Table Leader: Rick Clark

Participants: Alex Branistreanu, Scripps Health

(sorry did not capture everyone’s information)

Questions to lead the discussion:

- Do you feel VM is working and worth the effort?
- When do we worry about or address?
- Do you feel software vendors are doing enough (reporting, fixing, liability)?
- What works? What doesn’t work?
- What metrics are the right metrics to provide a true picture?

**Key points from Discussion:**

Vulnerability management – “It’s like treating germs”

The scope typically includes the following:

- Network
- Applications
- Cloud
- Supplier management
- Endpoint security (mobile security)
- Then there is always scope creep

We are fighting a difficult battle as criminals have the same tools and sometime better tools.

Vulnerabilities are all over the map and IT can’t keep up. Companies struggle with systems that are running legacy apps that can’t be patched.

Managing vulnerabilities is about threat management and first steps are identifying the know (and the unknown).
Can we blame the vendor for holes in the application, or the end user for not implementing using best practices? Security is not part of the developer’s job requirements. End users are not taking the time to implement in accordance with vendors best practices (just want it up and running).

Ways to mitigate include best practices:

- Developing security standards for patch management
- Sharing of threat intelligent
- Reduce threat environment through network segmentation
- Cooperate with vendors
- Define security requirements in RFP/RFQ
- Contextual security, consider the situation and location
- Protection must be built into the cloud contracts (cloud providers won’t allow scanning)

Convey to the business owner the impact ($ and reputational) of the vulnerabilities on their assets by considering the vulnerability, threat, and risk level, keeping in mind the data classification to help raise or lower the risk.

Reporting to C level should be done using four quadrants either in a format similar to SWOT or a scatterplot.

We need to start the education early and mandate educators teach securing coding as early as high school. iPad apps can be approach to educating the young.

To address vulnerabilities “built-in” to applications there should be a correlation of indicators and forcing vendors to talk to each other.

Companies should look at white papers discussing best practices, add contract language (templates available from Software Assurance Forum), and ask the questions about how the company addresses vulnerability management in the RFP.