OCTOBER 17, 2017

Legaltech news ONLINE

An ALM Publication

Time, Not Buy-In, Becomes Biggest Barrier to Broader Cybersecurity Awareness

Inspired eLearning moves into the legal market and aims not to certify, but constantly educate.

BY JARED MICHAEL COSEGLIA

Looking to jumpstart your legal technology career but don't know how? Jared Coseglia of TRU Staffing Partners writes a monthly column for Legaltech News on industry certifications to know and training to acquire. This month's piece takes a look at Inspire eLearning's new training offerings.

Shifting away from the professional power and leverage of individual certification, Inspired eLearning draws the focus to how organizations can educate their entire human capital on cybersecurity to improve the health and wealth of the company. Individuals can register for Inspired eLearning training, but that is not the primary business model (B2B, not B2C). This quarter, Inspired eLearning, ranked No. 50 in Cybersecurity Ventures' top global cybersecurity companies, released notable training offerings geared toward legal for its current and prospective clients, with more to come throughout 2017 and 2018.

This turn toward legal-focused content was quite deliberate. "Our leadership identified legal as a niche with potential opportunity for demand," says Matt Urbancic, head of marketing for Inspired eLearning. "Cybersecurity awareness is becoming bigger and bigger in law firms as organizations insist that third parties have the proper security protocols in place, like properly addressing legal IT requirements."

This impulse has proved to be fruitful for Inspired eLearning, reinforcing the vital role outside counsel and in-house attorneys continue to play in the decision-making process and institutional protection of critical data, infrastructure and intelligence.

In addition to broader legal security training like "What to Do If You Are Breached," Inspired eLearning is on the

JARED COSEGLIA

cusp of offering GDPR (General Data Protection Regulation) training to its customers. The EU GDPR is the self-proclaimed "most important change in data privacy regulation in 20 years" passed by the European Union and will dynamically affect any company doing business in or with Europe. "Courses are built to help learners understand what the regulations are, whether in the EU or in the

U.S., and what their obligations are regarding the regulations," says Urbancic.

The GDPR product is just one of over 150 training modules immediately available to Inspired eLearning consumers, with hundreds more in development or left behind on the cutting room floor. Inspired eLearning is constantly creating new content, looking for the gems that become most wildly required and desired by corporate and now Am Law clientele.

Legal and GDPR training modules constitute more advanced product offerings from Inspired eLearning. Just as security is a constantly evolving technological art form, so too must the training and education around security constantly adapt. Inspired finds that customers are often coming to them uncertain about what security training they need depending on the maturity model of their existing human and technology infrastructure. Security awareness training is not a one-and-done or even an annual effort.

"Ideally, you don't do this once a year," says Kyle Metcalf, the newly-minted Inspired eLearning CEO. Metcalf describes what he calls the "cyber knowledge continuum" as taking education beyond formal training modules and into areas where the corporation can intuitively

remind people of proper techniques for cybersecurity. "This is something you need to be reinforcing throughout the year, through training, yes, but also with short videos, assessments, digital displays in a hallway or call center and more."

For Inspired, it is an iterative process with customers to determine what continuing education they need; however, for the basics, most customers are consuming the same initial training modules. Metcalf notes that there are "a handful of courses that cover most everyone in the beginning." Most learning modules are between 15 and 30 minutes, with more sophisticated content being shorter and targeted, and the broader and less advanced modules being longer and often segmented into shorter digestible units.

For example, one of Inspired's most popular training modules is one called "A Day in the Life," which Metcalf describes as "covering everything from phishing to social engineering to physical security badge access and no tailgating to laptop security and more." The module takes about one hour and 20 minutes to complete, and is almost always "broken into chunks" when delivered, according to Metcalf and Urbancic.

The segmenting and time requirement for training has quickly become a forefront concern for Inspired eLearning's the creative and product development teams. "Larger organizations have certain time allotments for this training and rarely want their employees spending over an hour consecutively for security awareness," states Metcalf.

Within any corporation, regardless of size, there are a variety of business divisions vying for the time of all employees to roll out training. Security

awareness, whether purchased externally or developed organically, competes with other agendas like human resources, marketing, compliance and business intelligence. Companies like Inspired eLearning are not necessarily in the business of creating content that is acutely specific and customized to the niche needs and vernacular of a company spanning the breadth of all their training and educational requirements. Like products at a drugstore fighting for shelf space, so too do various training initiatives compete within a corporation for visibility and priority of deployment to the employees. Where once the awareness itself was the barrier to consumption, now time has become the most critical variable in creating the right package of education and product deployment.

"In 2015, we saw a massive shift in the market," says Metcalf. "Very public hacks led to a massive rush for corporations to get this training out to their people. Prior to that it was a bit of a challenge." The American awakening to cyber vulnerability is often attributed to the Sony hacks of 2014.

Metcalf asserts, "Who's going to care if the public doesn't? Over the last three years, the threat landscape has radically changed. Hacks have everyone's attention, and all companies are thinking about security in a different way now."

However, just because organizations are "thinking" about security does not mean they are doing anything to enhance the defensive fortitude of their employees' education, often because of the time it takes to educate everyone. To combat the time variable, Inspired has created ways for employers to help employees "place out" of certain training requirements. By offering targeted assessment surveys, an organization can measure someone's security aptitude through self-examination. This saves time by giving some employees basic training and others targeted training, all while keeping a balance of job productivity and cyber safety.

Inspired has also developed exercises corporate stakeholders can secretly deploy to evaluate which employees may need critical security awareness training. One example is its proprietary phishing simulator. "One of the biggest threats we see right now, and one of the easiest ways for bad guys to come into an organization, is a phishing attack," professes Metcalf. Inspired can run simulated phishing attacks to employees and assess how difficult is it to trick specific individuals. As for those who open the emails, follow the instructions, click on malware links or do not think to click the custom "malware" button, Inspired can embed their information within a company's Outlook, flagging them as employees who are most vulnerable to becoming unwitting actors in a potential hack.

This is a dynamic shift from trying to convince corporate stakeholders that security awareness is essential and has value in order to sell products to instead selling focused on convincing employers how they can commit the time and customize their security awareness training. "We can give clients everything they need to get the right security awareness training," says Metcalf, "but we can't force them to do it. The responsibility is on the customer to follow through with the training, make the time, and make employees invest the time to take the training."

Jared Coseglia *is the founder and CEO of TRU Staffing Partners, an Inc 5000 Fastest Growing American Company 2016 and National Law Journal's #1 Legal Staffing Agency, and has over 13 years of experience placing thousands of professionals in e-discovery, litigation support, cybersecurity and broadly throughout legal and technology staffing.*