ALA + ILTA March 9th 2016 Panel Discussion on IT Security Compliance and Auditing

Q&A, and Comments from the Panel Discussion:

Q – How can we manage attorneys using their personal email accounts?

A – Marco: This becomes a bigger question of scalability. Somehow some think this doesn't apply to law firms, but it certainly does. Start with explaining the policies and rules with why they exist first. Walk them through a live story so they understand why the policy was created. For example, show a mobile phone with a simple password of 1234, and then open a document or email in front of them.

Q – We have a large client asking us for an audit. How do we navigate this? What audits are available?

A – Marco: If you represent a major health care client and are considered a "Business Associate" because of receiving patient personal information, then the firm is required to be HIPPA compliant. The HIPAA Omnibus Rule led a corporate client to instruct a smaller law firm to remove all their USB ports from everything including laptops, workstations, printers, etc., to help prevent data from leaving the firm. Another firm we're helping is going through a SOC audit, because they represent a financial institution. Other security audits may include vulnerability assessments and penetration tests, performed by third party companies.

A –Jeff: Or, at my company [Raytheon] we allow encrypted USB drives, but they cost more than your traditional USB drives, more than 15 times. Another further service offering can be security monitoring offered by one of Raytheon's acquisitions, Oakley Systems, Inc. First the company agrees to being monitored for protecting its data assets, intellectual property, and infrastructure. For example when 500GB of data is downloaded at 4AM on a Saturday morning, this would be flagged as the unusual activity that it suggests. They minimize this data loss by especially monitoring the outbound traffic, and don't "let them leave," said Jeff. Jeff added that he was on a panel recently with Congressman Michael McCaul, along with former DHS Secretary Michael Chertoff. Jeff's takeaway was that Congressman McCaul spent five minutes during his opening remarks talking about how rampant intellectual property theft is with this closing statement: "why invent when you can steal it." Our economic stability associated with IP theft is a huge issue. Cybercriminals are targeting law firms for your client's IP, thus this data needs to be protected. Another way to is map to a NIST cybersecurity framework. Again, a third party company help you with this.

Q –There seems to be no standard. Attorneys don't go to meetings on cybersecurity. When will they be held to these standards?

A –Steve: Corporate Counsels are now holding them to these standards, with indemnification, along with giving us the right to audit our outside firms, or otherwise you will face large litigation insurance premiums.

Q –How can we overcome the technophobia among maturing attorneys and others?

A –Marco: Although law firms do not yet have to report breaches, with legislation possibly eminent, the pressure to adapt and change is here, being pushed by the corporations you represent. IBM says costs of breaches have cost them $6.5 million dollars. Social engineering hackers continue to be very sophisticated, scraping law firm websites to learn client names, and other data to aid in their phishing exercises.

Marco: [comments] When All Covered performs ethical hacking and social engineering experiments within a law firm, we receive an alarming 82% response rate. Some employees clicking on links they shouldn't are sharing personal information that they shouldn't send us. Why is the response rate so high, and what can you do about it? One reason, is that the hacker is has chosen carefully the target (usually just a handful, or even one person within the firm, and include some highly sensitive information that lends the targeted to trust the hacker and share a little more data. The hacker may only be seeking one more piece of critical information, with the attempt to fly under the radar of suspicion. Therefore the need for more employee education is paramount if a firm is to attempt to stay protected.

Jeff: [comments] A FISMA quarterly audit might define a remediation plan. However this no longer makes sense with more and more MSPs (Managed Security Provider) entering the market. Solutions might include employing cross domain, compartmental and financial service

Q –Law firms are lagging; somebody needs to set a standard to reduce this liability. My colleague's firm recently had a data breach, and it could have easily been ours. No joke. Do you see any enforcement coming soon?

A –Steve: Where state governments do not set standards, the Federal Government does by way of the FBI, and FTC with prosecution. Law firms are actually beginning to step up, with adding responsibilities of oversight to key personnel, and by partnering with third-party IT companies who offer security solutions specific to law firms.

A –Marco: Keep the nightmares coming… As a national legal IT provider, I hear these stories first hand. It is challenging to bring senior influencers along within law firms. Many state bars have set standards around cloud computing. There is a lot of case law that has come about, given all of the constant data breaches we've been seeing, and more to come for sure. Take a look at Document management software. It has been shifting from client centric to matter centric solutions, because data is also being leaked within the walls of the firm by way of paper.

A –Jeff: Risk varies and effect the priorities of protecting this data vs. that data. Some data must absolutely be protected, with some you *may* want to protect, while other data is less of a priority. The cloud encryption business is growing. Again, this all flows down to the critical 16 infrastructures.

A –Steve: [comments] With the growing space of IOT (Internet of Things), we have to be even more on guard. Think of refrigerators, smart TVs, smart phones, Wi-Fi in automobiles; it's endless. Even jet engines that are flying over us [pointing up to the sky] are being monitored 24x7 for maintenance and performance.

Q –What are ways to assess and reduce this risk?

A –Marco: Reasonable effort has to be made. If you need help, get help. Seek help outside of the firm.

A –Steve: For myself, if I don't, I risk losing my license to practice law. Yes, outsourcing is an answer.

A –Jeff: Email encryption is a must. SafeNet or another solution will do this. Quantum cryptography is also changing how we encrypt information. Many national labs are working together on this so it will be available on your home computers soon. At Raytheon, we perform annual training on IT security with all employees. Tests are then given after training, and until the employee passes, they cycle through it again.

Q –Our primary focus in our job is to bill the client. How can we do training? Can CLE be added to this training to encourage attorneys to buy in further?

A –Marco: If attorneys are not attending training, they do not understand the risk. Encription of email is fundamental, and begins at the grass roots. Shock and awe works; read them the headlines, or share a story. Firms have must begin with user education.

A –Steve: Read the Northern District of California opinion to deny the motion to dismiss a complaint filed against Google alleging that its Gmail service unlawfully intercepts the contents of emails sent by and to Gmail users. You might also read Volume 21 Issue 3 of the Richmond Journal of Law & Technology, an article by Timothy J. Toohey which talks about the uneasy relationship between lawyers practicing law and using technology. Toohey writes the "…technophobic attitude may no longer just be harmless conservatism. In the world of growing security risks, ignorance of technology may lead to violations of lawyers' fundamental ethical duties of competence and confidentiality."

Q –Are there affordable products to help manage protecting data on mobile devices?

A –Steve: Webscense, now ForcePoint, and AirWatch are both leading inexpensive solutions available. We refer to this as Mobile Device Management (MDM) software.