12TH ANNUAL LEADERSHIP EVENT

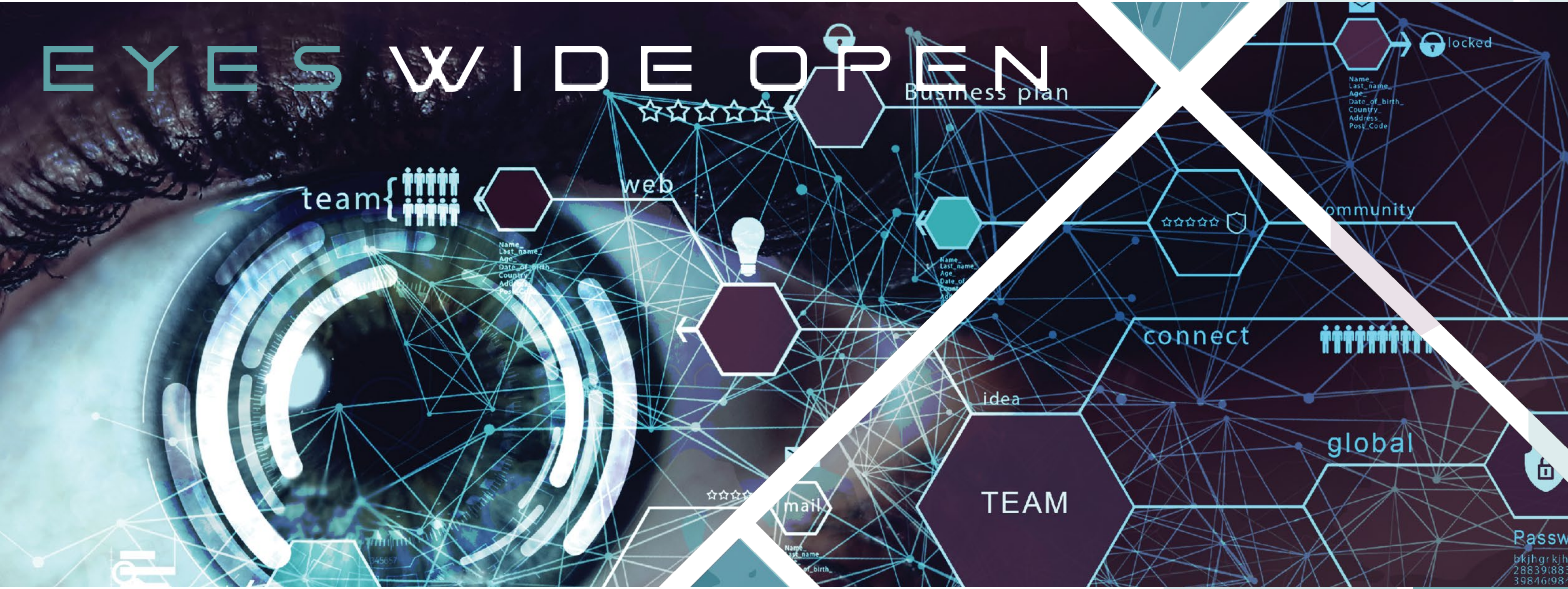
CYBER SECURITY SUMMIT

Security solutions through collaboration.™

TITLE SPONSOR

Island

EYES WIDE OPEN



CYBER SECURITY SUMMIT Security solutions through collaboration.™ 12th Annual Cyber Security Summit | October 24-26, 2022

cybersecuritysummit.org

Security Resilience Program and Medical Devices

Debra Breummer

Senior Manager,
Mayo Clinic

MAYO CLINIC

Security Resilience Program and Medical Devices

Debra Bruemmer, BS, MBA, CISSP
Senior Manager, Office of Information Security
Mayo Clinic

Cyber Security Summit, Minneapolis
October 24,2022

The New York Times

Cyber Attack Suspected in German Woman's Death

Prosecutors believe the woman died from delayed treatment after hackers attacked a hospital's computers. It could be the first fatality from a ransomware attack.

Attack September 10 2020, Article September 18, 2020

The ransomware attack involved servers at the University Hospital Düsseldorf on Sept. 10. Roland Weihrauch/dpa, via ZUMA Press

HEALTH IT SECURITY
xtelligent HEALTHCARE MEDIA

Home | News | Features | Interviews

HIPAA and Compliance | Cybersecurity | Cloud | Mobile | Patient Privacy | Data Breaches

EWS

UVM Health Continues to Feel Effects of Ransomware Attack

Eight months after a ransomware attack that incurred costs upwards of $63 million, UVM Health continues to experience setbacks and financial losses.

Attack October 2020, Article June 2021

HEALTH IT SECURITY
xtelligent HEALTHCARE MEDIA

Home | News | Features | Interviews

HIPAA and Compliance | Cybersecurity | Cloud | Mobile | Patient Privacy | Data Breaches

INTERESTED IN LEARNING MORE ON HEALTHCARE TOPICS
DISCOVER OUR HEALTHCARE STRATEGIES PODCAST
SUBSCRIBE AND LISTEN NOW

EWS

AZ Ransomware Attack Leads to Unrecoverable EHRs, Data Loss

An Arizona medical center will have to rebuild thousands of patient records after a ransomware attack resulted in corrupted EHRs and data loss.

Attack May 2021, Article September 2021

HEALTHCARE INFO SECURITY

Topics | News | Training | Resources | Events | Jobs

TRENDING: A Journey to Mitigate Cyber Risk with Trusted Data • Live Expert Panel | Threat Detection & Incident Res

Fraud Management & Cybercrime , Healthcare , Incident & Breach Response

Hospital Chain's Patient Portals, Other IT Still Offline

CommonSpirit Facilities Still Hampered by Last Week's Cyber Incident

Marianne Kolbasuk McGee (HealthInfoSec) • October 11, 2022

Twitter | Facebook | LinkedIn | Credit Eligible | Get Permission

We are continuing to manage an IT issue that is affecting some of our systems. Our IT teams are working diligently and we will provide an update as soon as we are able. Our clinics and hospitals remain open and we continue to provide care to patients.

MORE INFORMATION

CHI Health

We apologize for the inconvenience. This site is temporarily unavailable.

Attack Oct 4 2022, Article Oct 12 2022

CHI Health says that its patient portal and other IT systems are still affected by an incident last week involving parent company CommonSpirit.

MAYO CLINIC

Change is Slow but it is Happening….

- **Limited financial resources**
  - ~ 70% of healthcare providers have less than 200 beds
  - ~ 80% of medical device vendors have less than 50 employees
- **Medical Devices are an “easy” target for cyber attack**
  - Long “shelf life” compared to standard technology
  - Large presence of Windows 7 (unsupported January 2020)
  - Fleet of Windows 10 assets (fully unsupported October 2025)
- **Manage risk through guidance not always understood**

Contains Nonbinding Recommendations

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Contains Nonbinding Recommendations

Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Scope of Healthcare Assets

- Network (e.g. wired, wireless)
- Traditional IT managed assets (e.g., workstations, servers)
- Applications (e.g., traditional and FDA certified applications)
- IoT devices (e.g., card access, refrigerators, infant protection, cameras)
- Medical Devices (e.g., infusion pumps, MRI, medication stations)

Patient Care is delivered through a diverse set of assets …..
Some requiring special handling

©2014 MFMER

Security Approaches, Tools, and Technology

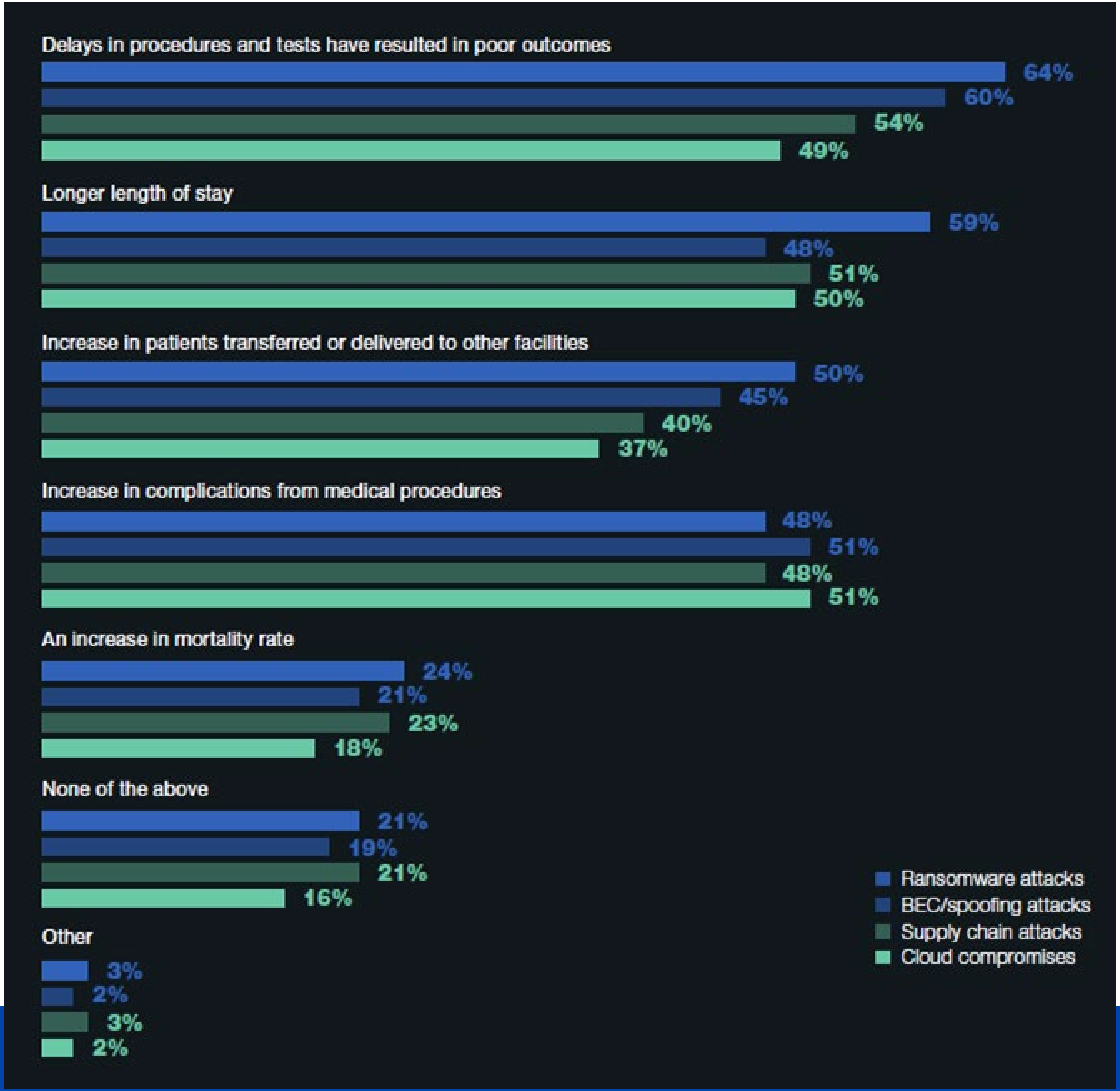
- Network Access Control (NAC)
- Network Segmentation
- Monitoring tools
- Application code scanning
- Vulnerability scanning tools
- Anti-virus, Application Whitelisting
- Patching
- Privileged Access Management tools
- Manage Remote Access tools
- Etc.

Medical Devices and SaaMD are not managed like traditional technology

©2014 MFMER

What impact have cyberattacks had on patient care? *(multiple responses allowed)*

- Ransomware attacks are more likely to hurt patient safety and care delivery than other cyberattacks.
- 64% stated delayed procedures and tests resulted in poor patient outcomes.
- 50% saw an increase in patients being transferred or delivered to other facilities.
- 24% saw an increase in mortality rate.



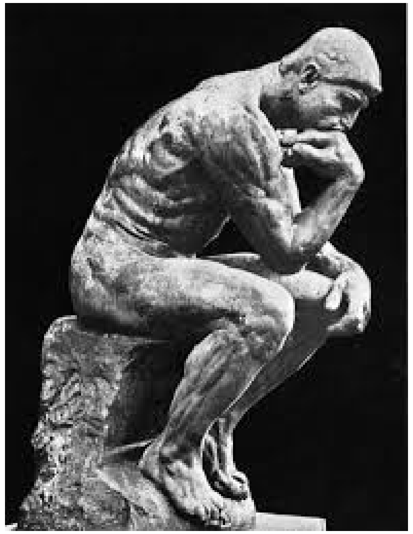
Source: pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf(proofpoint.com)

To protect clinical workflows, medical devices need to be secure

©2014 MFMER

Information Security Philosophy - Medical Device

- **Provide a secure environment**
  - Apply technical and administrative controls
  - Educate workforce
- **Incorporate security into the procurement process**
  - RFP questions and standard security contract language
  - Practice drives purchase decision, security enables secure execution
- **Apply security actions to the fleet of legacy devices**
- **Test medical devices – but be strategic**
  - Expect testing to be part of manufacturer's processes
- **Support industry collaboration**
  - Customer Advisory Boards
  - HISAC, HSCC, IMDFR, CMDC, etc.
- **Benefit society by using Mayo Clinic's influence**
  - Require changes to be made to standard product
  - Drive changes for long term vendor process improvements



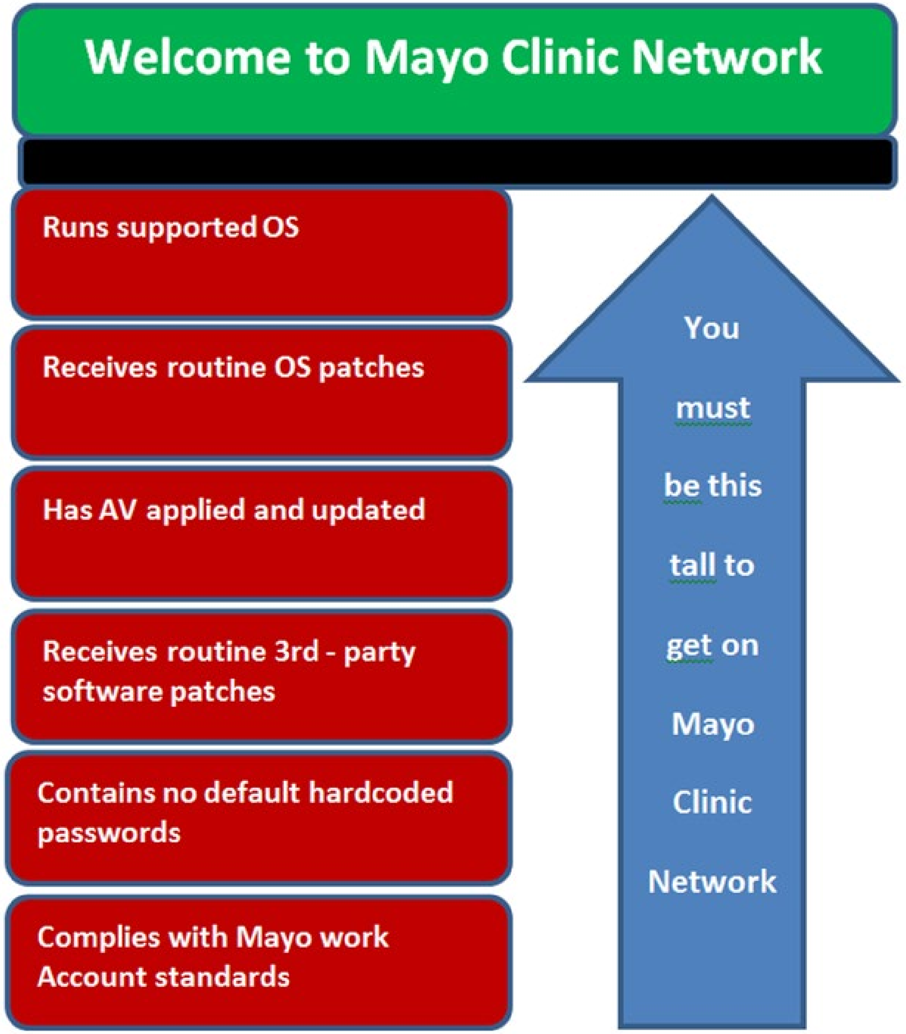
Reduce Risk through Proactive Actions

1. Set security standard
2. Set minimum security requirements
3. Evaluate new purchases, implement across fleet
4. Implement governance process for risk
5. Develop procurement and contract security requirements
6. Require remediation and mitigation actions
7. Develop communication plan
8. Expect compliance with FDA guidance
9. Document non-compliance with internal policies/standards (represents risk)
10. Align policies and procedures with standards as security evolves

Embed security up front in decision-making processes

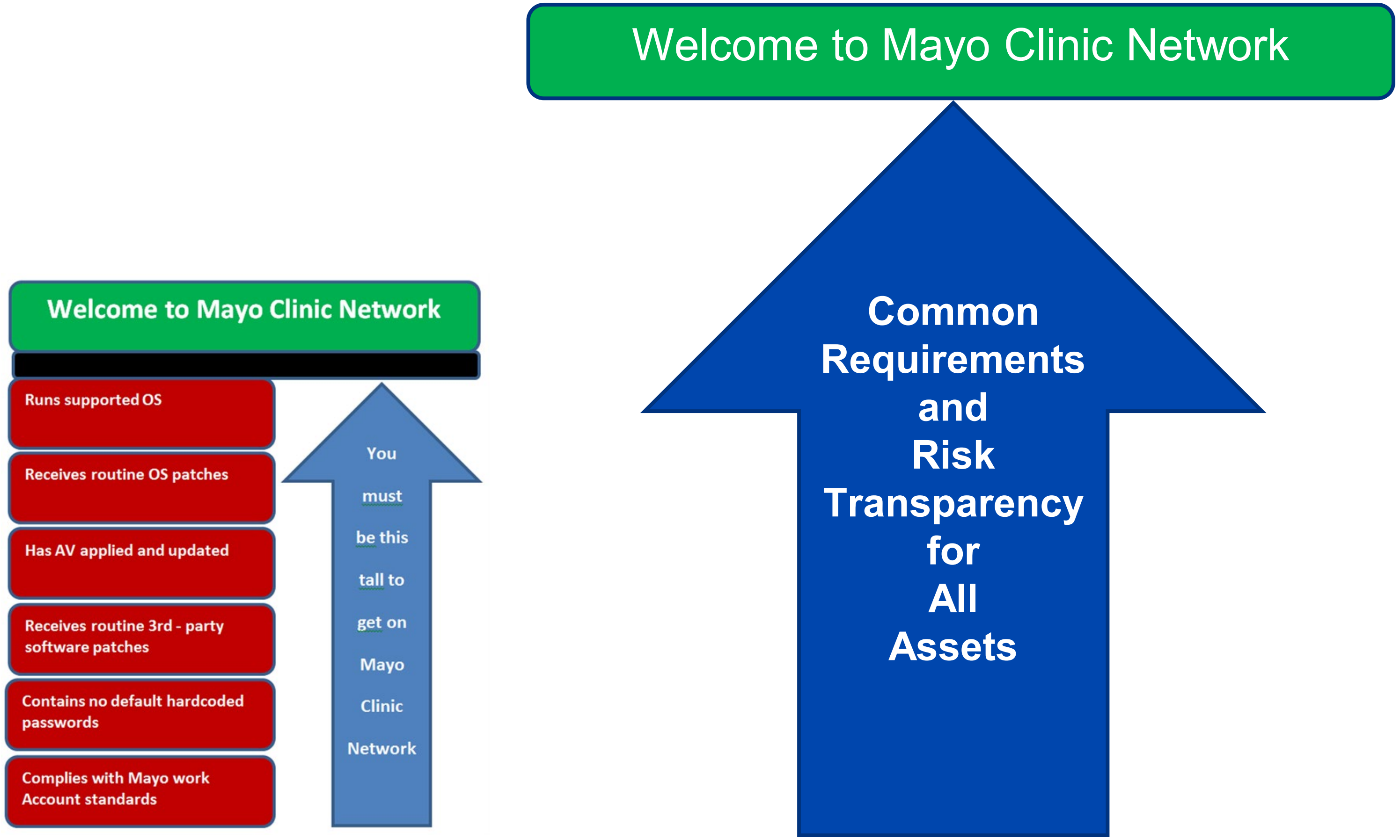
MAYO CLINIC

Established Minimum Security Requirements – Medical Devices



©2014 MFMER |

Transitioning to Security Resilience Program



Threat actors do not intentionally avoid vulnerable medical devices

What does Security Resilience mean at Mayo Clinic?

Mayo Clinic is able to maintain safe patient care during targeted or unintended cyber events by applying proactive and reactive defenses.

Security Resilience Program Deliverables

- **Determine Baseline Security Resilience Requirements** (What is measured)
- **Establish and Implement Certification Program** (How it's measured)
- **Establish and Implement Validation Process for Certified Assets** (Measure drift over time)

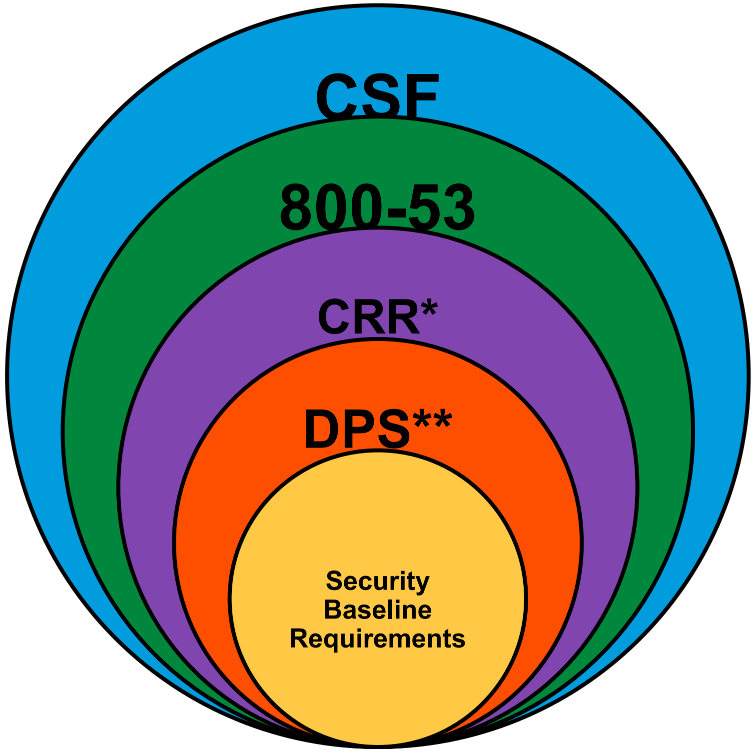
Security Resilience Approach

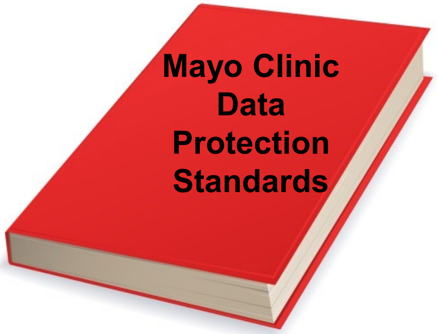
- Maintain a consistent set of baseline requirements across all asset groups
  (achieving baseline requirements results in policy/standard compliance)
- Identify tools and attributes to measure baseline security requirements
  (measured attributes may vary by asset group due to tool capabilities)
- Leverage consistent algorithm for the fleet risk score, when possible
- Leverage common monthly reporting templates, processes, and tools
- Integrate baseline requirements into the procurement process
  (ensures status of baseline requirements are known at time of purchase)

Goal: measure and communicate security risk throughout an asset's life

Defining Security Resilience Requirements

(What is measured)





MAYO CLINIC

Baseline Security Resilience Requirements
by Foundational Asset Type
(What is measured)

	System	System / Enterprise	Enterprise	Total
Workstation	19	2	12	33
Windows Server	18	2	12	32
*NIX Server	18	2	12	32
Med Device	19	2	11	32
IoT	19	2	11	32
Application	15	2	11	28
Network Hardware	19	2	11	32
Standard Accounts	11	1	8	20
Priv Accounts	11	1	8	20
Total	19	2	12	33

MAYO CLINIC

Focus on a single asset fleet to achieve incremental risk reduction

Baseline Security Resilience Requirements
System Level (20*)

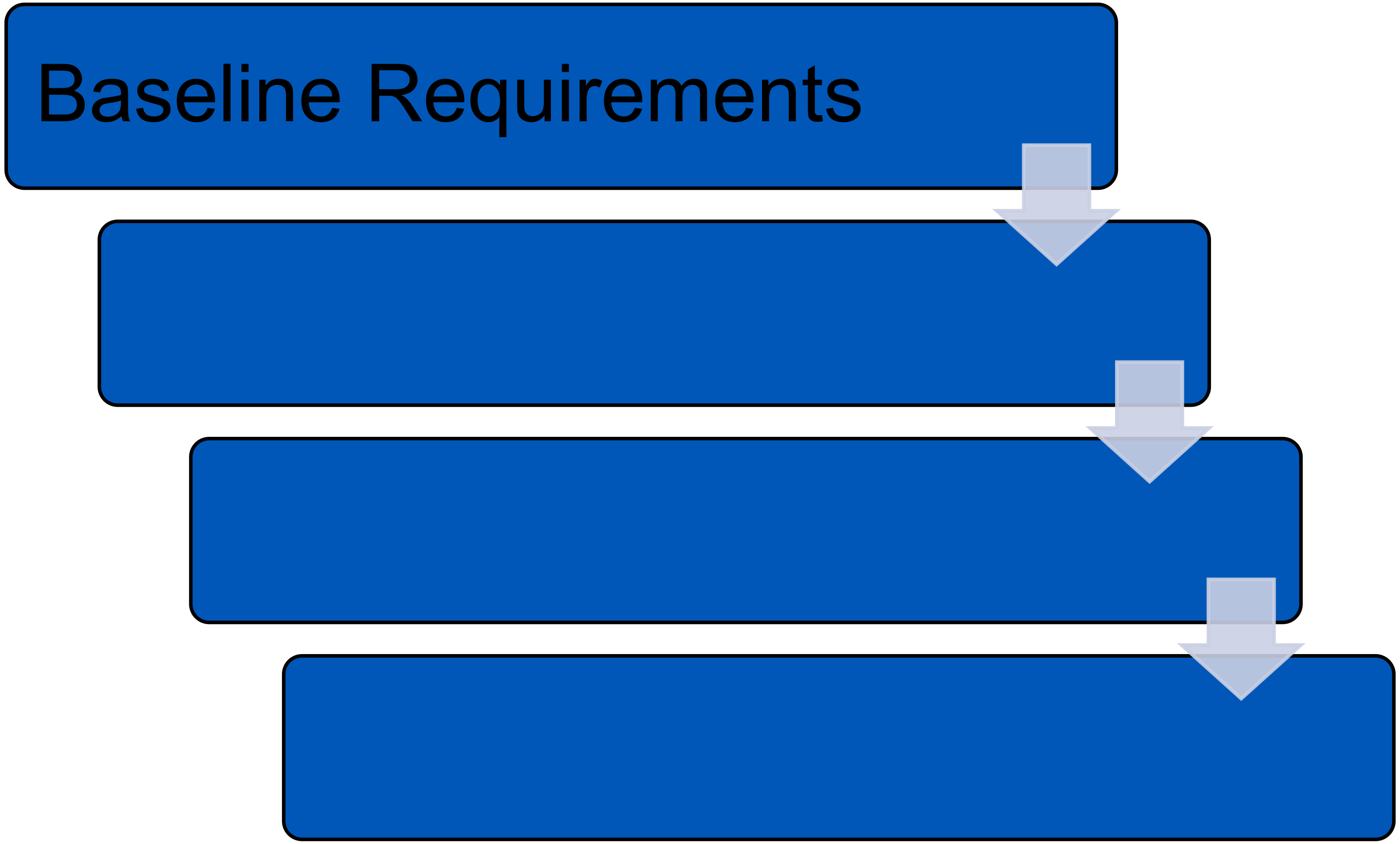
1. System Compliance with Remote Access Policy
2. Screen Timeout and Session Lockout Compliant with Policy and Standard
3. System Complies with IDMP Program
4. System Complies with Account Lockout Policy and Standard
5. Data Flows and External Connections Established and Maintained through Hardened Configuration Controls
6. System Compliance with Asset Management Policy and Standard
7. Installed Baseline Configuration and Change Processes Complies with Policy and Standard**
8. Business Continuity/Disaster Recovery Plan Established, Tested, and Maintained
9. Information Security Agreement Signed and Monitored for Compliance**
10. System Enrolled in Vulnerability Management Program

MAYO CLINIC

1. System Architecture (i.e. Enterprise Architecture Packet completed) Documented
2. Wireless Protections Established and Maintained

**** Duplicates Removed***
***** Enterprise/System Requirement***

Security Resilience Foundation



Security Resilience Risk:
(How it's measured)

- Identify measurement criteria and sources
- Leverage automation
  - Use empirical data
  - Minimize cost
- Define scoring methodology

Measuring Security Resilience Fleet Risk

Baseline Requirement	Attribute	Empirical	Score Range
Installed Baseline Configuration and Change Processes Complies with Policy and Standard	OS Version Supported	Yes	0 to 20 (refining)
Installed Baseline Configuration and Change Processes Complies with Policy and Standard	SMB Version	Evaluating	
Anti-Malware Complies with Policy and Standards	Anti-malware Enabled	Yes	
System Complies with Asset Management Policy and Standard	Managed by Mayo or Vendor	No	
Data at rest is encrpted	Encryption Applied	Evaluating	
Wireless Protections Established and Maintained	Wi-Fi Capability Exists	No	
Wireless Protections Established and Maintained	Wi-Fi Enabled	Yes	
Wireless Protections Established and Maintained	Bluetooth Capability Exists	No	
Asset is apporpriately segmented	SGT	Yes	
RDP Traffic uses Enterprise Resources	Validated through Gateway	Yes	
Patient Harm (risk factor)	Criticality (Direct Patient Harm)	No	
Data Type (risk factor)	PHI Exists on Asset	Yes	
FDA Class (risk factor)	FDA Class	Yes	
Additional Attributes starting in 2023	* Remote Support Tool * Scanning Agent Installed * TBD	Yes	

MAYO CLINIC

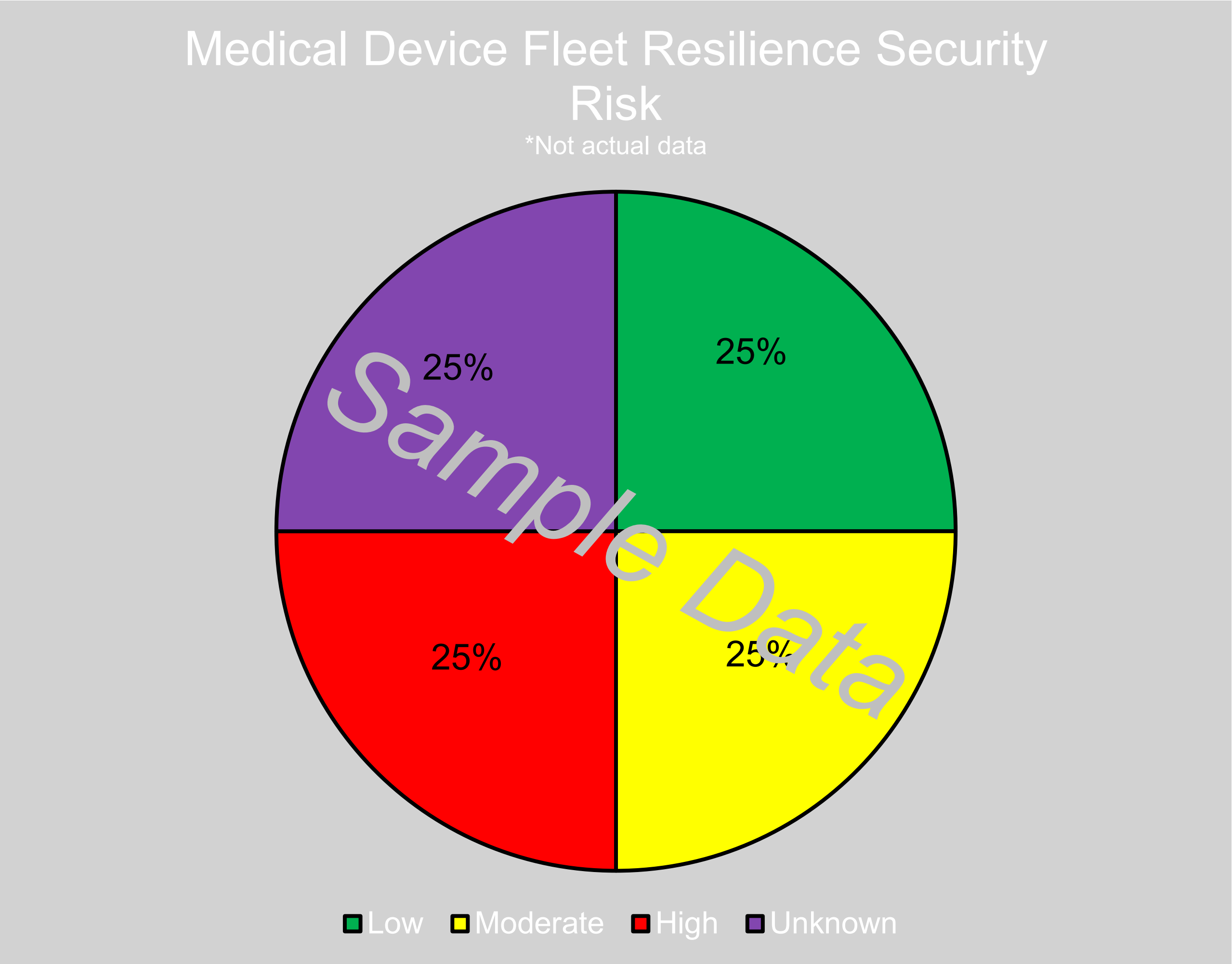
Seek empirical measurement, but not always possible

Attributes by Fleet

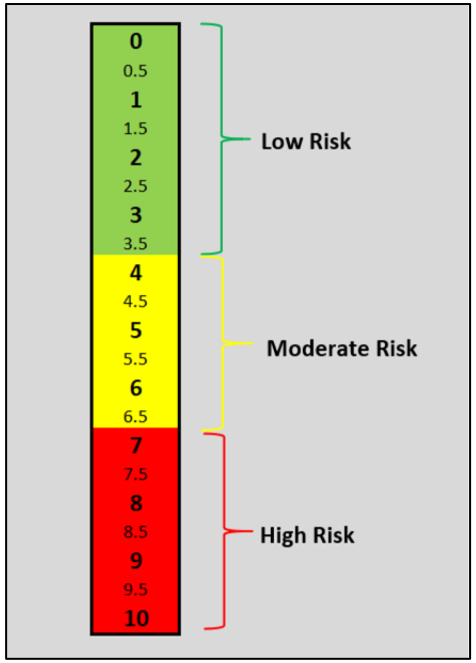
Asset Fleet	Attributes Measured
Workstations	21
Windows Server	12
Medical Devices	10

Available tools impact what can be measured

SECURITY RESILIENCE RISK ALGORITHM
(HOW IT'S MEASURED & MEASURE DRIFT OVER TIME)

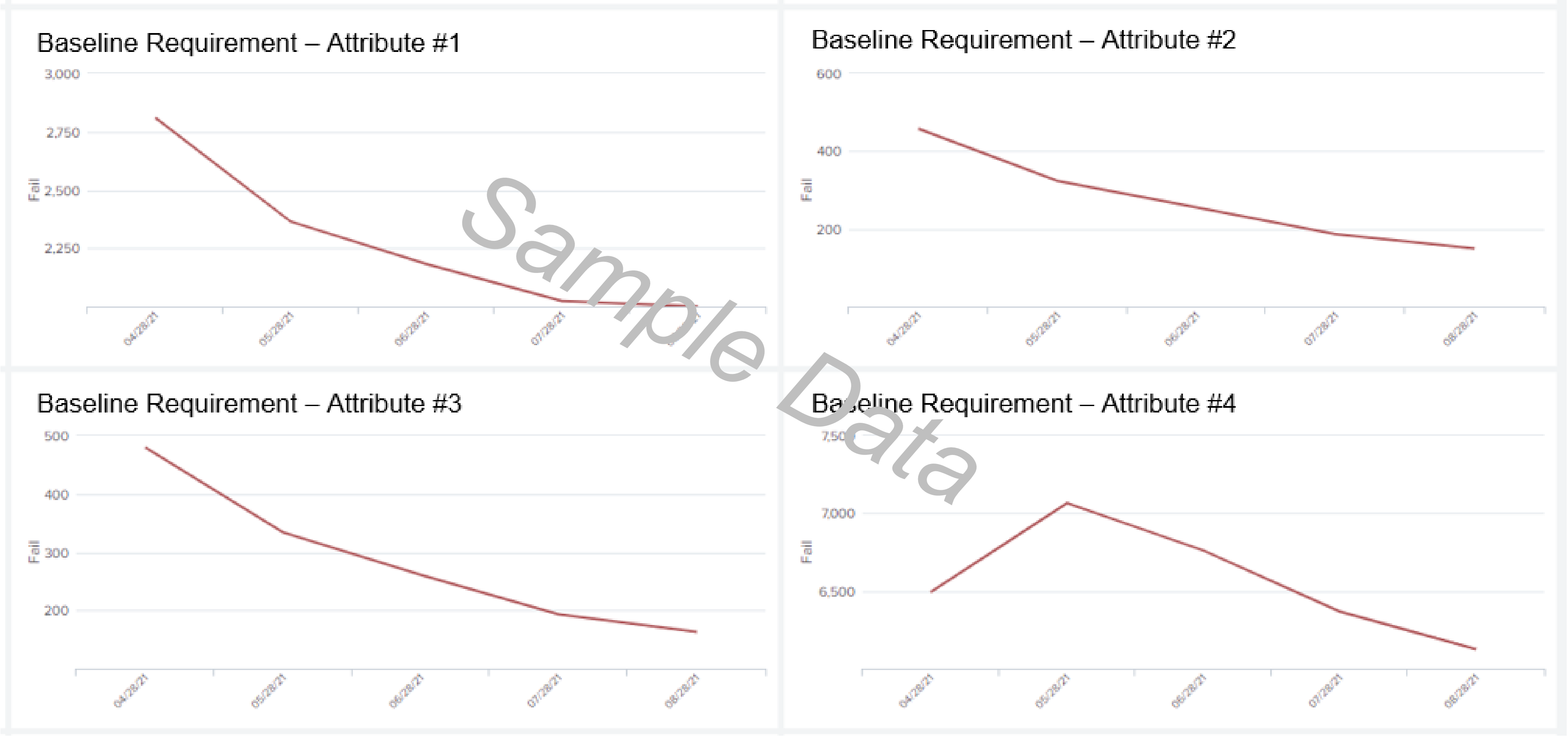


- ***Calculated***
  - Data attributes are captured for each asset
  - Score supported by defined attributes and logic to show trending and details at the asset and fleet level (enables action)
- ***Algorithm Scoring Range***
  - 0 (low risk) to 10 (high risk)
  - Aligns with other security risk scoring used at Mayo Clinic
- ***Report Monthly***
  - Measure point in time
  - Measure trend
  - Validate asset drift



©2022 Mayo Foundation for Medical Education and Research

Monthly Validation
Asset Fleet - Leverage Automation
(Measure drift over time)



Create fleet level reports to identify process gaps

Monthly Validation
Asset Fleet - Leverage Automation
(Measure drift over time)

Date	Host Name	MAC Address	Asset Owner	Risk Score	Remote Suport Tool	Pass/Fail	Attribute #2	Pass/Fail
DDMMYYYY 00:00:00	XXXXXXXXX	XX:XX:XX:XX:XX:XX	John Doe	HIGH	Non-Standard Remote Support Tool	Fail	XXX	Fail
DDMMYYYY 00:00:00	XXXXXXXXX	XX:XX:XX:XX:XX:XX	John Doe	LOW	No Remote Support Tool	Pass	YYY	Pass
DDMMYYYY 00:00:00	XXXXXXXXX	XX:XX:XX:XX:XX:XX	John Doe	LOW	Non-Standard Remote Support Tool	Fail	XXX	Fail
DDMMYYYY 00:00:00	XXXXXXXXX	XX:XX:XX:XX:XX:XX	John Doe	MODERATE	No Remote Support Tool	Pass	XXX	Fail
DDMMYYYY 00:00:00	XXXXXXXXX	XX:XX:XX:XX:XX:XX	John Doe	HIGH	Non-Standard Remote Support Tool	Fail	YYY	Pass
DDMMYYYY 00:00:00	XXXXXXXXX	XX:XX:XX:XX:XX:XX	John Doe	HIGH	No Remote Support Tool	Pass	XXX	Fail
DDMMYYYY 00:00:00	XXXXXXXXX	XX:XX:XX:XX:XX:XX	John Doe	MODERATE	Mayo Standard Remote Support Tool	Pass	XXX	Fail
DDMMYYYY 00:00:00	XXXXXXXXX	XX:XX:XX:XX:XX:XX	John Doe	LOW	No Remote Support Tool	Pass	YYY	Pass
DDMMYYYY 00:00:00	XXXXXXXXX	XX:XX:XX:XX:XX:XX	John Doe	HIGH	Non-Standard Remote Support Tool	Fail	XXX	Fail
DDMMYYYY 00:00:00	XXXXXXXXX	XX:XX:XX:XX:XX:XX	John Doe	HIGH	No Remote Support Tool	Pass	XXX	Fail

Actionable data is needed to enable risk reduction

Patient safety and security is a shared responsibility requiring ***collaboration*** *across and within organization*

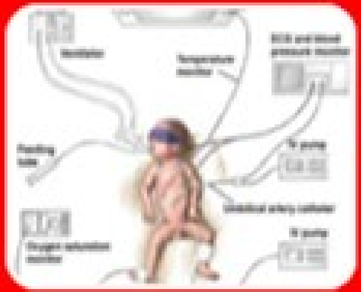
©2014 MFMER

Expand Thinking from Asset to Clinical Workflow

- ***Hold all network connected assets to same standard***
  - Communicate standards to those purchasing assets
  - Assess all assets against the same standards
  - Track and report risk, identified solution, and timeline to resolve
- ***Engage all organizational stakeholders***
  - Technical resources (Information Technology, Information Security, HTM)
  - End user (Physicians, Nurses, Lab Techs, Administrative Support)
  - Procurement resources (Supply Chain Management, Contract Management)
- ***Build upon current collaboration***
  - Manufacturers, Healthcare Providers, Government
  - Cross industry vertical
  - Security tool manufacturers
  - Globally

MAYO CLINIC

The Vision: Program Priorities



Patient Safety

- Shield workflow assets necessary to sustain life during a cyber event

Workflow Continuity

- Maintain availability of workflow assets supporting ongoing patient care during a cyber event

Data Integrity & Availabilty

- Protect the integrity & availabilty of data on patient-critical assets during a cyber event

Key Take-Aways:

1. Define baseline security requirements
   - Industry standards
   - Organizational threats
2. Support requirements with
   - Organizational policies and standards
   - Map relationship (industry standard, policy, requirement, attribute, score)
3. Leverage automation to measure
   - Empirical data (identify drift)
   - Minimize cost (scalable)
4. Use a transparent risk algorithm
   - Measurable attributes
   - Numeric score
   - Actionable data to reduce risk
5. Measure and report risk
   - Asset owners
   - Risk governance

MAYO CLINIC

Thank You

bruemmer.debra@mayo.edu