Peterson, G.L., Raines, R.A., and Baldwin, R.O., "Digital Forensics Educational Needs in the Miami Valley Region," *Journal of Applied Security Research*, vol. 3, no. 3-4, pp. 429-439, 2008. DOI: 10.1080/19361610801981662.

Digital Forensics Educational Needs in the Miami Valley Region

Gilbert L. Peterson, Richard A. Raines, Rusty O. Baldwin
Air Force Institute of Technology
Department of Electrical and Computer Engineering
2950 Hobson Way
Wright-Patterson AFB, OH 45433-7765
{gilbert.peterson,richard.raines,rusty.baldwin}@afit.edu

Abstract: We have surveyed information technology employees in the corporate environment of the Miami Valley to gauge the interest in transitioning a graduate level digital forensics course to a community college setting. Specifically, we were interested whether a digital forensics security course at the community college level would fill a need in corporate security processes. The survey results indicate that companies and IT employees in the region have a need for and are interested in an accessible digital forensics course. Additionally, the results identify specific needs a digital forensics course can fill. Meeting these needs will then become the primary focus of the course.

Keywords: digital forensics education, corporate computer security, community college education

INTRODUCTION

In March of 2007, TJ Maxx was the victim of what has been labeled the largest security breach ever with the loss of 45.7 million credit card numbers [Brodkin, 2007]. After suffering a breach like this, the first concern is to determine what was taken, how it was taken, and what can be done to prevent it in the future. A specialist in digital forensics can help answer these questions, and corporations are realizing these skills will be important for their future security [Discini, 2005].

Because of this need, the Air Force Institute of Technology (AFIT) is interested in transitioning our graduate level expertise in computer security to local schools. We are transitioning our digital forensics course to Sinclair Community College. One of the requirements for this transition is to be able to show that Sinclair will have enough community interest and long term attendance for the course.

The Department of Electrical and Computer Engineering at the Air Force Institute of Technology (AFIT) has offered a hands-on course in Digital Forensics since 2003. This course has been extremely popular with the students averaging 20 students in each class which for a graduating student body of 70 students is quite high. Being taught at the United States Air Force's graduate school, the course is directed to the needs of the Air Force officers taking the course, and contains content which directly pertains to the policies of the Air Force.

Sinclair Community College is our local university partner for transitioning our digital forensics course. Sinclair Community College is a public two-year college with its main campus located in Dayton, Ohio. Sinclair is one of only 20 member colleges of the prestigious League for Innovation in the Community College and a Vanguard Learning College. Serving more than 50,000 students annually, Sinclair's university parallel courses are designed to transfer to 4-year baccalaureate programs. Sinclair students earn Associate of Arts, Associate of Science, Associate of Applied Science, and Associate of Technical Studies degrees.

In addition, Sinclair offers coursework that supports many information technology and security certifications, as well as some information technology certifications. To continue building on Sinclair's strong position among community colleges and current information technology coursework, Sinclair wishes to offer a course in Digital Forensics. This benefits AFIT since it provides technology transfer and education and training for a student population AFIT currently can not reach. This population is the same individuals that are eventually hired by the Air Force to manage its networks.

In the next section, we present some related work on surveys in the area of digital forensics. This is followed by a brief description of the survey and the detailed survey results. The paper closes with an overview of the conclusions which we draw from the results.

RELATED WORK

Conducting surveys to determine needs for education coursework have been conducted many times [Lund, 1999, Bogolea and Wijekumar, 2004, and Katz, 2005]. However, as far as we are aware, this is the first time that a survey of this nature has been used to determine the need for education in the digital forensics domain. There have been other digital forensics surveys conducted, namely those of CIS/FBI which occur yearly [Gordon, et al., 2007], and that of the National White Collar Crime Center and Federal Bureau of Investigation, also a yearly publication [NWC2 and FBI, 2007]. We have made use of several of the demographics questions from this to gauge the size of the corporate and corporate IT community. The results of the demographical information help gauge the potential class sizes, and the size of the community of interest for the course.

There have been other surveys conducted on the topic of digital forensics. The oldest of these was conducted by the US Secret Service to assess law enforcement and government agency readiness for digital forensics. They found that almost half of the agencies had a digital forensics department and that many law enforcement organizations were making use of these resources [Norblett, 1995].

Two of the more recent surveys perform a needs analysis, which targets existing digital forensics practitioners in corporate, education [Rogers and Seigfried, 2004], and law enforcement [Stambaugh, et al., 2001]. These individuals were asked questions on current and potential upcoming issues in digital forensics. The findings indicate that a primary concern, from both surveys, is standardization of training and certification requirements. Beyond this, the needs of the law enforcement community tended toward ensuring a greater awareness of computer forensics at all levels, judge, prosecutors, and general public [Stambaugh, et al., 2001]. The needs identified by the practitioners, and educators, tend toward more reliability and formalism in testing [Rogers and Seigfried, 2004].

SURVEY DESCRIPTION AND FINDINGS

This section is an overview of our survey and a discussion of the respondents of the survey. This is followed with a discussion of the survey results. The full survey can be found in Appendix A.

Respondent Description

The survey consists of 18 questions, 6 of which request corporate and individual background information. Including demographic questions on the size of the company, size of the information technology department and on whether anyone at the company has any digital forensics certifications or would be interested in any. The remaining 12 questions ask about the preparedness of the company and past experiences with attack and data loss. The purpose of these questions is to determine the needs of the regional corporate security community for digital forensics, so that the materials of our course can be tailored to best meet these needs.

The survey was executed using the Zoomerang online survey tools (http://info.zoomerang.com). The address to the survey with an introduction and instructions was e-mailed to approximately 75 individuals. The individuals were identified based on their membership in the Dayton Information Systems Security Association (ISSA), the local Direct Marketing Association which includes sub groups for Information Technologists, and Corporate Information Officers. We were specifically targeting information technology specialists and the managers in charge of information technology in the Miami Valley Region of Ohio. The Miami Valley Region is centered in the city of Dayton, Ohio and includes the surrounding cities and suburbs.

From the survey population, we received 14 full responses and 3 partial responses, a 22.6% response rate. The respondents companies ranged in size from 2 with 1-9 employees and 9 companies with 500 or more employees. The detailed responses to the most significant questions are presented in the following section.

Survey Findings

The survey results underscore the need for a course on digital forensics and incident response in the Miami Valley Region. From the 17 company responses that we received, with an Information Technology employee base of more than 75, only seven individuals had any type of digital forensics security certification. The two certifications were the EnCase Certified Examiner and IACIS Computer Forensics External Certification. In addition, 50% of the respondents indicated that they would be very interested in having their IT employees participate in a digital forensics course.

The respondents indicated that 70% have had between 1 and 4 security incidents within the last year, with the remaining indicating that they have had no incidents. For those that have had an incident, they indicated that as a company, that their primary concerns after a security breach are to determine how the breach occurred, what information was lost, and whether any information can be recovered. This information is duplicated in the question on corporate response, with almost half of the respondents indicating that their company responds with a broad brush using multiple approaches. Some of these responses include identifying the perpetrator, installing additional security hardware, installing security software, and updates, and tightened corporate security policies.

With better information and processes that a digital forensics course provides to determine how and

what information was lost, the companies could focus and perform better cost analysis before instigating new security measures.

Of concern is that 50% of the respondents have no policy in place for a computer incident. It is critical that IT employees be aware of what to do and who to notify in case of a security breach so that evidence is not lost, damaged, or rendered inadmissible for court. However, although 50% of companies do not have a policy in place to deal with a security breach, they have an 86% belief that their employees are prepared for an incident. Comparing this result with that of the respondents' believing that their employees are aware of the legal implications when handling a computer incident, which is 30%, again indicates a role for a digital forensics course target at these individuals. The IT person responding to an incident must be aware of how their actions could affect future legal proceedings.

In terms of education requirements for their employees and new hires, there is some variation between the requirements that are used for new employees and those for existing employees interested in continuing education. For new employees, existing training, certification from coursework, certification from examination, and experience are all rated as being important with degrees only being moderately important. For employee continuing education however, they are most interested in training and certification examinations where training includes individual courses. This underscores the importance of individual courses with few prerequisites. Existing employee continuing education is further restricted by the fact that companies are least likely to support continuing education for degreed programs and feel that mentorship is only moderately useful.

Respondents did not see any benefit in sending individuals for a digital forensics course over that of incident response, network administration, system administration, secure software development, or specific hardware training. In fact, the ratings for all of these potential courses had similar results, all were perceived as equally important. From this, we can only assume that companies are looking for balanced individuals rather than topic specialists. Because of this balancing, a single course in incident response is probably going to be much more useful to the companies and the individuals than a set of courses or a degree.

CONCLUSION

Our survey results from the Miami Valley region indicate that there is a strong interest in developing a course at the community college level in digital forensics and incidence response. In addition to the respondents indicating this, having employees with this type of education is in important due to the information the companies desire after a computer incident, specifically that of who and what information was compromised, how the compromise occurred, and can the information be retrieved.

In developing the digital forensics course for Sinclair, the determination of how, when, and what will take precedence in the course material of interest. It is also noted that the information technology personnel must also be made aware of the legal ramifications their actions can have in terms of criminal law and of more importance to most companies, employee and corporate law. To ensure that any action that they take does not invalidate the admissibility of the evidence collected.

ACKNOWLEDGEMENTS

This material is based upon work supported by the National Science Foundation under Grant No. 0516134 and we add to our disclaimer that any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

BIBLIOGRAPHY

Bogolea, Bradley, and Wijekumar, K., Information Security Curriculum Creation: A Case Study, Proceedings of the 1st Annual Conference on Information Security Curriculum Development InfoSecCD '04, pp. 59-65.

Brodkin, Jon, TJX breach may spur greater adoption of credit card security standards, March 2007. Available at: http://www.networkworld.com/news/2007/032907-tjx-breach-adopt-standards.html

Discini, Sonny, Digital Forensics Readiness: Are You In?, 2005. Available at: http://www.enterpriseitplanet.com/security/features/article.php/3572206

Gordon, Lawrence A., Loeb, Martin P., Lucyshyn, William, and Richardson, R., 2006 CSI/FBI Computer Crime and Security Survey, 2006, Available at: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf

Katz, Frank H., Pedagogy: the effect of a university information security survey on instruction methods in information security, Proceedings of the 2nd Annual Conference on Information Security Curriculum Development InfoSecCD '05, pp. 43-48.

Lund, H.H., "Robot Soccer in Education", Survey for Advanced Robotics Journal, Special Issue on RoboCup, 1999.

National White Collar Crime Center and Federal Bureau of Investigation, Internet Crime Report: January 1, 2006 – December 31, 2006, 2007, Available at: http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf

Noblett, M. G. Report of the Federal Bureau of Investigation on development of forensic tools and examinations for data recovery from computer evidence. In: Proceedings of the 11th INTERPOL Forensic Science Symposium, Lyon, France. The Forensic Sciences Foundation Press, Boulder, Colorado, 1995.

Rogers, Marcus K., and Seigfried, Kate, The future of computer forensics: a needs analysis survey, Computers & Security, Vol. 23(1), 2004, pp 12-16.

Stambaugh, H., Beaupre, D., Icove, D., Cassaday, W., & Williams, W. (2001). State and local law enforcement needs to combat electronic crime. National Institute of Justice Research in Brief.

Appendix A:Sinclair Incident Response and Digital Forensics Course Survey

The survey is part of a study to be conducted on corporate digital forensics education and training needs in the Miami Valley. The following questions examine your company's current experience and interest in digital forensic education. The questions also examine corporate preparedness in the field of digital forensics. Information from the survey will be used to develop coursework at Sinclair Community College and AFIT that best respond to the needs of the corporate community

Demographics

1) What size is your organization's Information Technology department?
    a. 1-3 employees

b. 4-7 employees
c. 7-10 employees
d. 11+ employees
e. IT Outsourced

2) How many employees does your organization have?
    a. 1-9
    b. 10-49
    c. 50-99
    d. 100-499
    e. 500+
3) What is your job title?
    a. Chief Information Officer
    b. Chief Executive Officer
    c. Company Security Officer
    d. Chief Information Security Officer
    e. Security Officer/Director
    f. Systems Administrator
    g. Other Please List:

Digital Forensics Education/Certification

4) How many IT employees hold a digital forensics or incident response security certification?
    a. 0
    b. 1
    c. 2
    d. 3
    e. 4+
5) Which digital forensics security specific certifications are held?
    a. GIAC Certified Forensics Analyst
    b. SANS System Forensics, Investigation and Response
    c. EnCase Certified Examiner
    d. IACIS Computer Forensics External Certification
    e. Certified International Information Systems Forensics Investigator
    f. LC Tech Forensic Certifications
    g. Other List:
    h. None
6) On a scale from 1-5, rate your interest in having your IT employees participate in a digital forensics course.
    a. Scale 1 2 3 4 5

Digital Forensics Response Questions

7) How many computer security incidents occurred in your organization with the last 12 months?
    a. None
    b. 1-4
    c. 5-9
    d. 10+.
8) After a computer security incident occurred, which actions did your organization take? ([circle] all that apply)

a. Did not report the incident to anyone outside the organization
b. Reported incident to law enforcement agency
c. Consulted with a lawyer for legal prosecution
d. Engaged an outside security investigator
e. Attempted to identify the perpetrator of the computer security incident
f. Installed additional computer security hardware
g. Installed additional computer security software
h. Installed security updates on the network
i. Tightened corporate security policies
j. No action was taken
k. Other List:

9) Is there an organizational policy in place when responding to a computer security incident?
   a. Yes/No
10) On a scale of 1-5, rate your IT employees' preparedness in the event of computer incident occurrence
   a. Scale 1 2 3 4 5
11) On a scale of 1-5, rate your IT employees' awareness of the procedures to follow when handling a response to a computer incident occurrence.
   a. Scale 1-5
12) On a scale of 1-5 rate the following in their importance when handling a computer incident.
   a. Maintaining chain of evidence for prosecution Scale 1-5
   b. Return systems to operating state Scale 1-5
   c. Determining information lost Scale 1-5
   d. Determining how the information was lost Scale 1-5
   e. Installing preventive theft measures Scale 1-5
   f. Data recovery from loss Scale 1-5
13) How long do you keep logs for the following network operations
   a. OS system logsDo not keep/5-29 days/1-3 months /3+ months
   b. Network access logs Do not keep/5-29 days/1-3 months /3+ months
   c. Proxy server logs Do not keep/5-29 days/1-3 months /3+ months
   d. IDS logs Do not keep/5-29 days/1-3 months /3+ months
   e. Internal IDS logs Do not keep/5-29 days/1-3 months /3+ months
   f. File access logs (m,a,c times with filename) Do not keep/5-29 days/1-3 months /3+ months
14) What forensic technologies does your organization employ (Check all that apply)
   a. Packet sniffer
   b. Media analysis
   c. Media imaging
   d. Server-based log analysis
   e. Other List:
15) Which other security technologies does your organization employ (Check all that apply)
   a. Policies restricting data devices (USB, iPods, etc)
   b. WWW restrictions
   c. Employee monitoring
   d. Mobile phones restrictions
   e. Access control policies
   f. Intrusion Detection Systems
   g. Firewalls and antivirus

h. Encryption for data in transit
i. Intrusion prevention system
j. Public key infrastructure
k. Encrypted files
l. Other List

16) On a scale from 1-5 rate the following categories based on their importance in the hiring process, when considering hiring new employees for your information technology department
    a. Degree Program Completion Scale 1-5
    b. Training Scale 1-5
    c. Certification from coursework Scale 1-5
    d. Certification via examination Scale 1-5
    e. Experience Scale 1-5
17) Rank the following in importance according to your corporate mission when sending or supporting employees in further education.
    a. Degreed Programs
    b. Training
    c. Certification
    d. Certification Examinations
    e. Mentorship
18) On a scale from 1-5 rate the potential benefit that you feel your company would gain by sending employees for education/training/certification in the following areas:
    a. Digital forensics Scale 1-5
    b. Incident response Scale 1-5
    c. Network administration Scale 1-5
    d. Systems administration Scale 1-5
    e. Secure software development Scale 1-5
    f. Specific hardware training Scale 1-5