CYBER CERTIFICATIONS

FUTURE-PROOFING FOR THE *Ediscovery Professional*

by Janice Jaco

When we work with clients or industry groups on topics related to the maturation of ediscovery practice and professionals, invariably the "what's next?" part of the conversation flows into data privacy and security. Baseline competence in these areas is now table stakes, and well-rounded ediscovery pros are adding rigorous privacy and cybersecurity certifications to validate the bona fides of their teams.

JANICE JACO
Janice Jaco, ACEDS 2015 eDiscovery Person of the Year, is a senior eDiscovery Project Manager for boutique litigation powerhouse Keesal, Young & Logan. Janice's professional volunteer work includes extensive involvement in authoring LTC4's eDiscovery Core Competency, participation in ACEDS' CEDS Exam Standard Setting Exercise, and updating ACEDS' University online content. Janice is currently a member of ILTA's Litigation & Practice Support Content Team and recently completed the BARBRI Cybint courses in Cyber Protection and Intelligence.

Cyber-related job openings on LinkedIn outnumber ediscovery job openings 20 to 1, and there is virtually zero percent unemployment in cybersecurity. This unprecedented career opportunity tells a powerful story: there is compelling evidence that for ediscovery professionals interested in the future arc of their careers, retraining to expand skill sets in these areas is becoming compulsory.

Certifications As Client and Stakeholder Confidence Builders

Our firm represents clients in highly regulated industries, many of whom have been conducting regular on-premises security audits for the past eight years. These clients were focused on security even before they zeroed in on ediscovery practices and are more concerned today than ever before. Law departments expect their law firms to have excellent security hygiene and expect that same excellence from all downstream vendors who touch their data. Legal professionals must pursue cyber education and certifications as evidence of a minimum skill set in security or privacy.

In response to client expectations, our firm encourages the pursuit of the Certified Ediscovery Specialist certification (CEDS) created by the Association of Certified Ediscovery Specialists (ACEDS) for litigation support professionals who handle ediscovery. More recently we have encouraged training and certifications related to security, Cyber Security Protection (CSPC) and Cyber Intelligence (CIC) training and certifications offered by Cybint Solutions, a BARBRI Professional Association; the Certified Ethical Hacker (CEH) offered by the EC-Council; and the Certified Information Systems Security Professional (CISSP) created by (ISC)2. These certifications add credibility to RFP responses where assurances are given for secure data management practices.

This article will focus on security certifications. There are numerous privacy certifications available, and many of the same considerations outlined here apply to the selection of a privacy certification.

Certifications As Competitive Advantage

According to the 2017 report "Cybersecurity and Data Privacy Practice Overview" from BTI Consulting Group, "cybersecurity and data privacy is the fastest growing segment of outside counsel spending and the biggest issue keeping clients awake at night." Law departments must ensure that all their vendors, including law firms, know how to keep their data secure, particularly global companies required to comply with the EU's new General Data Protection Regulation. Certifications are a fast and relatively inexpensive way to upskill, demonstrate competence and signal commitment to areas of expertise. Executive leadership has more confidence in professionals who hold these security certifications, which help firms win business and law departments manage risk. Ediscovery professionals with security certifications are better positioned to remain relevant in current and future positions.

Security Certifications As "Wins" in the Cyberthreat Environment

Information security skills are in higher demand today than at any other time due to the cost associated with human error or attack. As certified ediscovery professionals already know, knowledge, experience and skills are sometimes not enough to convince peers and clients of your expertise. You need the solid evidence of competence that a certification provides.

Certifications are a fast and relatively inexpensive way to upskill, demonstrate competence and signal commitment to areas of expertise.

Client "Wins"

» Clients want evidence that the expertise they require has been independently verified by a reputable certifying organization.

» Clients and law departments must feel confident that their team members and vendors have the requisite knowledge and experience to keep confidential data secure in today's threat environment. The continuing education required to maintain certifications keeps the skills of those responding to evolving threats fresh.

Law Firm "Wins"

» Law firms with dedicated security professionals can set the tone for a culture of security, a strategic business requirement in today's market. Certified security professionals are better positioned to retain and attract work, particularly from clients in highly regulated industries.

» Law firms can state the certifications of their professionals in responses to RFPs, which carry more weight than responses without them.

Individual "Wins"

» An ediscovery professional with security certification training helps reduce risk for the firm and its clients, which increases the professional's value to the organization.

» Security skills give ediscovery practitioners the competence to vet the security of downstream vendors, including ediscovery and even print vendors.

» A certification demonstrates to employers (or prospective employers) the professional's commitment to his or her current career trajectory, signaling career stability.

Choosing an Appropriate Certification

So you are ready to work on a certification; where do you begin? Dozens of quality security certifications are offered by well-respected certifying organizations. Determining what certification to pursue requires an honest assessment of current experience, skills, interests and professional objectives. Are you looking to transition from an ediscovery position to a security position within a corporation? For law firm staff, do you want to support a practice in cybersecurity or to augment your ediscovery skills to work on matters in the firm's cybersecurity practice? Do you intend to become savvy at vetting vendor security responses?

Experience in forensics work translates well to digital forensics, a core component of breach incident response. Breach response is a wide and deep field, requiring extensive knowledge of hardware, software, operating systems, malware and mobile device analyses. Digital forensics is also in constant evolution and will require a long-term commitment to education and an apprenticeship if you wish to transition to this work.

It is important that you enjoy any work you are pursuing; if you do not enjoy studying for the exam, you likely will not enjoy the work either. Cost and time will factor into any decision, so clarifying goals in advance will help align your personal investment with your professional objectives.

Certifying Organizations in Security

Here are a few good certifying organizations that offer helpful certifications:

» **Cybint Solutions, a BARBRI Corporation**
Given the current technological landscape, cyber literacy has never been more important. To prepare professionals for success online and to enhance career development, Cybint is offering Cyber Intelligence (CIC) and Cyber Security (CSPC) certification training. Cybint delivers the best-inclass legal industry training and certifications in the industry.

Cybint's training offers superior cyberawareness to protect your organization from vulnerabilities and equip you to find obscure facts about parties that might not be located using standard search methods. The Cyber Intelligence (CIC) training and the open-source cyber security tools are immediately useful to all legal practitioners. Major U.S. law enforcement

and governing agencies, including the U.S. Attorney's Office, FBI, American Bar Association and International Bar Association, have already partnered with Cybint as a cyber training provider.

Recently, Cybint has launched an advanced training program for professionals seeking a career in cyber. Their level 2 solution consists of a "real-life," hands-on training Cyber Security Analyst (CSA) Lab. Trainees learn the ins and outs of working in simulated Security Operations Center (SOC) by problem-solving real-life based case scenarios in a virtual machine environment. The CSA lab is Cybint's solution to the ever growing cyber skills gap in the industry.

» **(ISC)2**

One of the best-known and respected security training, education and certification organizations is (ISC) 2. Their flagship certification, the Certified Information Systems Security Professional (CISSP), is among the most sought-after certifications today. As of this writing, 14,568 LinkedIn jobs are requesting the CISSP. (ISC)2 has other great certifications focusing on systems security, cloud security, authorization, healthcare information security and other categories. Training is offered directly through (ISC)2 or through partners on their website. There are numerous training options, including online, on-demand training.

» **SANS**

Another excellent and well-established training organization is SANS. SANS develops and maintains the largest collection of security-related research documents in the world and created the Internet Storm Center to monitor and report on malicious activity on the internet, especially for large infrastructure events.

SANS created the Global Information Assurance Certification (GIAC) program to validate the skills of its security professionals. GIAC offers certifications in areas such as cyberdefense, penetration testing, incident response and forensics, management, audit and legal. There are over 30 information security certifications that focus on specific job skills.

Today ediscovery, security and privacy are converging to form a single discipline; we can no longer consider one independently of the others. This convergence requires ediscovery professionals to develop deep skills in security and privacy. The time is now to pursue certifications in security and privacy to show competence in these areas. **P2P**

Today ediscovery, security and privacy are converging to form a single discipline; we can no longer consider one independently of the others.

This article was first published in ILTA's Winter 2017 issue of *Peer to Peer* titled "2017 In Review: Successes and Lessons Learned" and is reprinted here with permission. For more information about ILTA, visit www.iltanet.org.

Vocational and Educational Certifications

by Jared Michael Coseglia of TRU Staffing Partners

There are two types of certification: vocational and educational. Vocational certs are product-specific; educational are more broadly around expertise in a niche discipline, agnostic of tools used. Here are a couple of important market trends to consider when mapping a desired career path and budgeting professional development investments for you or your staff, or hiring in either vertical:

- Ediscovery hiring managers focus on vocational certification (RCA, Ipro, Nuix, iConect, EnCase, etc) first and foremost when considering applicants because most jobs are in law firms or vendors, and these companies want employees who can plug-and-play into the workflow and begin adding billable hours immediately.
- Having a product-specific certification used to increase your earning potential in electronically stored information (ESI); now, not having a certification in the tools requested means you may not even get an interview. There are a growing number of professionals getting vocational ESI certifications, making the job market more competitive.
- Cybersecurity certifications are generally far less product focused and more principle- and practice-oriented. Take, for example, the CISSP, ISC, CISA, CISM, CIPP, and the GIAC certifications. These are some of the most widely accepted certifications in the industry, and none are holistically focused on brands.
- In ediscovery the only truly accepted educational certification is CEDS. In cyber, the CISSP is considered the gold standard for fundamental industry educational validation.
- The Relativity Certified Administrator (RCA) is the certification most frequently asked for by hiring managers in ediscovery. TRU has found that candidates without an RCA have a 20% placement rate while individuals with an RCA have a 29% placement rate.
- There are more jobs posted online requesting CISSP, CISA, and CISM certified professionals than there are people who have them available.
- Transitioning from ESI to cybersecurity requires patience. Getting these cybercerts may take time, advanced training and self-guided education as well as formal classwork. Making the parlay from one industry to the other is a process, not a jump.
- Cybersecurity professionals generally do not want to learn or move into ESI, so it is unlikely that these talents will take jobs from ESI pros. However, ediscovery professionals see cybersecurity as where future opportunities exist and are aggressively looking for ways to make the transition. **P2P**