STEVENSON UNIVERSITY

CUS FORENSIC FOCUS FOREN

Collected By: School of Graduate and Professional Studies

Issue: Fall 2015

IN THIS ISSUE

Contact Information

Thomas Coogan
Associate Dean, Forensics & Director, Center for Forensic Excellence
443-352-4075
tcoogan@stevenson.edu

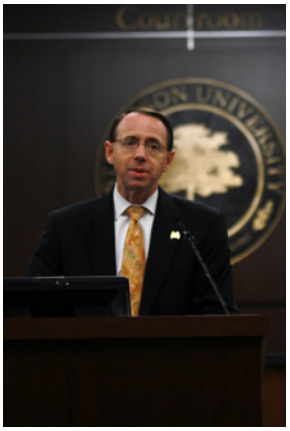
Angela Reynolds
Director, School of Graduate and Professional Studies Recruiting & Admissions
443-352-4414
amreynolds@stevenson.edu

STEVENSON UNIVERSITY
Imagine your future. Design your career.®
School of Graduate and Professional Studies

Maryland Leaders Raise Concerns about Computer Forensic Shortages

According to RAND Institute's 2014 research report *Hackers Wanted*, the perception that there is a shortage of cybersecurity professionals within the United States could leave the country vulnerable to cyber-attacks. While initiatives have been set in motion to combat the shortage, the labor market continues to lag and is predicted to slowly catch up to the demand.

To address forensic challenges, Stevenson University established a Center for Forensic Excellence. The Center's inaugural meeting held in May 2015, gathered many local, state, and federal law enforcement leaders from Maryland to help identify opportunities and challenges facing forensic professionals in the state. Several of the meeting's attendees echoed the concerns stated in the RAND report and have first-hand experience with the shortage of cyber and computer forensics personnel, facilities, and services.



Honorable Rod Rosenstein, United States Attorney delivering the keynote address at the Center for Forensic Excellence May 15 meeting.

Among the attendees was Stevenson's Cyber Forensics Program Coordinator and Professor Michael Robinson. Robinson has experience performing computer and cell phone exploitation and analysis for agencies in the U.S. Intelligence Community. He has also worked for the FBI's Investigative Analysis Unit and various corporations as a computer forensic examiner.

As a practitioner in the field, Robinson describes the extent of the issue by noting, "Investigations conducted by law enforcement agencies as well as commercial and private organizations are directly impacted by the shortage of computer forensic services."

Robinson believes the shortage has developed for the following reasons:

- An overall lack of qualified personnel to perform investigations in the industry. As organizations start to appreciate the need for this service, a greater demand is created.
- Competition for qualified personnel between law enforcement and private organizations. The pool of candidates is now divided up among an increasing number of employers.
- The amount of storage on personal computers, servers, and mobile devices, as well as the amount of data being communicated, has grown to an incredibly high volume. Therefore, the workload for an individual case has grown exponentially and it takes longer for a qualified professional to complete a single examination.

Per Robinson, insufficient resources in computer forensic services cause many issues. He explains, "The backlog is growing and it takes weeks or months to complete a case. As of May 2015, the directors of the Maryland area crime labs indicated they have cases with backlogs of approximately 18 months. These backlogs in turn may cause an examiner to omit certain analytical techniques in order to expedite and rush a case rather than give an extensive treatment of data." Robinson also discloses, "Some forensic examinations may not even be conducted in the first place due to time and cost."

Stevenson's Forensic Studies Professor Emmet Davitt also attended the Center's meeting and shared his expert opinion on the matter. Prior to his arrival as Maryland's State

> We need to provide more personnel with training. If hiring departments can employ more qualified people, the backlog can be addressed.

Prosecutor, Davitt's office had its own on-site computer forensics lab. Eventually, Davitt was forced to close the lab due to the expense of maintaining the facility, as well as the cost of training and re-training qualified personnel. Davitt states, "The equipment is very expensive to obtain and equally expensive to maintain and keep updated. For small prosecution offices and police departments, it simply isn't feasible to maintain one's own facility. The practical effect," Davitt adds, "is that the office is required to ask state and federal agencies to analyze evidence." Davitt's office focused on white collar crime, which unfortunately meant his work often took a back seat to high priority cases where lives were at stake. This amounted to months, sometimes even years of delays before his office would receive computer forensics assistance.

When posed with offering a possible solution to the shortage, Davitt states, "It is easy to say, 'create more facilities.' But we are all aware of the costs involved in both creating and maintaining the equipment and keeping qualified personnel." He concludes, "Certainly, the concept of additional shared facilities among law enforcement agencies, prosecution offices, and universities is worth considering."

Robinson offers his opinion on the insufficient resources and says, "We need to provide more personnel with training. If hiring departments can employ more qualified people, the backlog can be addressed. Training should be constantly evolving to introduce new digital forensic techniques. Additionally, we need to decrease the need for human labor with an increase in effective ways to triage a case using an automated computer process."

For more details about the Center for Forensic Excellence's findings and solutions for the shortage of computer forensics services, contact Stevenson University for a copy of the July 2015 Progress Report at gps-inquiry@stevenson.edu or call us at 1-877-531-7118.

Rand Corporation, (2014). *Hackers Wanted An Examination of the Cybersecurity Labor Market*. Retrieved from http://www.rand.org/pubs/research_reports/RR430.html

A Guide to Advancement in the Digital Forensics Field

Digital forensic professionals seeking to advance their careers are aware that both a master's degree and certifications are often required to remain competitive in the field. In recent years, the volume of advanced degrees and certifications in the market have reached an all-time high, making it challenging for professionals to decide which path to choose. The following advice can help a professional make an informed decision to build their credentials as a digital forensics professional.

There are a number of important factors in considering the ideal academic institution. In relation to forensics, the top two factors include the program of study and the school's accreditation status and reputation. Students can pursue programs that are research-based or focused primarily on digital forensics, and should avoid computer science or security focused programs that only offer forensic courses as electives. The ideal program for a student looking to advance their career has both a heavy emphasis on learning digital forensic techniques as well as a substantial amount of practical application. Students can check reliable sources that evaluate the relative strengths and weaknesses of academic institutions, such as college reviews or the U.S. News and World Report.

To demonstrate proficiency in the digital forensics field, professionals are advised to couple their advanced degrees with certifications. In the decision making process, a professional should consider the following questions:

Which certifications are applicable to the recipient's field of practice? For example: Digital forensics?

Digital forensics has various specialties and there are certifications geared towards each such as: computer forensics, malware analysis, penetration testing, mobile device forensics, and network security.

What is the initial cost of the certification in terms of training and examination fees?

Some training courses and examination fees can cost approximately $3,000 to $7,000 (without travel expenses).

How long is the certification valid?

Many vendors and associations impose expiration dates on their exams after three years.

Will the certification demonstrate mastery of a specific product or will it demonstrate broader knowledge?

Typically, vendor-based training and certifications focus on using particular tools. This may be important if a particular tool is used within a specific employment position. The value of the certification may change if the recipient switches employment to an organization where different tools are used.

Will the certification make the recipient more marketable in the field and to employers?

Some agencies, consulting firms, and private organizations require specific certifications. For example, the DoD requires individuals in key computer security positions to maintain one of the certifications specified in DoD Directive 8570.

There are a variety of certifications available in the digital forensics field to consider. Below is a sampling of the more popular certifications:

Vendor specific certifications that are designed to demonstrate proficiency with a tool:

- AccessData Certified Examiner (ACE)
- Cellebrite Certified Mobile Examiner (CCME)
- Guidance Software's EnCase Certified Examiner (EnCE)
- MSAB's XRY Certification

Non-vendor specific trainings that demonstrate proficiency with forensic concepts but are not tied to a specific tool:

- International Association of Computer Investigative Specialists (IACIS)
- Certified Forensic Computer Examiner (CFCE)
- International Information System Security Certification Consortium, Inc., (ISC)²®
- Certified Cyber Forensic Professional (CCFP)
- International Society of Forensic Computer Examiner's (ISFCE)
- Certified Computer Examiner (CCE)

Specialty focused examinations that target a specific discipline:

- The EC-Council's Computer Hacking Forensic Investigator (CHFI)
- The EC-Council's Certified Ethical Hacker (CEH), which is popular with network penetration testers
- Global Information Assurance Certification (GIAC) Reverse Engineering Malware, which is popular with malware analysts

Avoid computer science or security focused programs that only offer forensic courses as electives.

Due to the volume of certifications available, it is advisable for professionals to consider what certifications will be most beneficial to their career advancement prior to spending their time and money. Current trends and industry standards for certifications are often found within an organization's employment opportunities. Additionally, asking other computer forensic professionals about their experiences in the field can prove useful. Stevenson University is fortunate to have numerous computer forensic professionals as faculty and students who are available as valuable resources to prospective students and other professionals. For advice on where to start your search for an advanced education or career, contact Stevenson University at gps-inquiry@stevenson.edu or call us at 1-877-531-7118.

CYBER SECURITY AWARENESS MONTH

Between 2012 and 2013, the cost of cyber crime increased **$2.6 BILLION**

The FBI's Internet Crime Complaint Center receives 300,000 complaints a year, totaling over **$800M** in losses

92% of human resources professionals said increased vulnerability of business technology will affect the U.S. workplace in the next 5 years

44% of small businesses reported being the victim of a cyber attack

608 MILLION total number of records with sensitive information lost in data breaches since 2005

$9000 is the average cost of a cyber attack

Homeland Security. (2015). Stop.Think.Connect. Toolkit. Retrieved from http://www.dhs.gov/stopthinkconnect-toolkit

Cuckoo's Egg: The Case that Put Digital Forensics on the Map

Imagine if a routine work assignment propelled you into a world of espionage. That is exactly what happened to Clifford Stoll. Stoll was working as a systems manager at the Lawrence Berkeley National Laboratory and was asked to investigate a seventy-five cent accounting discrepancy in the laboratory's computer usage account. Little did Stoll know this simple task would lead to a lengthy investigation and test his merit as a computer forensics professional.

Stoll recounts his investigation in the book, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage,* and explains how it all started with tracking an unauthorized user who used nine seconds of computer time without paying for it. After Stoll realized the unauthorized user was a hacker, he spent the next 10 months attempting to trace the origin of the hacker.

As one of the earliest documented cases of computer hacking, there were no processes or procedures in place within federal agencies to investigate this new phenomenon. Stoll was met with great resistance throughout the investigation from the FBI and CIA due to their reluctance to share information between the agencies. Additionally, there was even confusion about who had jurisdiction over the case.

Despite all of the roadblocks Stoll encountered, he was eventually able to determine the hacker's location. Through his own investigation, Stoll realized the hacker was using a telephone modem connection. He tracked the intrusion to a defense contractor's call center and began recording all of the hacker's activities. Per the activity logs, it appeared the hacker was active in the middle of the day, however Stoll hypothesized the hacker was in a time zone east of California because most hackers are active at night.

Stoll's expert knowledge of sophisticated computer systems and sheer persistence lead to the identification and capture of the hacker, Markus Hess. Stoll discovered Hess had been successfully hacking U.S. systems for several years and selling the results to the Soviet KGB.

Recognized as one of the first examples of digital forensics, Stoll's investigation occurred almost 30 years ago and illustrates the determination and creativity needed to be a successful cyber forensics expert. To join the ranks of Clifford Stoll and other cyber-crime fighters, learn more about earning your master's in Cyber Forensics with Stevenson University at stevenson.edu/gps.

Faculty Profile

Professor Michael K. Robinson

Hometown: Winston-Salem, North Carolina

Profession: Stevenson University's Program Coordinator of Cyber Forensics, Cyber Threat Intelligence Analyst, Digital Forensic Examiner, and Security Researcher aka "Breaker of Things"

Hobbies: You mean work isn't a hobby? Okay, quadcopters and drones, hacking phones, and breaking things.

Last Book Read: Marc Goodman's Future Crimes: Everything is Connected, Everyone is Vulnerable, and What We Can Do About It

Last Accomplishment: Giving a fun presentation at DEF CON in Las Vegas

Quote: "It's time to unlevel the playing field."

Profile: In addition to teaching at Stevenson University, I am currently a Cyber Threat Intelligence Analyst and Senior Digital Forensic Examiner for a large, international company. Prior to Stevenson, I was a Senior Digital Forensic Examiner with the FBI's Investigative Analysis Unit, where I performed digital forensic examinations in support of counter terrorism, counter intelligence, and criminal cases. Before working for the FBI, I was the CIO for a U.S. Department of Defense agency, where I oversaw all Information Technology and Information Assurance operations for the Agency, including all incident response and forensic investigations.

I have also worked for other agencies in the U.S. Intelligence Community performing a variety of digital forensic examinations on both computers and mobile devices, supporting classified and unclassified projects. In addition to working with the government, I have performed forensic examinations for commercial organizations and served as the technical editor for forensic books. I have delivered numerous presentations at national and international conferences such as DEF CON, InfoSec World, the DoD and U.S. Cyber Crime Conferences, CEIC, HTCIA International Conference, and BCISS Conference on Intelligence Analysis.

Courses taught: Mobile Device Forensics; IDS, Firewalls, and Auditing; Mock Intrusion; Co-teacher in the Forensic Studies Mock Trial capstone course.

STEVENSON
UNIVERSITY
Imagine your future. Design your career.®
School of Graduate and Professional Studies

100 Campus Circle
Owings Mills, MD, 21117

443-352-4399
1-877-531-7118

stevenson.edu/gps

Center for Forensic Excellence

STEVENSON UNIVERSITY

Maryland Forensic Educators Meeting

Friday, November 13, 2015
Brown School of Business and Leadership
Owings Mills campus

Stevenson University's Center for Forensic Excellence is inviting educators from area institutions to discuss and address the challenges and opportunities in forensic education in Maryland. The meeting will be hosted on Friday, November 13 at Stevenson's Owings Mills campus.

Visit **stevenson.edu/cfex** for more information. Contact us at **gps-inquiry@stevenson.edu** or call 1-887-531-7118.