crico | Protecting Providers. Promoting Safety.

CASUALTY ACTUARIAL SOCIETY

MPL Issues & Trends for 2014 and Beyond

Ratemaking and Product Management (RPM) Seminar – March 30 – April 1, 2014

Arvind P. Kumar, FHIMSS, Sr. VP Technology & Alliances
CRICO

crico

Who We Are

CRICO

- Controlled Risk Insurance Co.
- Premium: $150M for $5M coverage
- Insure:
  - 12,400 physicians (including over 4,000 residents and fellows)
  - 32 hospitals
  - 100,000+ employees (Nurses, technicians, etc.)

CRICO STRATEGIES

- A division of CRICO
- Strategic risk intelligence solutions and national community of learning
- Partners:
  - 125,000 physicians
  - 550 hospitals
    - University systems
    - Physician insurers
    - Captive insurers

crico

Our Community

Representative members of our data and/or community of learning

Comparative Data
Community of Peers

CRICO

- Partners HealthCare System
- Care Group
- Children's Hospital Boston
- Dana-Farber Cancer Institute
- Harvard Vanguard Medical Assoc.
- Massachusetts Eye and Ear Infirmary
- Cambridge Health Alliance
- Presidents & Fellows of Harvard College
- Joslin Diabetes Center
- Judge Baker Children's Center
- Massachusetts Institute of Technology

PRODUCTS & SERVICES

CRICO STRATEGIES

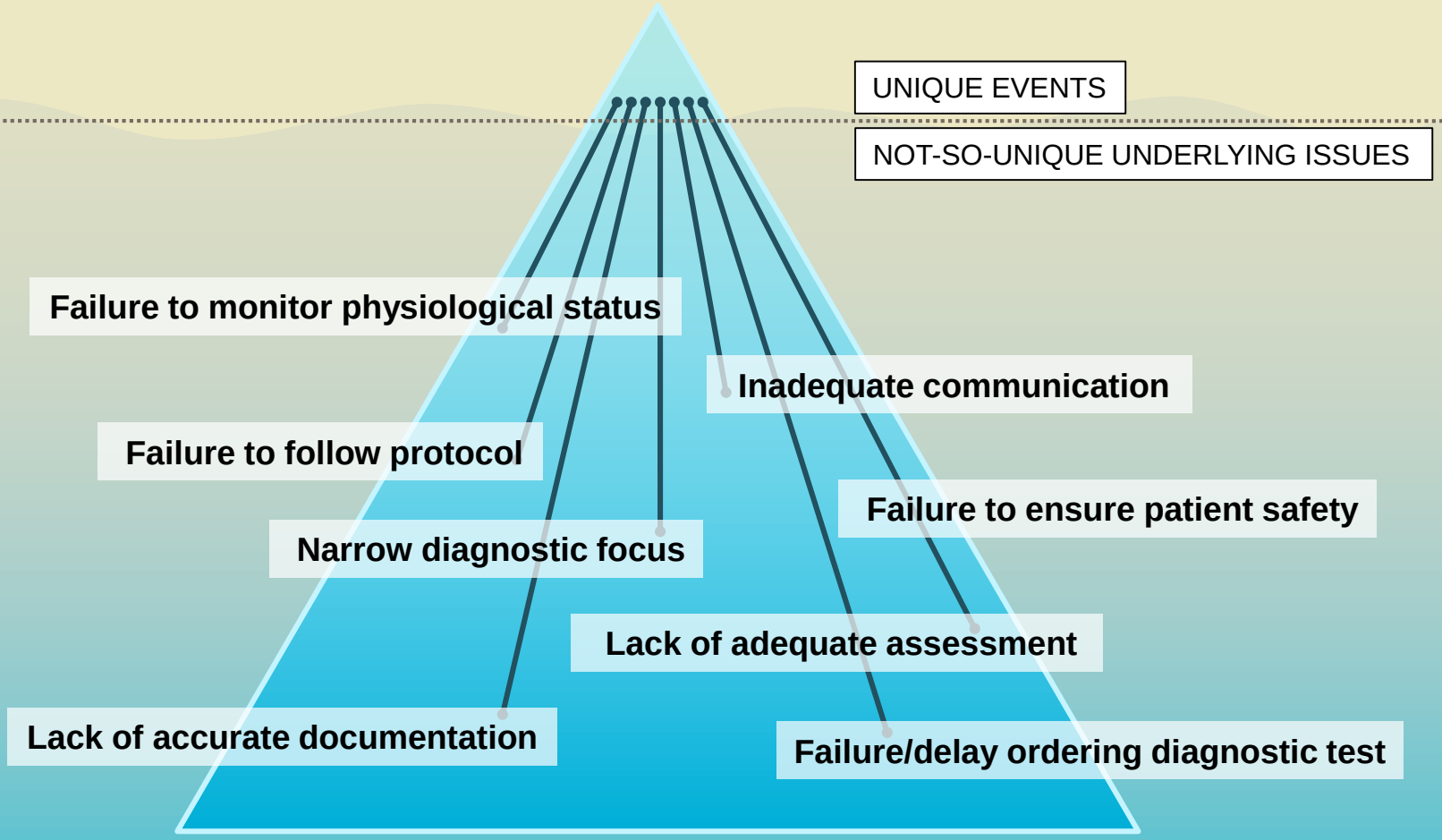
- Stanford University
- Temple University Health System
- Maine Medical Center
- PHTS
- University of Florida
- University of Maryland
- MedStar Health
- Cassatt
- Princeton Insurance Company
- The Doctors Company
- Medical Protective
- MMIC

Mission

CRICO's mission is to provide a superior medical malpractice insurance program to our members, and to assist them in delivering the safest healthcare in the world.

crico

Claims are a unique convergence of events that arise from not-so-unique contributing factors.



crico

Transforming Events into Data

Import Client Claims → **Apply Clinical Coding** → **Produce Data Analysis** → **Prioritize Interventions**

- Adverse Events: RCA
- Claim Files
- Medical Records

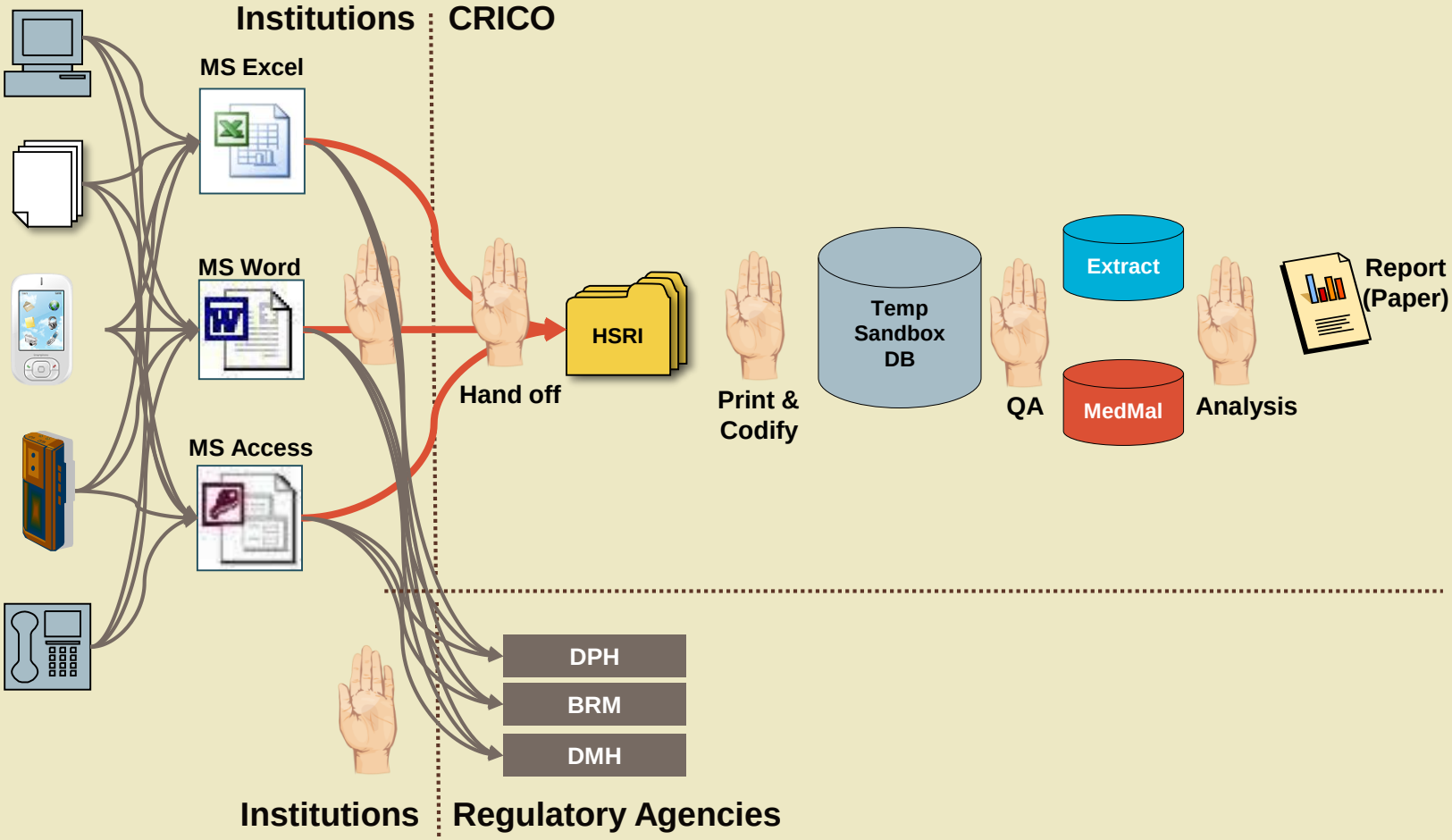
- Reports & Trends

Adverse Events: Root Cause Analysis

crico

Root Cause Analyses Submission Process

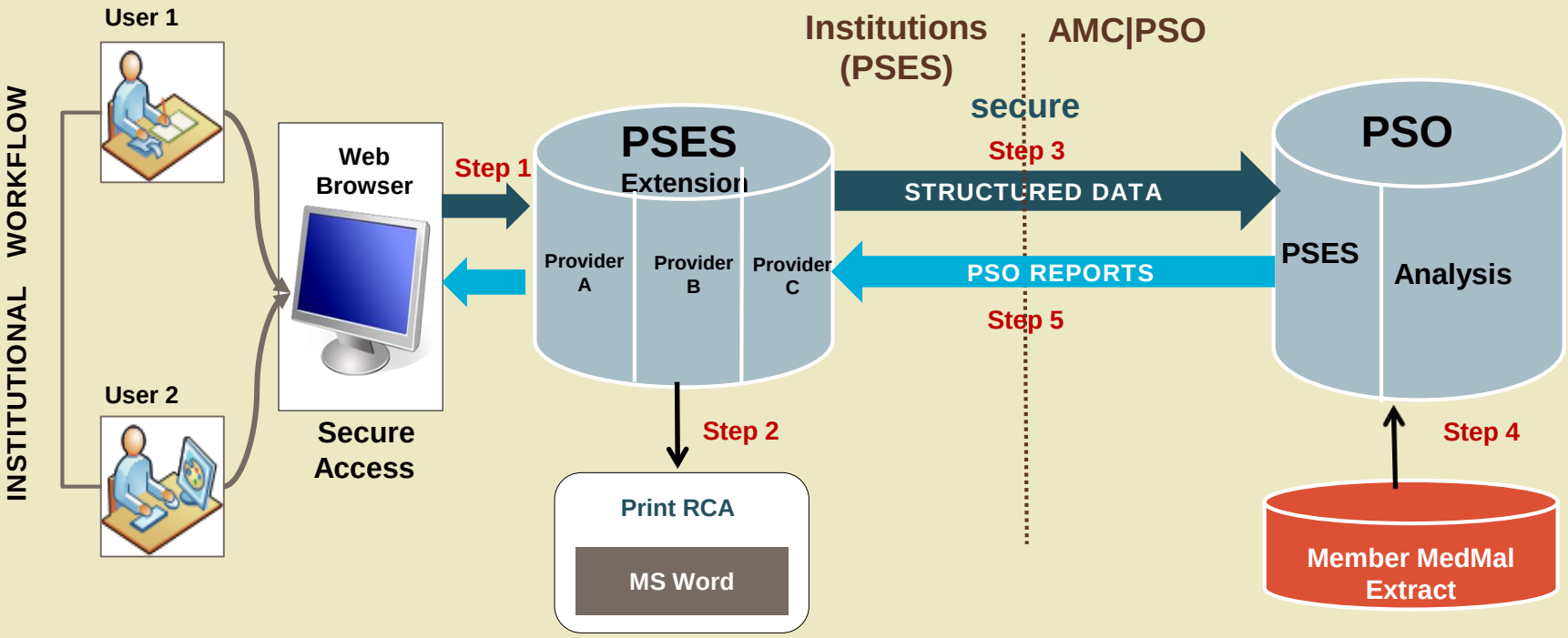
Current State: A manual process requiring 4–6 weeks



crico

Root Cause Analyses Intelligence Exchange

Technology-enabled process, **almost** real time



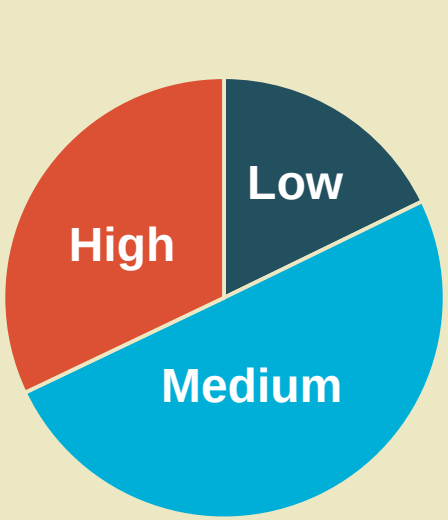
Initial Results

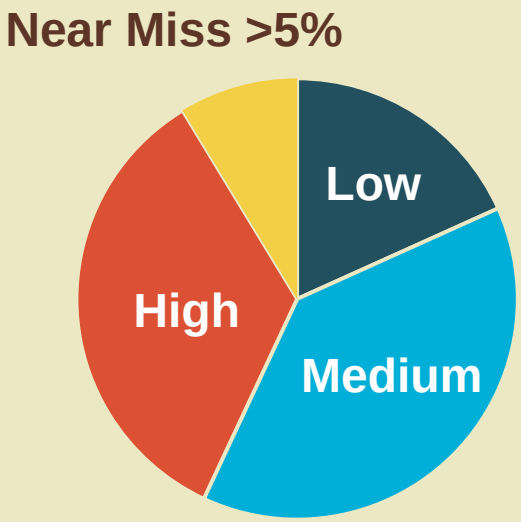
crico

SAMPLE:
Injury Severity

>5% of RCAs capture “near misses”

CLAIMS	RCAs





Severity Scale: High=Death, Permanent Grave, Permanent Major, or Permanent Significant
Medium=Permanent Minor, Temporary Major, or Temporary Minor
Low= Temporary Insignificant, Emotional Only, or Legal Issue Only

crico

SAMPLE:
Top 5 Primary Responsible Services

Rank order varies between claims and RCAs.

CLAIMS	RCAs
1. Medicine	1. Surgery
2. Surgery	2. Nursing
3. Nursing	3. Medicine
4. OB/Gyn	4. OB/Gyn
5. Orthopedics	5. Emergency

crico

SAMPLE:
Top 5 Event Types

Rank order varies between claims and RCAs.

CLAIMS	RCAs
1. Surgery	1. Surgery
2. Medical Treatment	2. Safety & Security
3. Diagnosis	3. Medication
4. Medication	4. Medical Treatment
5. Safety & Security	5. Patient Monitoring

crico

RCA Surgery Event Subtypes

Retained Foreign Objects Most Frequent

RCA Surgery Event Subtypes
1. Retained foreign body, surgical
2. Wrong-site surgery or other invasive procedure
3. Issues with management of surgical patient
4. Issues with performance of surgery/procedure

Malpractice Data: Retained Foreign Object	
% cases closed with payment	55%
Average indemnity payment	$75k

crico

VA National Center for Patient Safety: Hierarchy of Action Scale

STRONGER	INTERMEDIATE	WEAKER
Architectural / Physical Plant Changes	Adding double-check to process as a non-independent re-examination	Additional Study / Analysis
Engineering Change or added control to a medical device (ex. software or hardware)	Checklist / cognitive aid	Double checks
New Device – add new, additional or replacement devices	Eliminate / reduce distractions	New or clarified procedure or policy
Simplify / Streamline process and remove unnecessary steps	Enhanced Documentation / communication	Training
Standardization of equipment or process including a method to ensure compliance (beyond written policy)	Establish / perform quality control checks	Warnings and labels
Tangible involvement and action by leadership in support of patient safety	Increase in staffing / decrease in workload	
	Modifications or software / hardware enhancements to non-medical devices	
	Read back	
	Reduce Similarities, eliminate look and sound alike	
	Redundancy – duplicate critical components or functions	

Action Steps

- Identify a non-uniform pattern of action steps
- Opportunity to encourage through sharing and shift to stronger action steps

Cyber Security

crico

Our overarching goal is to enhance cyber security at all insured organizations

DRIVERS FOR IMPROVED SECURITY

- **Information Integrity for Patient Care and Safety**
- **Exponential Vulnerability and Risk Growth**
- **Optimize Return on Investments**

CYBER SECURITY OBJECTIVES

- Foster and promote a culture of information
- Build mutual trust and momentum addressing cyber security risks
- Develop a common view of security best practices
- Test and learn from security efforts
- Create a mechanism to effectively communicate and ensure transparency and with key stakeholders (e.g., CRICO Board, business executives, CIOs, etc.)
- Facilitate analysis, research, and presentations on cyber security topics
- Eliminate duplication of effort, reduce time to implementation, manage resources, and drive focus

crico

CRICO Cyber Insurance Vision & Roadmap?

Phase 1
Capability Piloting

Establish Cyber Security Working Group

#1 Beacon Toolkit
#2 Beacon Toolkit
#3 Beacon Toolkit
NAC

Conduct Ongoing Policy Analysis

Create Awareness Communications

Pilot Managed Services

Objectives

- Quick wins
- Build trust
- Member-driven agenda
- Refine approach

Now

Phase 2
Capability Building & Refinement

Cyber Security Working Group

Beacon Toolkit
Beacon Toolkit
Beacon Toolkit
ENAC

Beacon Toolkit
Beacon Toolkit
Beacon Toolkit
End Point

Policy Development

Awareness & Training

Threat Intelligence

…

Vulnerability Assessments

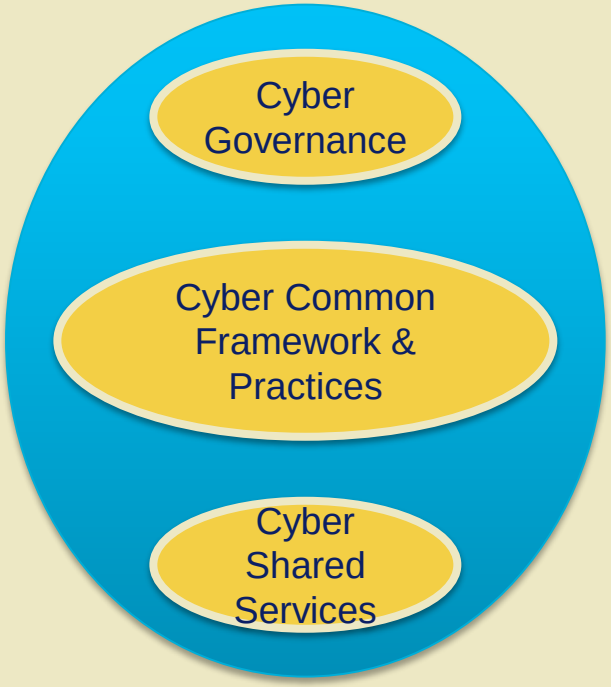
Penetration Testing

…

Objectives

- Reduce external support to SME only (if needed) – greater allocation of funding to Beacons
- Larger scope, harder problems
- CRICO-driven project agenda
- Prioritized/sequence towards vision state

Vision
CRICO Cyber Insurance Offering



Objectives

- Shared vision/strategy/policy
- Common core cybersecurity
- Readily insurable institutions
- Continual partnership, sharing and improvement

crico

In phase 1 we launched three work streams under a CSW Partnership for collaboration, sharing and creating momentum

Cyber Security Working Partnership (CSW)

- Monthly meeting with CISO's; formed Steering Group
- Involves Children's, BIDMC, Atrius & Partners
- Encourages sharing of ideas and lessons learned

1

Conducted High-Level Policy Analysis (Four Policies)

- Mobility BYOD & Unmanaged Devices
- Information Protection Social Media
- Identity Access Management (Two-Factor Authentication)
- Identity Access Management (Remote Access

2

Executing Network Access Control Beacon (Capability Demonstrations)

- Involves Children's, BIDMC, Atrius and Partners
- Phases include vendor selection, pilot testing of 200 users and development of a lessons learned playbook

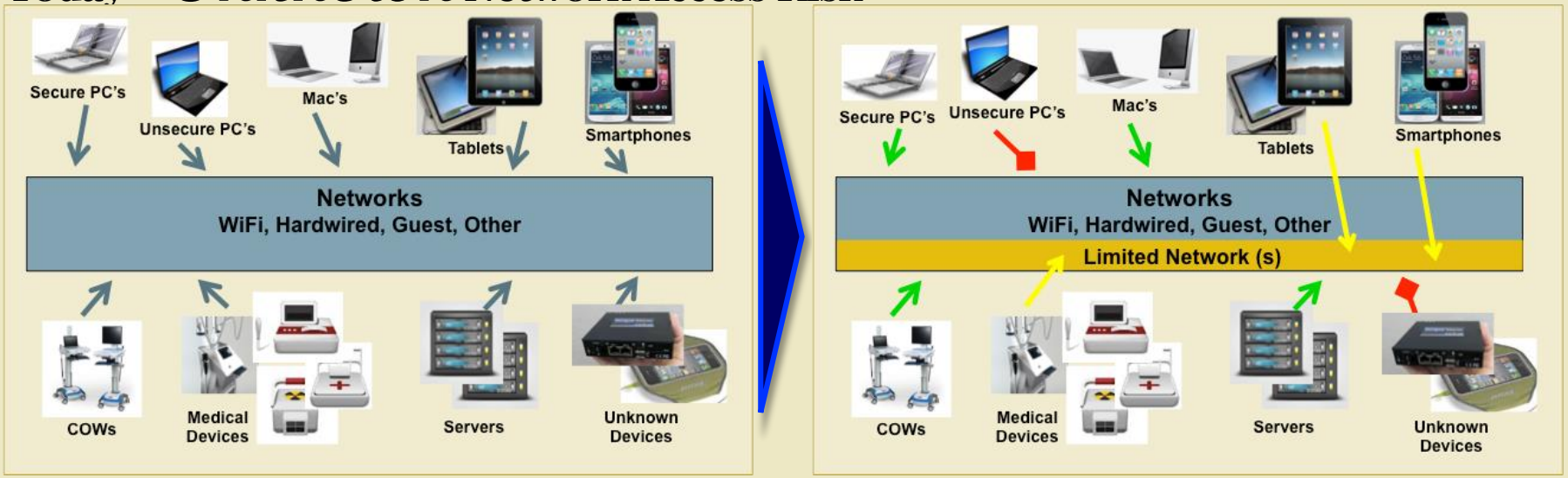
3

Executing Assessment Services Beacon (Capability Demonstrations)

- Involves Children's and Atrius
- Phases include vendor selection, penetration pilot testing and development of a lessons learned playbook

crico Measuring NAC Success in March 2014

Today – *Unknown* Network Access Risk ➢ ***Managed* Network Access Risk**



Before NAC	Risk Area	Patient Health & Safety Impact	After NAC
🔴	**Unknown Devices connecting to Network**	Reduced exposure from uncontrolled devices	🟢
🟡	**Insecure Devices connecting to network**	Devices must meet information security policies before connecting	🟡
🔴	**Medical Devices competing for network resources**	Medical device network access prioritized and monitored	🟡
🔴	**Smartphones & Tablets accessing Patient Records**	Only known users/devices gain access to protected systems	🟢
🟡	**Compliance**	Extra security layer improves compliance with HIPAA and other regulations to protect patient information.	🟢

crico

Measuring AS Success in March

Before

- Limited Testing
- Limited Test Protocol
- Testing not validated with compliance requirements
- Pricing limits testing schedule and capability

Assessment Services

Systems Improvements

After

- Prioritized and Consistent Testing
- Testing aligned to compliance requirements
- Threat-based use case testing (e.g., insider)
- Evergreen pricing

Before AS	Risk	Health & Safety Impact	After AS
	**Confidentiality & Integrity of Information on Internal-facing systems**	Information on internally facing systems protected consistently	
	**System compliance not fully verified**	Improved compliance with HIPAA and other regulations to protect patient information	
	**Security awareness and focus not maintained**	External systems are tested on a regular basis to ensure defensive measures meet current threat environment	
	**Unknown, external, Attack Surface includes unknown/forgotten servers**	Rogue and forgotten servers are identified and remediated, ensuring consistent protection of stored data,	
	**External systems allow unauthorized access internal systems, or environmental controls and physical plant.**	Improved protection from outside attacks that could: • access internal networks that expose patient records • Impact power and HVAC that protect safe, comfortable working environment	
	**External systems gain unauthorized access through exposed server allowing hacker access to compromise medical devices.**	External servers prevent attacker access to internal networks and prevent compromise of medical devices.	

crico

Our phase 2 proposal expands capabilities while continuing to build trust and value among stakeholders

Proposed Beacon	Expected Outcomes/Benefits
1 **Expand NAC (ENAC)**	◆ Increased diversity of devices and users monitored ◆ Increased management and tool usage ◆ Data drives transition to policy development
2 **Endpoint Security Migration**	◆ Implemented policy rules and controls to reduce risk ◆ Better protected information storage and transport ◆ Secured PHI/PII on personal and corporate devices
3 **Information Security Policy (ISP)**	◆ Common guidelines based on HIPAA requirements and industry risk management practices ◆ Content Easily customizable to stakeholder organizations
4 **Threat Risk Analysis**	◆ External view of threat and risk environment ◆ External threat mapped to internal controls to reduce risk ◆ Increased predictive risk management ability
Continued CSW Partnership	◆ Increased partnership benefits, ◆ Reduced brand and reputation risk, ◆ Readiness for cyber insurance

Action Steps – Strength by Institution

Count by Actions Steps

Institution	Stronger	Intermediate	Weaker	None
A	5.7%	22.9%	70.2%	1.2%
B	20.5%	28.8%	48.4%	2.3%
C	10.8%	18.3%	69.0%	1.9%
D	20.6%	8.8%	70.6%	0.0%
E	50.0%	50.0%	0.0%	0.0%
Grand Total	**12.9%**	**21.9%**	**63.6%**	**1.6%**

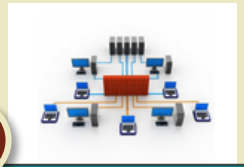
crico

NAC Beacon Project Discussion

Project Area	
1 Major challenges/issues with implementing NAC	• Ensuring Business alignment with management, IT and end user community • Defining specific goals that are supportable by IT • Insuring that the Infrastructure capabilities and scalability exist to support NAC deployment • Understanding security vs. productivity trade-off and impact to patient care • Lack of knowledgeable Staff to implement and maintain NAC resulting in Poor end-user experience • Integration with existing Infrastructure equipment & Software (e.g. Switches, Antivirus software, etc.) • Integration of Continuous Assessment and Remediation for multiple platforms
2 Major security choices need to be made	• What Devices and Operating Systems will be supported • Segregating devices by VLANs based on Policy-driving Attributes; Who – user/owner, What – endpoint type, Where – endpoint location, How – behavior • Identifying End-Point Security Assessment tools that supports all of the end-point devices in use • Selecting a NAC vendor with the capability of being integrated with Mobile Device Management system
3 Success Measures	• Implement a network access control (NAC) solution to ensure only authorized users and devices are connected to the network across all sites • Ensure all corporate endpoints are configured properly and have the necessary patches and software versions. • Eliminate usage of non-compliant software on all end points. • Achieve compliance with the industry best practices

crico

Phased Network Access Control Implementation



1 Assess Infrastructure Capabilities

The enterprise will need to consider Infrastructure capabilities:

- Switch support for VLAN's
- Support for 802.1X
- Wireless AP Capabilities
- Infrastructure scalability
- Enterprise Policy, Authentication and Environment end-point security (Posture Assessment)

2 Define NAC Scope

The enterprise will need to consider:

- Type of devices to be managed
- User roles and associated Policies
- Endpoint Compliance Validation requirements
- Locations to be managed
- Closely examine security vs. productivity trade-offs
- Policy-driving Attributes
- Which vendor meets requirements?

3 NAC Installation and Phase 1 Piloting

Considerations:

- Location of NAC (Local / Remote)
- Number of NAC systems
- ~ 200 users to start pilot with various types of users (Doctors, Nursing Staff, etc.) to be defined
- Appliances to be included (Printers, VoIP, etc.) in the pilot
- Define an enforceable policy that will have minimal impact to patient care
- Wireless devices
- Remote Access
- Staffing to support NAC

4 Phase 2 Single Facility Expanded NACRollout

The enterprise will need to consider:

- Review impact to user community by department and user type
- Expansion to ~10,000 users
- Monitor infrastructure components for utilization impact (e.g. Authentication servers, Switches, Wireless AP)
- Assess User Experience as rollout progresses
- Validate policy impact to user community

5 Phase 2 Multi-Facility Expanded NAC rollout

The enterprise will need to consider:

- Review performance requirements for centralized or decentralized NAC systems
- Validate user experience by department during rollout
- Monitor infrastructure components for utilization impact (e.g. Authentication servers, Switches, Wireless AP)

Complexity

Implementation

- Conduct initial assessment and develop requirements
- Define security requirements and incorporate into solution
- Review impact of NAC and Policy enforcement on the User community
- Review reports to validate the capture of all devices and their status
- Monitor incremental device acquisition against performance of infrastructure

crico

Future Security Research Topics and Best Practices Vignettes

Vignette Topics	Wants to Present	Wants to Hear About
Project Lighthouse	Partners	All
TBD Security Effort	Atrius	All
Third Party Contracts	Partners	All
Penetration Testing		
MDM Deployment		
EPIC Security Model		
WiFi Capacity and Security Management		
Security Strategy and/or Multi-year Plans		
….		

Security Research Topics	Who ?
Cloud Broker Services	All
Security Event Management Tools/Services	All
Emerging Threat/Risk Discussion	All
Next Generation Desktop Security	All
Assessment of threat/risk across CRICO institutions	
Outsourced SIEM tools and services	
Maturity model and security program assessment	
Information security policy checklist (audit)	
Incident response services	
Security staff hiring, retention, training	
….	