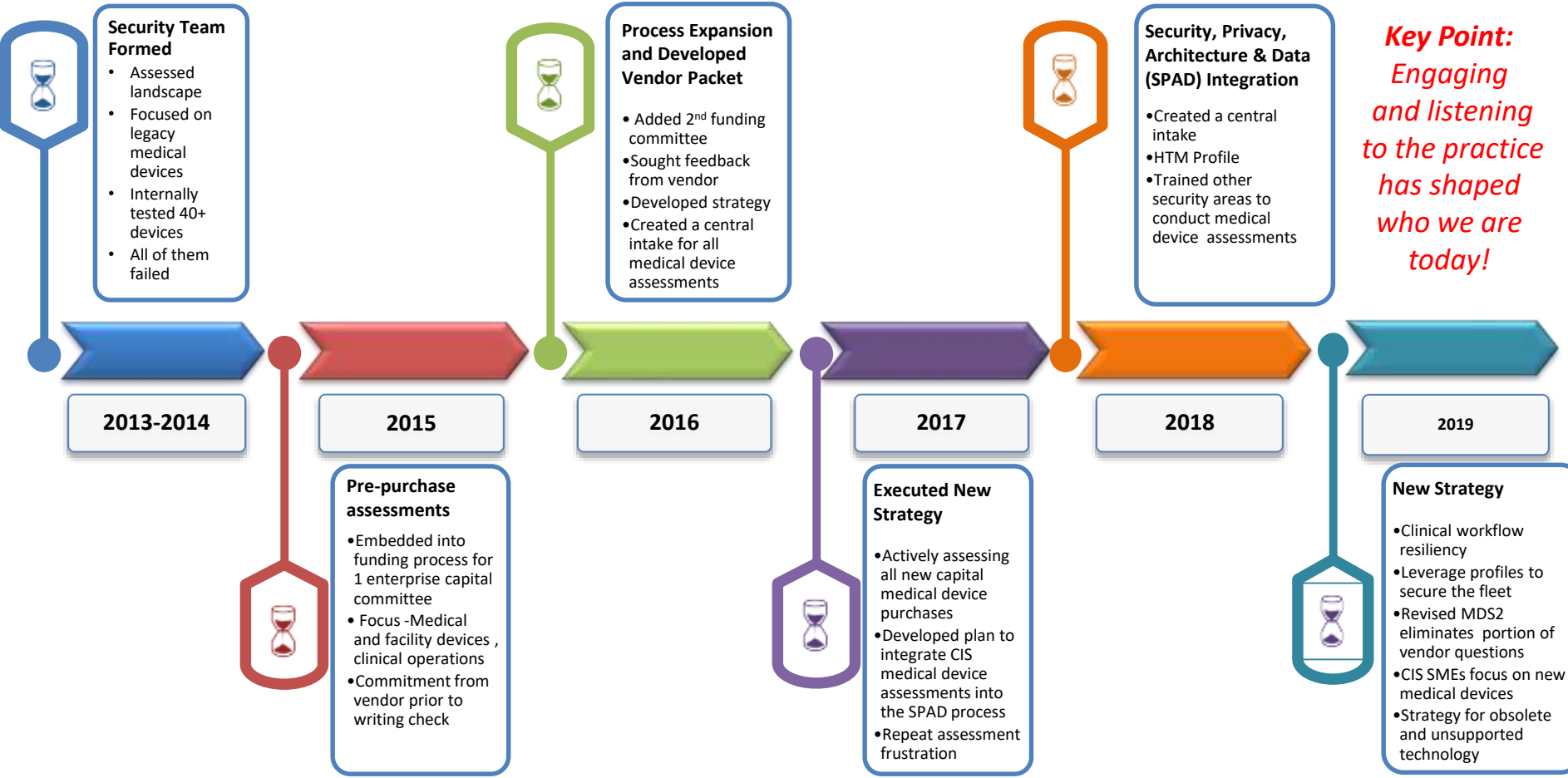
Roundtable Discussion on Medical Device Cyber Security

George Reed and Emily Mengel (WakeMed), LeahAnn Clemens (Mayo Clinic)

Mayo Clinic's Journey to Secure Medical Devices Timeline

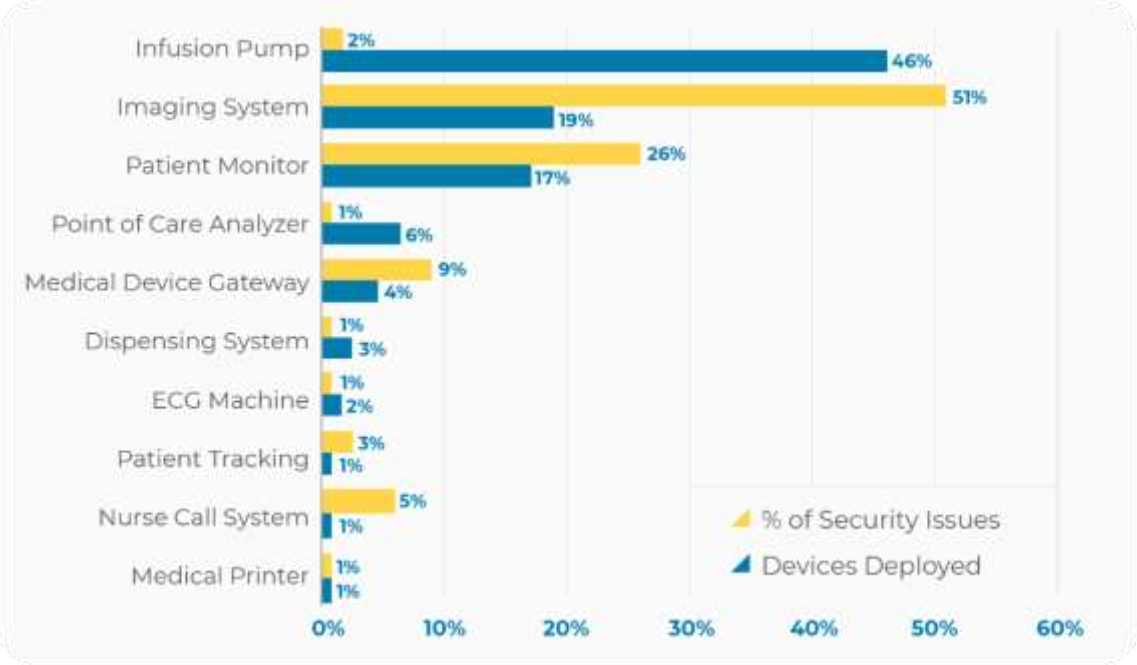


Develop a Medical Device Security plan

Standard Inventory/Procedure/Policy

1. Inventory
    1. Capture and document network information IP, MAC Address, Host name, VLAN, OS, SW, ePHI.
2. Patch Management Documented into CMMS
    1. Implement into Preventive Maintenance plan
3. Capital planning (legacy Equipment)
4. Security validate during preventive maintenance to ensure controls are on device. (last patch, Passwords etc..)
5. Security language within Purchase and Service agreements

How well do you know your medical device vulnerabilities?

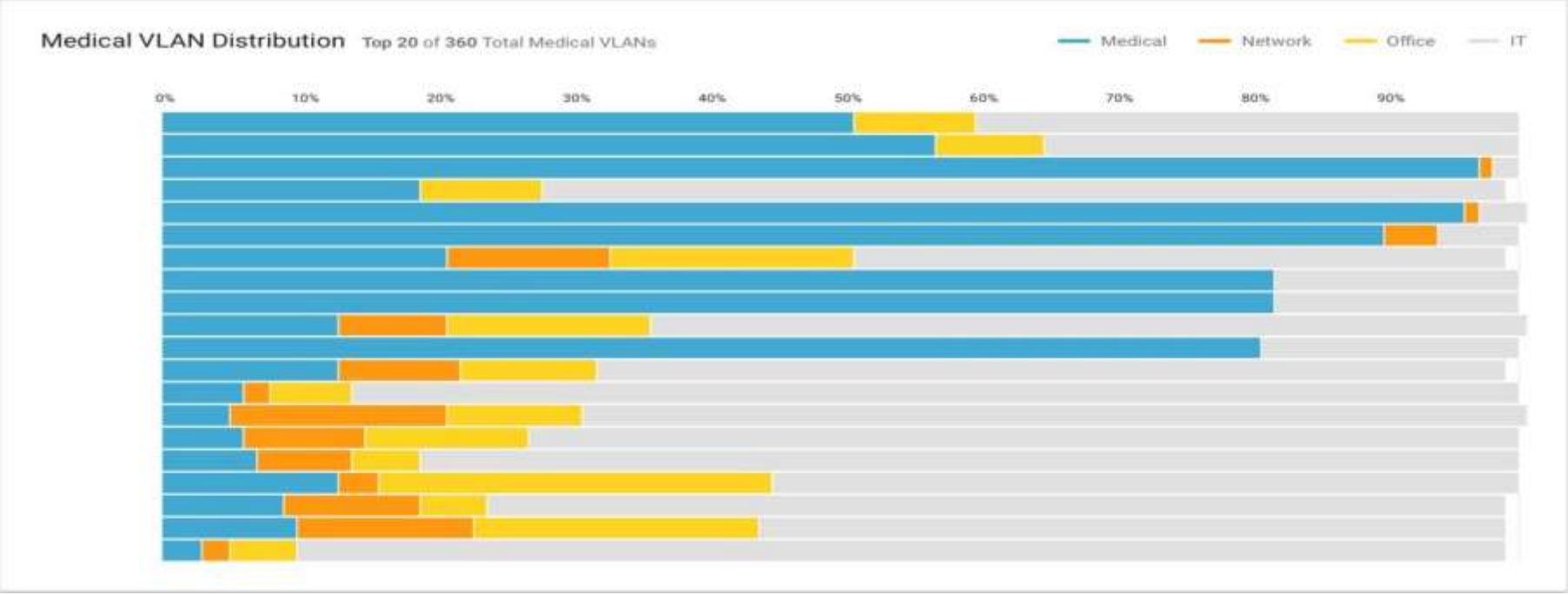


Information provided by Zingbox

Vulnerabilities/Actions

- Patching
    - Working with vendors on current and future patches
- Outdate OS/Legacy Device
    - Capital planning
- Misconfigured network devices or not properly isolated
    - *Zingbox*, Medigate, CloudPost

Medical device VLAN Discovery through use of Zingbox



Incident Response

- Tabletop Exercises and rounding- Wakemed
- Cybersecurity Simulations- Mayo Clinic

Action Plan for CE Departments

- Incorporate Security into medical device procurement planning
- Passive network monitoring tool
- High visibility on Patching status and ownership
- Build an IS, CE Security workflow

What questions can we answer?