CYBERSECURITY LAW & STRATEGY

MARCH 2018

Law Firm Security Goes Back to School

By Nina Cunningham, Ph.D.

Most readers of this publication today are faced with making business decisions in the face of vast cybersecurity risks. They must act defensively and understand more than just what software is available to prevent or repair an ambush. If law firms want to prevent crime, they must recognize their vulnerabilities and the associated liabilities. As one conference in Londonmarketed the concern, "*No Cybersecurity, No Clients*."

Armed with technical and regulatory weapons for preventing cyber crimes, law firms must administer policies to protect client data and use the systems and services held standard by industries like medicine and banking. No one knows when disruption will take place. New methods of adverse action force executives to make more choices and decisions. All departments must merge their vigilance and join with IT services as IT takes center stage in order to stay prepared.

What Are the Choices for Preparation?

Hiring the right people is a place to begin, but this is also a formidable task in a fast-paced risk environment. It is more difficult than ever to evaluate the credentials of new hires on the basis merely of where they worked or trained. Their focus, if not their training, must be very current. An IT staff member trained in network administration still needs regular briefing on the broader technical field. In every area of practice, whether tax or IP, the challenge is to keep up with IT advances and changes once school is out, the job search ends, and real work begins.

Andrew Jurczyk, CIO at Seyfarth Shaw LLP in Chicago, has spent three decades in law firm technology. He has a healthy perspective on the challenges law firms face in cybersecurity since he first faced post-9/11 risk management. In executive management at a major firm, Jurczyk also sees many substantive changes today in the way managers must work with technical staff. More people work from home, for example, and staff are spread across the country or world. In the risk environment, education of a *Cybersecurity Specialist* never ends.

Since cybersecurity is a threat to every industry, Jurczyk has seen a need to cross-train technical staff and provide support for a variety of educational goals and interests. Doing so improves the contribution each person makes to solving real workplace problems wherever they are. Formal training can be mixed with peer learning and mentoring at work, learning from each other to serve traditional hardware, software, and application needs, as well as ward off cyber crime.

Just as Seyfarth has responded to demands by integrating specialists throughout the organization, there is a growing collaboration with industry and government. Technology penetrates everything, and so is affected by regulation, policy, and credentialing. While industry and government try to inform the schools of future personnel needs, schools are not able to keep pace. Learning must be introduced in the workplace in order to meet client demand for security. The churning process demands renewed understanding of the talent pool and what new jobs are undertaken.

To help accomplish this, firms look to people such as Karla Jobling, a corporate governance recruiter who specializes in cybersecurity talent. Karla worked to develop the BeecherMadden consultancy into becoming an award-winning recruitment company and partner of choice in the UK for risk and resilience.

Complexity in the labor market has created a need for specialists like Karla. While practice management literature provides an overview of what is current, it does not always provide sensible direction for hiring or policy decisions. With less experienced firms, a specialized recruiter can introduce a practical outcome in the effort to unite legal obligation and management practices to protect stakeholders and their data from tampering and destruction. Confusion from the over-abundance of information has a chilling effect, so learning more may help to assuage some fear.

There are opportunities at almost every level to study computer technology. The focus breaks down into topics involving information, networks and security, but advancement is easy when most students enter colleges with a serious exposure to computers. Bright students are even foregoing MBAs to get a head start with new areas such as blockchain. Why not? Consultants at Fortify Experts identify cybersecurity as a field of *zero unemployment* for some time to come.

As risk and liability intensify, law firms are faced with employing the best talent for IT leadership as it becomes central to all firm activity. It is enlightening to get a handle on the latest scope of training and the investment needed. There are many possibilities among degrees, certifications and credentials for capable staff already in place. As each firm is different, it may be better to train the best generalists. This can help them get to Best Practices, for example, which can always change, but the firm can lead itself with a defensive cybersecurity strategy that takes advantage of best practices at a particular moment.

At the industry level, *cybersecurity strategy* grows out of what we already know: the global demand for valuable information is unlimited. The demand for legal services, however, may not be. Strategy for the profession follows what we know, but it also must be developed within the individual firm. Training throughout the organization should be part of the strategy. The levels of sophistication in training reflect heightened risk, which narrows the availability of expertise from outside the firm. This adds good reason for developing capability from within. But training those already doing well is just good policy.

The Department of Homeland Security has developed its own training initiative, including those requiring security clearance. If a firm supports a cybersecurity practice, this clearance could be an asset. The number of other opportunities for training are extensive, from free webinars to formal training through the doctorate. Cyberdegrees.org lists more than 10 institutions offering online degree programs from the basic security analyst to a master's degree.

With the global marketplace trending toward increased specialization and participation, it makes sense for law firms to expand all training into protecting client and firm information and electronic space. Heimdal Security posts a blog listing 50 cybersecurity online courses. Several of the courses are for beginners, others are more specialized. The online campus at Capella University even offers government-approved digital badges when they issue certificates.

More specialized courses in cybersecurity can be found with Syracuse University. Syracuse also grants a Certificate of Advanced Study for law students in National Security Law and Counterterrorism Law. Syracuse also provides access to sponsorship from federal government programs. Independent of how current these topics happen to be, this direction is a sign of things to come in advanced training. They can enhance a legal career as well as offer practitioners greater ability to contribute to data and system protection.

From a defensive posture, law firms will find it imperative to use the cross-training approach to help their IT staff get the latest wisdom on cybersecurity. The deeper the knowledge, the more specialized the staff will become, and thus better able to mentor their team or recommend the right scope of training. Executives and managers will sleep better.

From a risk-management perspective, it would be wise for interested and willing attorneys to select CLE options in cybersecurity. A handful of states require it. Law firms themselves should encourage or require it. Opportunities for CLE are abundant. They are offered by bar associations, such as the ABA, universities, such as the Cybersecurity Institute at the University of Texas (San Antonio), private law firms, such as Steptoe & Johnson, government agencies, such as the U.S. Computer Emergency Readiness team, and CLE specialty groups, such as Lawline. More and more lawyers are involved in robotics and new applications for research and transactional practice. Lawyers can take on new roles in law firms and corporations, and advise their clients on the risk they assume. The demand for cybersecurity personnel will not soon diminish; projections already suggest a shortage of 1.5 million personnel in 2019.

In such a market, lawyers can close the shortage gap by training themselves. A partner in IT would give a firm greater awareness of its vulnerabilities and give clients greater confidence. Cybersecurity will continue to grow as a practice area as clients seek defense and recovery. Firms will be led by IT rather than merely employing it. Lawyers with technical knowledge could better communicate with clients about applications, as well as security. They are already helping to build new computer applications.

Georgetown University is offering a Cybersecurity Law Institute this May for lawyers to stay abreast of legal developments. Designed to attend in person, the program nonetheless offers a live webinar, addressing the latest law on the topic. From a purely CLE perspective, LMG Security offers some unique topics nationwide or online at affordable rates, such as courses for Cyber First Responders for attorneys in law firms.

Conclusion

From any point of view, we no longer have a choice merely to leave the due diligence to the IT department, comfortable with the safeguards of the latest trade in software. This is an arms race like no other; being continually aware of developments will be everyone's job.

***** **Nina Cunningham, Ph.D.**, is an affiliate of Altman Weil, Inc., and president and CEO of Quidlibet Research Inc., a global strategic planning and cost management firm founded in 1983. She is also a member of the Board of Editors of this newsletter.