I’ve done my best to capture the questions I remembered from the presentation. When a presentation is not recorded it becomes a bit trickier to track, especially given all the good questions that arose. I jotted down the following (in no particular order):

**Q**. What do you do in ATX Forensics?

**A**. I primarily work in the threat intelligence and training lines of business for ATX Forensics. I also assist with the ISO accreditation work we perform as well. While I train individuals in one-, two-, and five-day courses throughout the year, I also present at conferences and associations like your own.

**Q**. You mentioned behavior analytics in the presentation. What are some uses/benefits of behavior analytics?

**A**. Behavior analytics (BA) allows you to gain a picture of network activity, to understand user behavior and craft patterns of normalcy and unusualness. Network awareness is something that both Threat Intelligence (TI) and Data Loss Prevention (DLP) focus heavily on. Behavior analytics allows you to understand – at a company level and individual level – network activity, its timing, its duration, its types and impact. This can be crafted into patterns that can spawn alerts to let you know when activity happens outside the norm. For example, someone accesses network shares that they don’t normally access. Or, several shares are enumerated back to back within a few seconds – a chief sign of ransomware. BA can provide valuable and actionable insights into possible insider or external threats.

**Q**. Where/how you store the data you collect? When you collect for another company (two-part question)?

**A**. It varies somewhat to the data collected and its eventual disposition. The short answer is in mongo and sqlite databases for text and archives of raw file storage for other data. The longer answer is a majority of threat data goes into CRITS (Collaborate Research into Threats), a MITRE written open source project. Data not appropriate for CRITS is stored in separate databases or in archives as required. A key item we strive to achieve is to collect data on the front the way we want to store it on the backend. That cuts down on a lot of data manipulation and makes it easier to retrieve.

Sensitive data that ATX Forensics retains is separated and encrypted. Customer data collected during a threat risk assessment, penetration test or other forensics activity is either purged or turned over to the customer at the termination of services. Unless specifically provided for in a contract, ATX Forensics does not retain customer data.

When we assist in a customer is designing, setting up or collecting data, we follow their guidelines while providing insight based on best practices we have seen in the industry.

**Q**. Could you discuss the security of storing data in the cloud versus storing locally?

**A**. Cloud storage is no more or less secure than local storage. Good security practices, proper configuration of hardware and software, and data awareness are key to securing information in either location. A misconfigured, leaking Amazon bucket is just as bad as a misconfigured local server open to the world.

**Q**. Do you perform trending in Behavior Analytics?

**A**. Absolutely! Trending provides history – historical insight into network levels and user activity. Historical views allow you to map activity, find peaks and valleys and understand the timing, duration and types of activity. With that in hand, you can look for outliers or pinpoint when unusual activity is occurring. For example, the network may not have a lot of outgoing upload traffic, especially during off peak times. Seeing unusual traffic here, especially if unexpected should generate an investigation to understand what’s leaving the network. It could lead to malware or something benign, like an employee upload research data at the completion of a project.

**Q**. Talk about security of a wireless Router versus Landline (Ethernet)?

**A**. Inherently a wired connection is more secure compared to a wireless one. Physical access is required to compromise a wire connection. Wireless broadcasts widely to cover your house and a bit beyond. While secured behind passcode, breaking into them is a fairly trivial to a trained hacker. War driving is a common concept. Routers are set up to broadcast an SSID for identification. If you can see the SSID, even if you have it hidden (not much of a stopping point), you can access the wireless point. From that juncture, it’s just a matter of time to guess the password to gain access. WEP is easy to break. WPS is better. As a reminder, physical access trumps everything. If you can put your hands on it, it becomes trivial to circumvent protections and gain access.

**Q**. You mentioned a Threat Assessment. What is that?

**A**. A threat assessment looks at a company from the outside, either passively or semi-actively, to gain a snapshot of threats that may exist. It looks for impersonation of the corporate identity, leaks of data in social media, phishing activity, content duplication, risk to employees and the company from large breaches, and around two-dozen other categories of information. This data is collected, compiled, analyzed and fed back to the company requesting the assessment to give them a snapshot of how vulnerable or protected they are against threats.

**Q**. Could you discuss how to implement a SOC/TI/DLP for a small business (three part question)?

**A**. This really depends on the size of your company. A small company likely would not profit from having a full-fledged SOC, even if only staffed by one individual. Most especially if the company deals primarily in tangible goods or services and is not moving a lot of valuable and/or financial data or has intellectual property to protect. An operations center can be outsourced but its not recommended. If a company is large enough or seated strongly enough in the digital space to require one, it’s best to do so in house to make the response effect workable.

Threat intelligence is another matter. Find a company that will sit down with you and tailor a product specifically to your intelligence needs. No threat intelligence product off the shelf will ever 100% meet your needs. Everyone and their situation are unique and that same uniqueness requires a tailored approach. A company that will sit down with you and educate you on what you need is the best one for you.

The DLP process should never be sent to a 3rd party. Exposing the inner workings of your company and where all your valuable data lies is not a good business decision. DLP should always be performed in house, whether by software, trained individual or both.

**Q**. Could you talk about incident response in relation to cyber insurance?

**A**. If you have cyber insurance you have an incident response team. While some variance exists in how these contracts are written, the insurer retains several companies that are engaged to perform incident clean up, mitigation and resolution. If you have an in-house team, it works in tandem with the one called in by the cyber insurance.