As seen in

IC Inside Counsel
NOVEMBER 9, 2016
BUSINESS INSIGHTS FOR THE LEGAL PROFESSIONAL

LJN LAW JOURNAL NEWSLETTERS Cybersecurity LAW & STRATEGY®
An ALM Website

MORE ON REGULATORY | RISK MANAGEMENT | CYBERSECURITY & PRIVACY

BY JARED COSEGLIA

Introducing the Cybersecurity Reference Model

Cybersecurity has penetrated our everyday existence, entertainment, and individual concern, but little has been written to help the legal community understand the roles and opportunities within this burgeoning corner of the job market.

CYBERSECURITY IS A RAPIDLY MATURING DISCIPLINE AND industry that has been thrust into the limelight of social consciousness and vernacular with globally publicized events such as the Sony hacks, breaches at JPMC, Democratic National Convention email leaks, and not to be overlooked, the critically acclaimed world of Mr. Robot, which chronicles the lives and events of a post-apocalyptic cyber-hacked society.

Cybersecurity has penetrated our everyday existence, entertainment, and individual concern, but little has been written to help the legal community understand the roles and opportunities within this burgeoning corner of the job market.

Not since the explosion of e-discovery at the turn of the millennium has a new wave of fear, knowledge, technology, compliance requirement, budgetary spend, talent demand and job opportunity hit the legal community as it has in recent years with cybersecurity. The effect that cybersecurity will have on the legal job market will have stark similarities to the boom of e-discovery in terms of opportunity volume, but there will also be radical differences on how these two disciplines have and will continue to change the landscape of the legal industry.

The EDRM (Electronic Discovery Reference Model), created and fostered by George Socha and Tom Gelbmann, has served as a phenomenal lexicon and cost-based approach to viewing and discussing the e-discovery lifecycle. In contrast, the TRU Cybersecurity Reference Model™ (CSRM) is a deliberate skills-based guide to the myriad of technical functions and job responsibilities that exist throughout the cyber continuum.

The CSRM (pictured below) gives clarity to what skills are required through the information security lifecycle and will be a reference to compartmentalize what stages of the model are in high growth and demand.

TRU's CSRM has six primary stages: Inventory, Assess, Compliance

& Governance, Security Architecture & Systems, Monitor, and Respond. This article highlights the similarities and differences between EDRM and CSRM as they relate to the impact on the job market, approach to defining or redefining a career, and how the hiring strategies in both disciplines will evolve over the coming years on each reference model.

The Overlaps

The highest demand for talent in the cybersecurity marketplace right now is on the far right side of the CSRM — Monitor and Respond. These two stages include Threat Analysts, SOC (Security Operations Center) staff, Malware Engineers, Incident Responders and Forensic Investigators. Digital Forensics is the greatest bridge between the EDRM and the CSRM.

Hands-on skills in EnCase, FTK, Cellebrite and many other collection software products are utilized in both e-discovery and cybersecurity. Those with these forensic certifications and experience in data collection will have the easiest time transitioning from e-discovery jobs to Incident Response teams.

The Respond stage is also where practicing Data Governance attorneys, many of whom had lengthy careers in e-discovery, reside and react. These attorneys are cornering a new demand for legal counsel on the nuances of preparing for, and responding to, a data breach.

These skills are in high demand and serve as the other greatest layer of job overlap between the EDRM and the CSRM. It is worth noting that the other primary professionals who have had some success transitioning their careers from e-discovery to cybersecurity are sales and business development professionals, particularly ones inside consulting firms where mature practices in both disciplines are available to sell.

Outside of forensic investigation, sales, and practicing data protection legal work, the career transition from one discipline to another (e-discovery to cyber) is not a short and easy path. It first requires determined intellectual curiosity, significant additional education and certification, an understanding of advanced developing technology proficiencies, and above all, career patience.

Many professionals who have successfully transitioned from e-discovery to cybersecurity will be found working in-house at major corporations across the country.

Hybrid Corporate In-house Talent

Professionals with experience working in-house at corporations in e-discovery almost always have longer job tenure than their counterparts at law firms and service providers. This is partially because these are rarely available and coveted jobs.

This is also because many corporate in-house e-discovery professionals were groomed from within, holding jobs or responsibilities other than e-discovery prior to their current position at the same employer. The few e-discovery professionals who have recently transitioned into the cybersecurity discipline are generally working — and have been working — in-house at major corporations, as opposed to law firms or the service provider community.

This is largely made possible because of how corporations utilize in-house human resources surrounding the collection and governance of their data, an area where e-discovery and cybersecurity overlap.

Inside corporations, the lines are more blurry and the boundaries less defined between the tools and talents that address both discovery and security-related issues. E-discovery professionals in-house are generally involved on a day-to-day basis on security-related issues and initiatives, internal investigations, and work constantly with the security department in IT.

Jay Sanchez, who began his career as a paralegal in Big Law then later became the e-discovery manager for Walgreens and recently transitioned to a Senior Specialist in a cybersecurity investigation role at Best Buy, says: "The need for corporations to accurately collect and understand the life-cycle and management of data is the reason why the interdisciplinary role, which combines cybersecurity, e-discovery and digital forensics, is rapidly evolving."

Sanchez continues to note the cost saving at the end of such investments in overlapping roles and responsibilities in cyber and e-discovery, stating: "This type of new hands-on role allows for a technical liaison to communicate effectively with all high-risk business partners in an organization and develop defensible policies and procedures to minimize risk, assist with investigations, and provide an organization with the ultimate ROI by leveraging tools and centralizing key responsibilities regarding forensics, e-discovery and cybersecurity workflow."

For the last 10 years, corporations have had a history of training and promoting people who know their systems, data and culture into new and evolving roles. For professionals already inside a major corporation who tangentially touch any vertical within the CSRM and want to dive more fully into that area of expertise, now is the time to advocate for role evaluation and realignment to meet the growing needs of the organization, as well as the corporation's ambitions.

Corporations have demonstrated they are more willing to invest in their existing talent and are generally slow to hire full-time from the outside. The more technically-minded could work toward the five-year (CISSP) practical experience eligibility requirement. The more policy-oriented professional could aim to get sponsorship for a CIPP and get involved in how the organization addresses Privacy Shield and matters of Safe Harbor, for example.

The Privacy Piece

Privacy resides in the Compliance & Governance stage and will impact different industries in different ways as a result of regulation. This stage involves developing training initiatives, getting executive buy-in and budget to deploy, executing training, measuring success of training, working collaboratively with security and IT departments and more.

Talent within this stage will assist organizations in following HIPAA, HITECH, PCI, NIST, ISO and a litany of other emerging federal and state regulations. Highly relevant certifications include CIPP, CSCS, CHA, CHP and CCSA.

This stage of the CSRM is a great place for non-practicing attorneys who are looking for a new and emerging career path. Many of these jobs will be in-house at corporations, however, there are and will be niche consulting and legal practices that focus on privacy as well.

In fact, unlike e-discovery, which did not uniformly develop into robust separate practice groups from litigation within Big Law (with the exception of few firms like Seyfarth, Morgan, Littler, Winston), privacy has developed into a standalone practice area and a clear career path for attorneys.

The Compliance & Governance stage of the CSRM is a required element of the model, but is more on the proactive than reactive side of things. So, the demand for talent in this stage will be steady but not overwhelming. Corporations will groom from within for these roles as a long-term talent growth and retention strategy, but corporations are also fully engaging consulting firms and their outside counsel for expertise in privacy and compliance.

When corporations do hire from the outside, they often hire consultants with whom they have a previous working relationship (again, because they already know their systems, culture, etc.). Understanding cyber insurance, for example, is in just as high demand as the privacy, compliance and security expertise. Examining all the stages of both EDRM and CSRM for levels of "reactive" versus "proactive" perspective can highlight and coincide with areas of expected job growth.

Proactive vs. Reactive

While EDRM moves from "volume" to "relevance" working from left to right, CSRM moves from "proactive" to "reactive." With EDRM, the model is almost entirely reactive, with the small exception of some far left work in information governance. In the CSRM, there is a more than healthy mix of proactive and reactive work.

Reactive work occurs on the right side of the CSRM in the Respond and Monitor stages, somewhat in Security Architecture & Systems. Proactive work typically occurs in the Technology Inventory, Assess, Compliance & Governance, and certainly the Security Architecture & Systems stages.

The more hiring an organization has that is reactive, the more likely the organization is in a place of triage or less mature in their security protocol development. If an organization does more hiring that is proactive on the CSRM, it is more likely the corporation has already survived incidents and matured as a result.

Examining the roles along EDRM and CSRM purely from their level of proactive versus reactive responsibility can illuminate a great deal about the kind of role and compensation growth that position will bear based on current market trends. Proactive positions will be in shorter supply, pay less, but have more stability long-term. Reactive positions will pay a premium, are often contract, tend to turn-over quickly but will be in higher availability — especially right now as so many companies

grapple with incident response and data breach for the first time in this new era.

E-discovery professionals, being almost entirely reactive in nature, will always experience higher peaks and valleys of quality-of-life and client demand as litigation spikes and recedes. The balance of proactive and reactive job opportunity in cybersecurity should, in theory, make for a greater level of predictability in volumes of work flow and work-life-balance.

The talent supply in cybersecurity has not, however, caught up with the demand causing a great inequality of compensation, role standardization and definition, and work-life-balance for professionals across the CSRM.

Additionally, with so much focus on breach response, there is a current imbalance of high demand/low supply for the reactive talent. This puts more strain on the proactive talent to develop protective solutions faster, and it puts more strain on the employed reactive talent in organizations who may find themselves over utilized in today's climate.

Some areas of cybersecurity are commoditizing, like pen testing and SOC operations, and have quickly moved to subscription-based or MSSP (Managed Security Service Provider) pricing models. These roles offer higher quality of life and workflow predictability, though they do not necessarily have the rapid compensation increase potential that their breach responder counterparts relish.

It is possible that as the e-discovery industry moves more toward Managed Services models, despite many efforts to maintain per-usage-based models, it will create more balanced work-life opportunities for its professional community. It is also possible that instead, e-discovery and the reactive areas of the CSRM will embrace another global staffing trend to address surging and sudden needs for talent: freelancing.

The Future of Freelancers

A future of freelancing requires a surplus of talent and a high area of talent demand. The highest talent demand across CSRM and EDRM is for "reactive" labor. Moments where talent demand spikes beyond the day-to-day norm (incidents, breach, all litigation) create an opportunity for employers to staff up.

The option for freelance staffing has become more viable than ever across the entire EDRM, but has slower adoption rates across the CSRM. Other than the fact that CSRM is more "proactive" than "reactive" compared with EDRM, why is freelancing more viable in e-discovery?

After a decade of maturation, talented e-discovery project managers and consultants are finding themselves hitting a ceiling of career growth unless they land a management or leadership role, of which very few are available in the market on an annual basis. So where does a seasoned e-discovery project manager or consultant go if not into management?

They are becoming contractors for moments of "reactivity" for the biggest and most complex cases exploding all over the world on a contract-to-contract basis. Employers are slowly realizing such talent is available, and the forward-thinking law firms, corporations, and e-discovery service providers are examining how to integrate contract staffing into their human capital strategy in order to reduce annual overhead, minimize employee liability, increase margins and profitability, scale rapidly, and provide alternate career paths for truly talented professionals in the space.

Contract litigation support professionals was synonymous with contract attorney staffing for almost a decade, but the kind of reactive contract employees that e-discovery vendors and in-house litigation support departments are hiring now are in no way just doc reviewers.

These e-discovery contractors are generally "plug-and-play," as they have dense professional experience in the identification, preservation, collection, processing, hosting and analysis stages of EDRM. These roles include highly consultative project managers and deeply technical analysts with specific skills in Relativity, Nuix and Law. The never-ending reactive nature of litigation, combined with the increasing pool of talent hitting a concrete ceiling at the "project manager" level, will likely support this staffing model and approach to scalability for organizations in e-discovery for many years to come.

A saturation of talent is also available in the cybersecurity vertical, but it has a radically different set of skills and professional experiences that may make the freelance staffing approach premature for cybersecurity job market conditions. In

the cybersecurity world, the current overflow of talent may require more investment in training and professional development from the employer in order to capitalize on the available surplus labor.

Talent in the cyber community is voluminous for two reasons: 1) colleges all over the country have aggressively developed information and cybersecurity programs (unlike e-discovery) and are churning out graduates in droves; and, 2) federal employees who have dense and highly sought after cybersecurity skills are retiring and/or matriculating over into the private sector to more fully monetize their experience.

The pool of talent drawing from recent graduates, however, comes with little to no actual work experience. They also tend to hail from college campuses that are far from the big cities where the job opportunities exist. This robust pool of available graduates is significantly less expensive than even mildly experienced cybersecurity professionals out in the workforce. These grads are also willing to work contract, relocate, travel — things that do not always come with seasoned and more tenured professionals.

The talent hailing from the government agencies comes with varying degrees of experience, technical prowess, and network of relationships. Like university graduates, many federal professionals have never worked for a major law firm or corporation outside of the government. This can prove culturally challenging for some federal employees when transitioning to the public sector, and employers are less forgiving and patient with seasoned talent than college graduates.

Additionally, government employees are often looking to dramatically increase their earning potential by moving to the private sector and thus have far greater compensation demands than college graduates. Most require full-time employment with full benefit packages and do not wish to travel extensively for their job.

Regardless of which surplus is invested in, employers must look closely at what the available cyber talent pool looks like, what the company's needs are across the CSRM, and then make calculated choices about when to hire full-time permanent, when to hire contract staff or, when to hire experienced talent versus up-and-comers.

Skills of the Future

This September at the ALM cyberSecure conference, in the session entitled The Next Generation Cybersecurity Technologies: Pros & Cons for Your Organization, I asked this question to the panel: "You all have spoken eloquently and in great detail about the security technology of tomorrow, but what are the skills that the next generation of cyber talent need in order to elevate and accelerate their careers?"

The answer across the panel, which featured Chaim A. Levin, Chief Legal Officer & General Counsel for the Americas, Tradition Group, Gunter Ollmann, Chief Security Officer (CSO), Vectra Networks, Jared Novick, CEO, BitVoyant, and Christopher Mellen, Director, BDO Consulting, was unanimous: Cyber talent will need to be more "business savvy" to succeed in the future.

With all the new technology swirling around, the leaders of today clearly feel that the leaders of tomorrow must take stock in the business of cyber, not just the technical or legal art of cyber warfare and information protection. So where does "business savvy" fit along the CSRM?

It is the CSRM in its entirety. Business savvy is people savvy, and people savvy comes from understanding what individuals do in order to make the whole of an organization healthy and effective. Business savvy is also understanding the dynamic between corporations, their outside counsel, and the consulting firms and security service providers that they so intimately engage with in business.

CONTRIBUTING AUTHOR

JARED COSEGLIA is the founder and CEO of TRU Staffing Partners, one of Inc. 5000's Fastest-Growing Companies 2016. A member of this newsletter's Board of Editors, he has over 13 years of experience representing talent in e-discovery, litigation support, cybersecurity and broadly throughout legal and technology staffing.