INSIDE BUSINESS
FOCUS ON CYBERSECURITY

NO COST, BIG REWARD
Free steps to enhance the security of your network: **Page 15**

September 18, 2017 · www.LVB.com

Next week: Office Environments & Work Spaces

Colleges step up to train next gen of cybersecurity pros

By BRENDA LANGE
Special for Lehigh Valley Business

Information security analysts are in demand nationwide, and it is the fastest growing technology job in the country.

PHOTO/JIRSAK

Cybercrime is on the rise and new cyberattacks are reported seemingly every week.

Most recently, Equifax reported that 143 million Americans' personal data had been compromised when cybercriminals hacked its systems.

This growing criminal element has opened the door to new career opportunities for men and women who want to work in the information technology field, and recently some institutions of higher education have begun responding to the growing skill gap by offering degrees, certifications and programming in cybersecurity.

DeSales University is one such local school and offers a master's of science degree in information systems with a concentration in cybersecurity.

The program is directed by Patricia Riola, assistant professor of computer science, who became interested in the field of electronic crime and its prevention about 12 years ago while teaching at Lehigh Carbon Community College, yet could find no definitive texts on the subject. Since then, demand for professionals in cybersecurity has skyrocketed.

FILLING A SKILLS GAP

Riola cited reports showing that job growth in the field is three times greater than in other IT positions, an area already in high demand.

"Demand for [cybersecurity] positions in the finance sector has seen a 137 percent growth over the past five years. In health care, it's 121 percent, and retail has an 89 percent growth," she said. "Information security analysts are in demand nationwide, and it is the fastest growing technology job in the country, with starting salaries nearing six figures."

She attributed the demand to the rising crime rate, the proliferation of mobile devices and the world's growing interconnectedness.

VITAL CAREER TRACK

What Riola calls cyberterrorism is a big concern for its potential to totally disrupt human lives.

Water and electric systems, machinery, mass transportation – all can be affected by someone out to render the populace helpless.

"This is why cybersecurity education programs are so important," she said. "It's not if it happens – we [cybersecurity experts] plan for it, evaluate the risk, determine the potential threats, put a

please see **CYBERSECURITY**, page **12**

FOCUS ON CYBERSECURITY

Wyomissing firm battles cybercrime for three decades

By JENNIFER TROXELL WOODWARD
Special for Lehigh Valley Business

Long before it was being called cybersecurity, David Kramer was protecting people and businesses against hackers.

"I have been doing cybersecurity before it was even considered cool to do cybersecurity," said Kramer, owner and president of Domain Technology Group Inc. in Wyomissing. "… It was just called computer security, and the hackers were guys that were considered computer wizards.

"Now, these are well-funded organizations, organized crime doing the computer infection. The players are trained and often groups from countries like Russia, China and Syria."

Kramer, who started his cybersecurity and information technology-managed services business in 1989, dedicates some of his time to training others on cybersecurity.

He said he does various public speaking engagements throughout the year and has written articles on the topic. One of his upcoming seminars will be in conjunction with members of the FBI, who will discuss tactics used by cybercriminals.

"In cybersecurity, the rewards are high and the risks are low," Kramer said. "The FBI will tell you that there are just too many hackers to go after all of them."

SMALL-TIMERS AVOID PROSECUTION

Government officials will go after the big money scammers before investigating the small-time hackers.

Kramer said international cybercriminals have a better chance to escape before U.S. authorities can go after them while domestic hackers "end up with a slap on the wrist" and don't get chased down as much because of the volume of hacker activity.

What – are they using to attack us
RaaS (Ransomware as a service)
Encrypting files and asking for a ransom
DoS/DDoS
Unprotected computers "owned" by bad guys
IOT devices and other unsecured routers/modems
Phishing
Spoofing
Zero-Day exploits
XSS (Cross site scripting)
Etc…

CONTRIBUTED PHOTO

Larry Goncea of Domain Technology makes a presentation at a seminar in Philadelphia.

DOMAIN TECHNOLOGY GROUP INC.

- **What:** Information technology-managed services providing cybersecurity.
- **Locations:** Berkshire Boulevard, Wyomissing, with a satellite office in Philadelphia.
- **No. of employees:** 5.
- **Website:** www.domain-group.com.

"A high school dropout can go online and purchase a hacking kit for $75. It is just too easy," Kramer said.

WORK IN WASHINGTON

Domain Technology is a spinoff of Integrity Data, which was a network infrastructure business that Kramer formed with a business partner in Exeter Township, he said.

"That company was started in 1988, and I bought out my business partner and became Domain Technology," Kramer said.

Kramer said his firm works with clients throughout eastern Pennsylvania as well as out-of-state.

"We are right now working with a company that provides software for the House of Representatives. So we are doing some work in Washington, D.C.," he said.

BOGUS EMAILS

Kramer said cybersecurity makes up at least half of his business, which also offers IT support and network services for mostly small and mid-sized businesses. He said that his team uses tools for network system audits and can do advanced assessments.

The tools or software detect when outsiders are trying to infiltrate the network. For example, it is common to find a perpetrator trying a large number of user names and passwords to get into a system.

A recent scam that Domain Technology was hired to probe involves a fake email being sent to a chief financial officer, purportedly from the company's CEO, requesting that money be transferred to a specific account. In this scenario, the transfer must be stopped in a timely manner before the money goes into that clandestine account.

"We are getting better at protection, finding encrypted files," Kramer said. "… We have been doing this for decades," Kramer said.

BE CAREFUL WITH LOG-ON INFO

Larry Goncea, a cybersecurity consultant at Domain Technology, said he has been with the business for 19 years.

Today, "most attacks have large financial motivation or are sponsored by national groups," Goncea said. "People are going for the low-hanging fruit and finding it easier to trick someone into revealing his or her password and user name."

He said in the past, a hacker would sit at the computer and make countless attempts to invade someone's computer, but everything today is automated. The bad guys have a system that is set to automatically run through passwords and user names to log into a network.

"We are improving our safety measures, but we are not at point where [as a whole] we can secure the entire environment," he said. "There is always a new way for people to find to attack you."

'A high school dropout can go online and purchase a hacking kit for $75. It is just too easy.'

— **David Kramer, Domain Technology Group**

BUSINESSES MUST DO SOMETHING

According to Kramer, cyberthieves who use ransomware to garble your computer screen and take data hostage want a ransom, and that money can be paid by phoning a call center that the hacker set up in order to take payments.

He said he will fight to enhance cybersecurity and continue to train others.

It is too risky to do nothing to protect yourself against savvy, aggressive cybercriminals, Kramer said, adding that businesses realize it is expensive and damaging to their reputation when they are hacked.

"In the industry, we look at the user as the first line of defense," Goncea said.

CYBERSECURITY

continued from page 11

continuity plan in place. … All along the way, we take preventative measures to protect systems as much as we are able to."

HIGHLY PAID

DeSales' program prepares students to work as security analysts, security auditors, even chief security officers, among other job titles; all tend to be high-paying positions.

Mike Brown is one such student. He graduated from DeSales' Master of Science and Information Systems program in May with a concentration in cybersecurity and works as a senior cybersecurity engineer with SageNet in Media.

The Bethlehem native earned his bachelor's degree from Temple University in business and IT education and chose DeSales to advance his career while working for Philadelphia Gas Works as an information security analyst.

SIMULATE ATTACKS

Brown's role with SageNet allows him to work with businesses to find weaknesses in their computer networks before they are found by attackers.

"I simulate an attack and then report this to the company, so they can make the necessary fixes," he said.

"This is a growing field and that's not going to change. What I do involves a variety of technologies such as database design, coding and a wide variety of different computer languages, all of which I learned at DeSales."

GROWING DEMAND

As recently as 30 years ago, such security (and the need for it) was nonexistent. Only in the past 10 or 15 years have companies begun to pay attention to the need for personnel to guard their information.

Scott Gingold, owner of Lehigh Valley Technology Company in Bethlehem, confirmed the importance of such safeguards and the need for trained personnel to implement them.

As companies scale back on IT departments or don't even have them, his company has grown, providing IT services and solutions to businesses, government agencies and nonprofits.

"The demand for experienced and qualified workforce to protect networks and information systems will continue to grow as technology grows," he said.

AFFINITY FOR SERVICE

East Stroudsburg University offers a bachelor's degree in computer security that combines the foundations of computer security, network security and computer science and was developed in conjunction with the National Security Agency and Department of Homeland Security in 2002.

As with the DeSales program, students at East Stroudsburg receive a solid grounding in computer science and programming fundamentals so they fully understand the nature of the systems they will protect on the job.

Students with an aptitude for technology, math and the sciences do particularly well in the program, according to Michael Jochen, associate professor of computer science at East Stroudsburg.

"Our students tend to like working with technology and often have an affinity for service. Many of our graduates seek employment with the federal government," he said. "We also have a good number of students who take their skills into the private sector or start their own businesses.

CONNECTIONS AND VULNERABILITY

Jochen agrees with Riola that the ubiquity of computers and networking has allowed for the relative ease with which cybercriminals have been able to attack systems around the world.

"Controls for our critical infrastructure, energy and water, national security, aviation and traffic lights are often all connected to the internet, which we rely on every day to accomplish the critical tasks required by our jobs and personal lives," he said.

"This reliance on an interconnected world exposes us to many threats and creates a need for the people with the skills to protect those devices."