONE

From beginners looking to learn about cybersecurity to seasoned professionals with years of experience in the field, MDC offers a range of courses and programs.

Students who want to learn the ins and outs of cybersecurity can opt for a College Credit Certificate or Associate in Science in Cybersecurity, both launching in fall of 2019. They can further their education by following the cybersecurity concentration in MDC's Bachelor of Science in Information Systems Technology.

Others who want to get a foot in the door to the industry may choose a more condensed course option, such as one of the certification boot camps offered at the center. These camps prepare students to take specific certification exams from leading cybersecurity organizations including EC-Council, CompTIA, Cisco, CheckPoint, Splunk and more.

"The center's Ethical Hacker certification boot camp has been especially sought after," Delgado said.

Anyone studying cybersecurity at MDC has access to the **Cybersecurity Center of the Americas** and its Cyber Range. Even those who aren't MDC students can take a course. Companies also can book blocks of time at the Cyber Range so their security teams can practice handling cyberthreats. ▸

For more information, visit mdc.edu/cybersecurity or email cybersecuritycenter@mdc.edu

AN ADVANCED TRAINING CENTER

Preparing for security jobs in the real world requires a realistic setting. That's why the **Cybersecurity Center of the Americas,** at Miami Dade College is not just another classroom. It was built in 2018 to look and function like a security operations center (SOC) so that students and professionals can get the hands-on experience they need in this quickly evolving industry.

"Cybersecurity is very fast," said Jorge Ortega, the center's director. "Things happen in a digital world where speed is measured in nanoseconds, so you don't have the luxury of time to research. You need professionals who know how to act in the moment – and with speed."

What makes the center stand out as a training facility is its exclusive Cyber Range, a virtual training ground for cybersecurity professionals. Outfitted with one of the most advanced training platforms available, the Cyber Range, created by leading Israeli security company CyberBit, provides a virtual environment with professional tools and several hyper-realistic cyberattack scenarios that mimics the training used by military and intelligence agencies.

STUDYING CYBERATTACKS

You wouldn't want to infect your computer with a virus and risk disabling your network. So how do you train for that and other attacks? Virtually, of course. Providing authentic, industry-grade tools including real firewalls, Security Information and Event Management (SIEMs), Intrusion Detection and Prevention Systems (IDS/IPS), packet analyzers and network monitoring systems within a network of about 50 computers in the cloud (virtual systems without physical servers), the Cyber Range can simulate cyberattacks in a safe environment for active training.

"Here we can unleash a cyberattack, let it create havoc and see how students or security teams deal with the attack," Ortega said. "That way if it happens on the job, they've already been through it."

The scenarios at Cyber Range emulate full-scale cyberattacks, from reconnaissance activities that take place prior to the launch of an attack to the very end of an incident. These attacks are not compartmentalized exercises, meaning they do not stop nor pause for trainees, but continue to exploit and wreak greater havoc as each minute passes. Once the clock starts, trainees are taken through a three step-process to resolve the issue.

First is **detection**, when trainees first have to find where the security breach originated. This is an essential skill for security professionals – especially at companies where thousands of computers are potential entry points of attack.

Next is **response**. Once the origin of a cyberattack is located, the team must figure out how to neutralize it and minimize the damage.

Finally, the team enters the **prevention** phase. After a threat has been handled, the team reviews how the attack could have been prevented and steps that can be taken to make sure it never happens again.

GLOBAL ACCESS

As a virtual environment and testing ground, the Cyber Range is accessible from anywhere, meaning instructors on all MDC campuses can use it. Companies all over the world also can book time to train their employees at their own sites.

The scenarios typically run four hours. The range offers 15 different options on which to train, including attacks aimed at disrupting business operations, exfiltrating confidential information and/or causing financial damage.

No matter what level of technical skill an individual has, MDC has an option to help them study cybersecurity with the knowledge, tools and technology they need to succeed in this exciting industry.

For more information, visit mdc.edu/cybersecurity or email cybersecuritycenter@mdc.edu

THE MANY TYPES OF CYBERATTACKS

The Cybersecurity Center of the Americas has training options in several key areas of cyberattacks, including:

Denial of service: With this attack, hackers prevent customers from accessing services online, often by using internet bots to flood a server with enough traffic to overload the bandwidth and cripple the server.

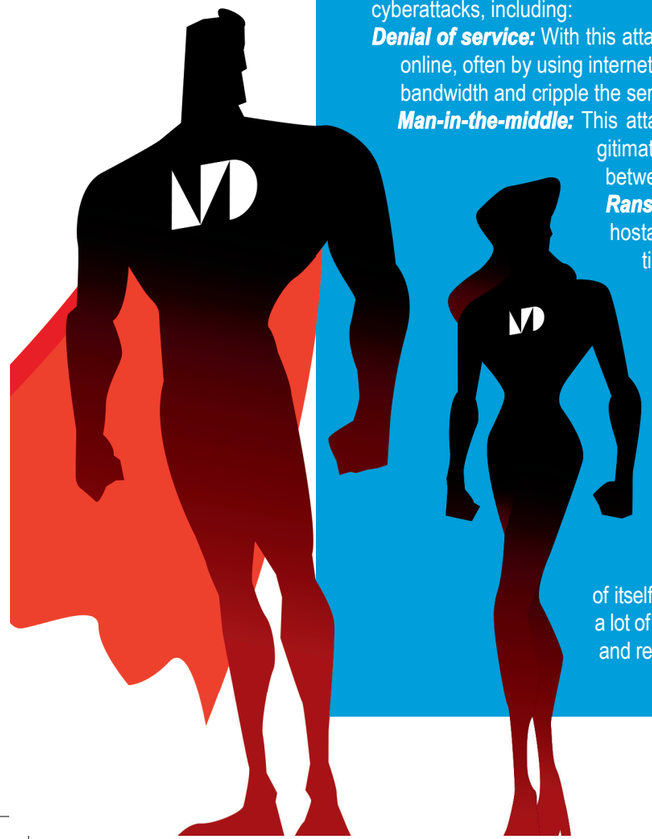
Man-in-the-middle: This attack involves deceiving the host by impersonating a legitimate proxy, allowing a hacker to intercept communication between two parties.

Ransomware: During an attack where information is held hostage, hackers using ransomware will encrypt an organization's sensitive files and threaten to delete them within a certain amount of time if not paid a ransom.

Trojan attack: Done a variety of ways, Trojan attacks involve gaining access to sensitive information by sneaking into a system undetected, such as by phishing to gain credentials or loading malicious material onto a networked computer via a USB.

Web defacement: Often used to damage an organization's reputation, this attack involves infiltrating a company's internet-facing web server and defacing its site to display a hacker's message.

Worm outbreak: A type of program that spreads copies of itself to other devices connected to a network, a worm can do a lot of damage to an internal network requiring malware analysis and reverse engineering to mitigate the threat.



SPONSORED REPORT

CYBERSECURITY BY THE NUMBERS

1.5 million cybersecurity positions will be unfilled by 2020 globally.

MDC is one of a handful of educational institutions in the country to have a **Cyber Range by Cyberbit**, a leader in cybersecurity whose platforms are used by military and intelligence agencies.

2018 is when Miami Dade College launched the Cybersecurity Center of the Americas.

$300 billion+ projected growth of global cybersecurity market by 2024, from current value of more than $120 billion

15+ different cyberattack scenarios are available for drills at the center's Cyber Range, a virtual training platform.

28% projected job growth for information security analysts by 2026*

82% of employers report a shortage of cybersecurity skills.**

13% projected job growth within cybersecurity by 2026*

*Bureau of Labor Statistics
**Center for Strategic & International Studies