Integrating a Proactive Security Strategy

Executive Summary by Frank Anastasio

The following is a recap of the April meeting of the Triangle Technology Executives Council (TTEC). With a discussion topic of *Integrating a Proactive Security Strategy*, the panel was made up of experts in the field from various organizations, business areas and roles.

Participating Panelists:

- **Jerry Fralick**: Chief Security Officer – Lenovo
- **Paul Dalberth**: Director of Infrastructure & Security – Martin Marietta
- **Ed Recavarren**: Head of Risk, Governance & Compliance Group – NetApp
- **Mike Lewis**: CIO – Trillium Health Resources
- **Dean Scharnhorst**: Asst. General Counsel – BB&T

Key Takeaways:

- It is important to understand legal regime under which you operate.
  - The patchwork of laws in US (and internationally) at both the national and state level drive increase levels of complexity.
  - Engage your legal team to demystify common misconceptions.
  - There are also multiple frameworks and standards that must be considered.
- A first step is to have an understanding of the data that requires protection.
- Current cyber security *defensive* measures are not as mature as the *offensive* measures utilized by the attackers.
- Current security strategy methods being incorporated:
  - Employee Training
    - User education across the organization helps stop threats before they materialize.
    - IMPORTANT: manage awareness and notification processes.
    - Sharing audit results internally can help drive behavior.
    - Improves the communication with security staff and counsel, so employees are comfortable asking their advice before taking an action.
  - Other Methods
    - Penetration Testing – which was argued that it is not as proactive as some think.
    - Remediation of previously discovered issues.
    - Data Loss Prevention Tools – protect employees from sending Personally Identifiable Information (PII).
    - Incident Response Plans – develop, test and modify regularly.
  - Process Oriented Approach
    - Business risk assessments and formal risk acceptances performed by appropriate executives.
    - In some cases, this approach if just emerging as the senior business executives view of technology and the threats is becoming clearer.
- Your approach must be constrained to what you own and control.
  - Accessing third party environments can put you in violation of regulations.
  - Some investigative practices can be at odds with defined policies and procedures.
- Impact of Internet of Things
  - Brand management can drive vendors to take the appropriate security measures.
  - Security must be built into app development
- Consider the entire technical stack
- Event sponsor Dimension Data provided a **Global Threat Report** for TTEC members.