Health IT Security User Education Roundtable:

A Best Practices Symposium

MHCC | MARYLAND HEALTH CARE COMMISSION

HSCRC Health Services Cost Review Commission

HIMSS MARYLAND Chapter

Maryland Hospital Association

WELCOME

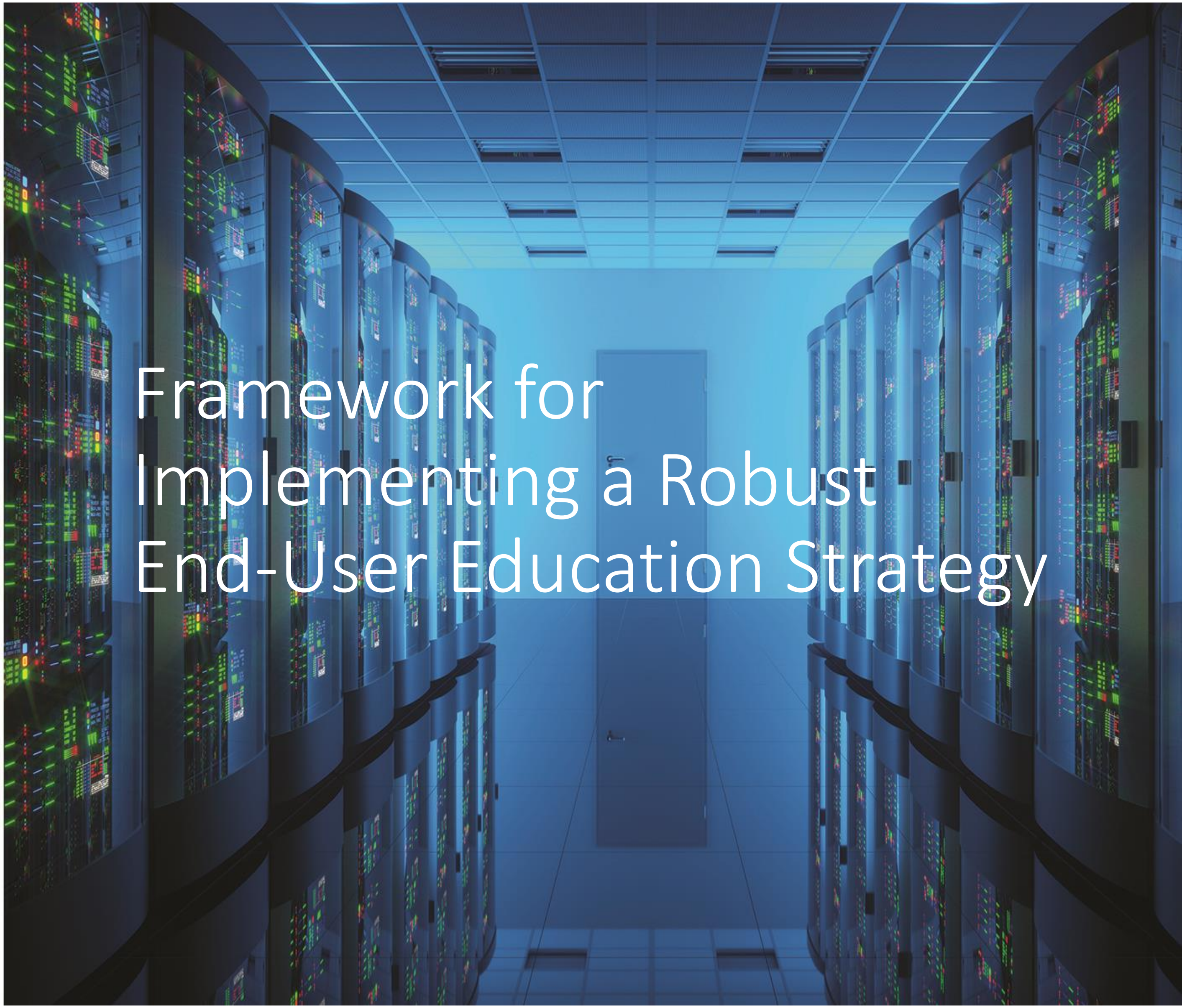
Ben Steffen – Executive Director, Maryland Health Care Commission

A Framework for Implementing a Robust End-User Education Strategy to Reduce Risk and Improve Cybersecurity Posture

Toby Gouker, PhD – Vice President of Strategy,
First Health Advisory – Cybersecurity and Health IT Solutions

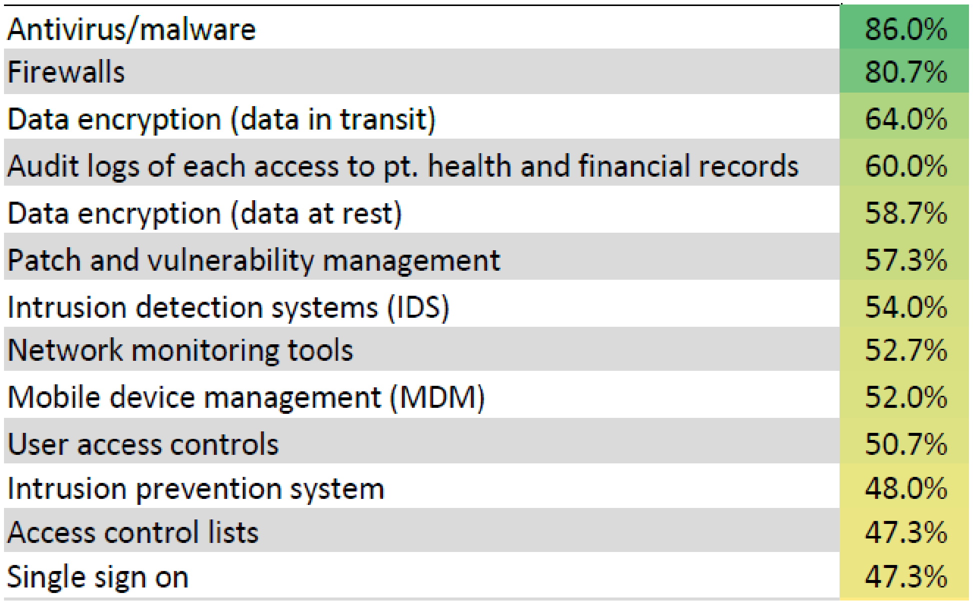
First

Cyber
Health
Solutions



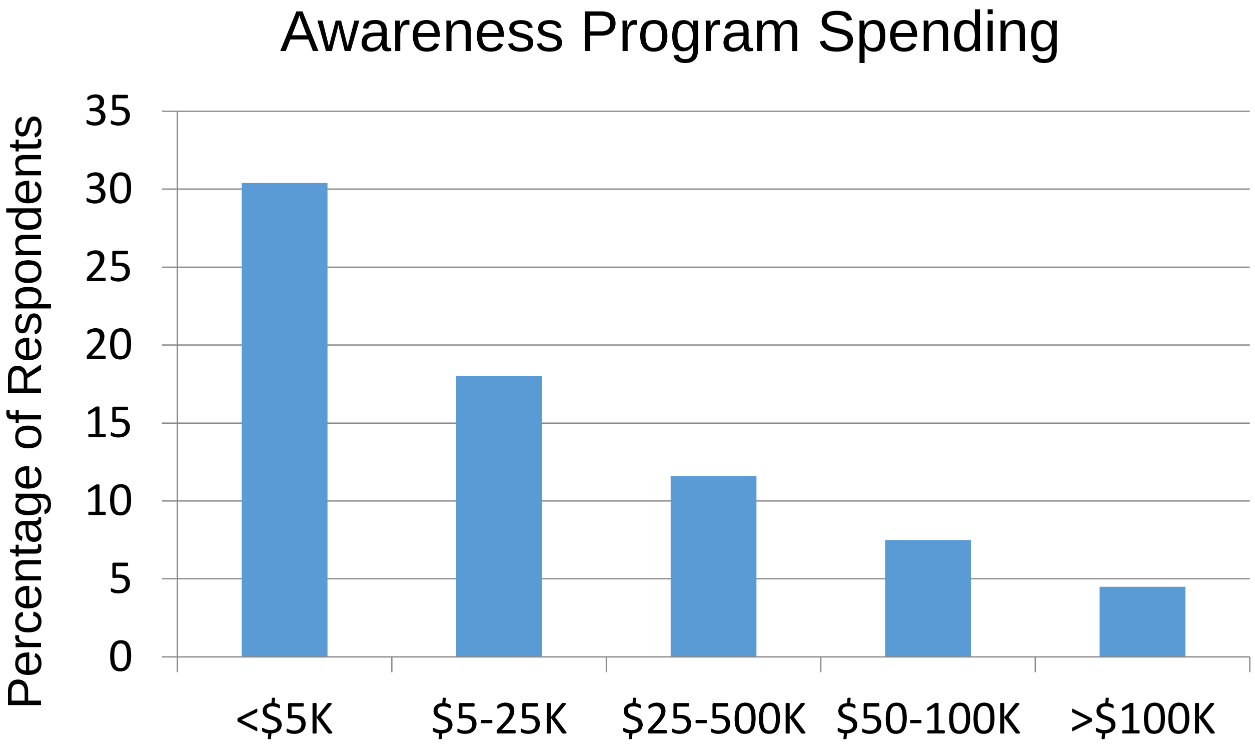
Framework for Implementing a Robust End-User Education Strategy

Security Tools Implemented by Healthcare Providers

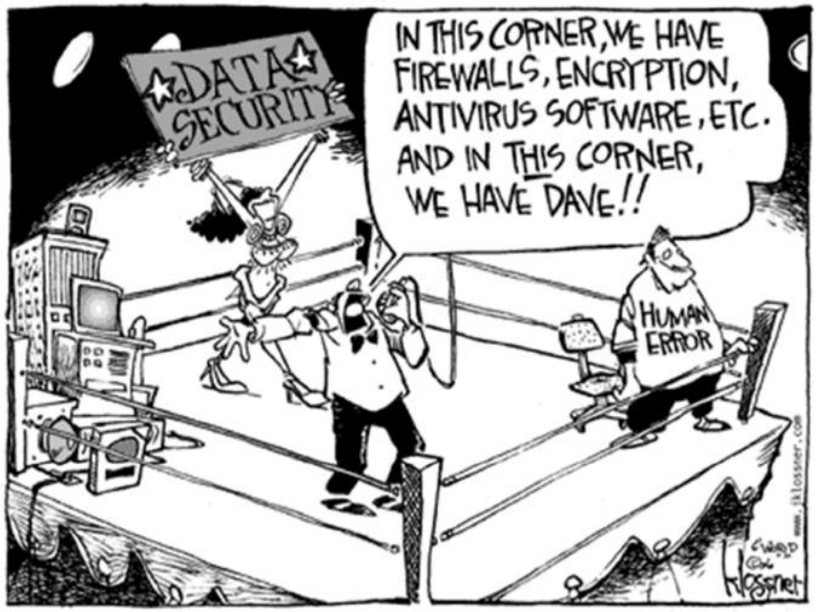


Antivirus/malware	86.0%
Firewalls	80.7%
Data encryption (data in transit)	64.0%
Audit logs of each access to pt. health and financial records	60.0%
Data encryption (data at rest)	58.7%
Patch and vulnerability management	57.3%
Intrusion detection systems (IDS)	54.0%
Network monitoring tools	52.7%
Mobile device management (MDM)	52.0%
User access controls	50.7%
Intrusion prevention system	48.0%
Access control lists	47.3%
Single sign on	47.3%

Source: 2016 HIMSS Cybersecurity Survey

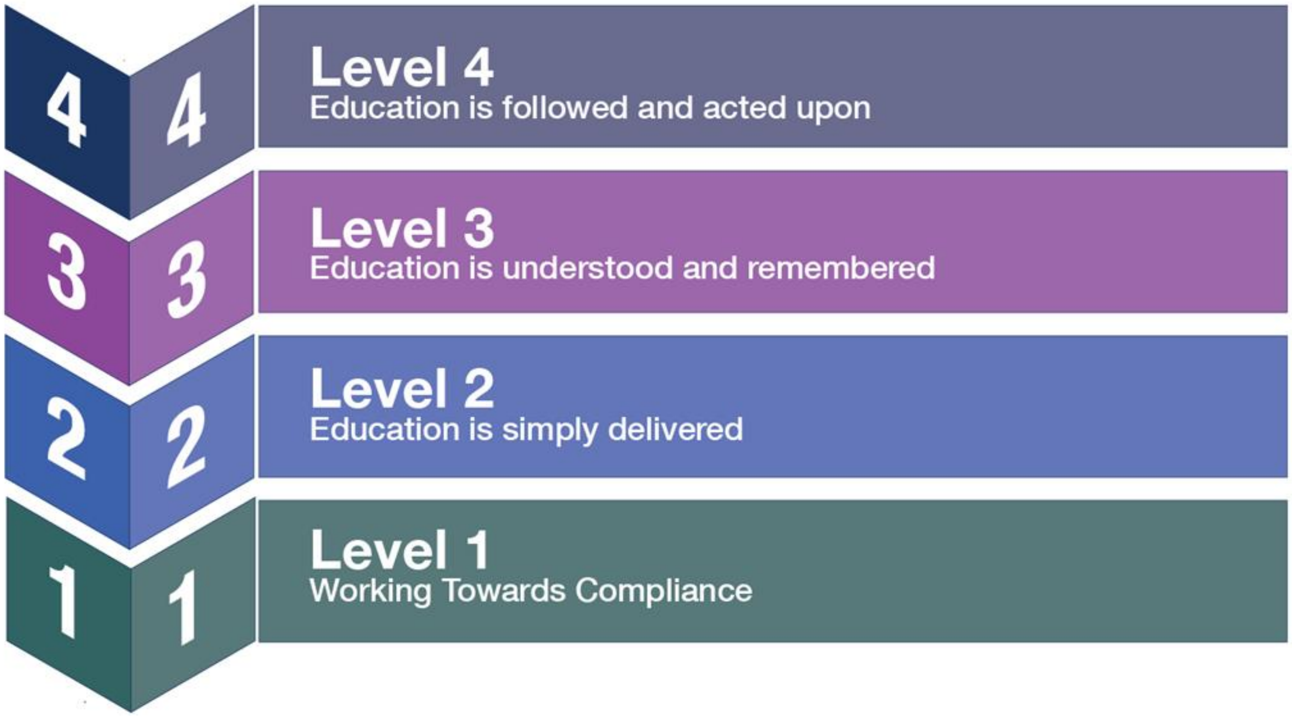


Source: 2016 SANS Security Awareness Report


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
Klossner

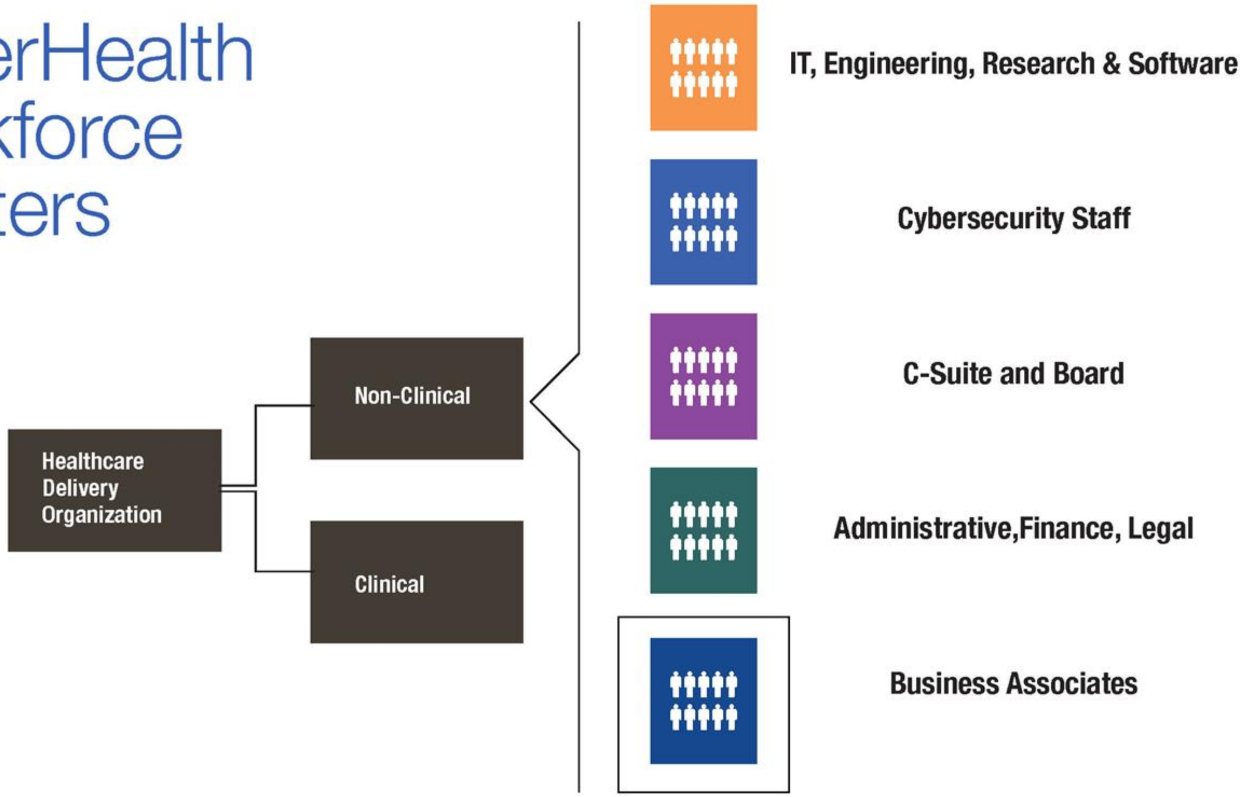
- Awareness Compliance ≠ Security
- >75% of security events in healthcare involve “the human element”
- Improper workforce behavior is the highest threat, therefore…
- Creating a cyber-savvy workforce is the best first line of defense

Awareness → Behavior Change



4
4
Level 4
Education is followed and acted upon
3
3
Level 3
Education is understood and remembered
2
2
Level 2
Education is simply delivered
1
1
Level 1
Working Towards Compliance

CyberHealth Workforce Clusters



Healthcare Delivery Organization

Non-Clinical

Clinical

IT, Engineering, Research & Software

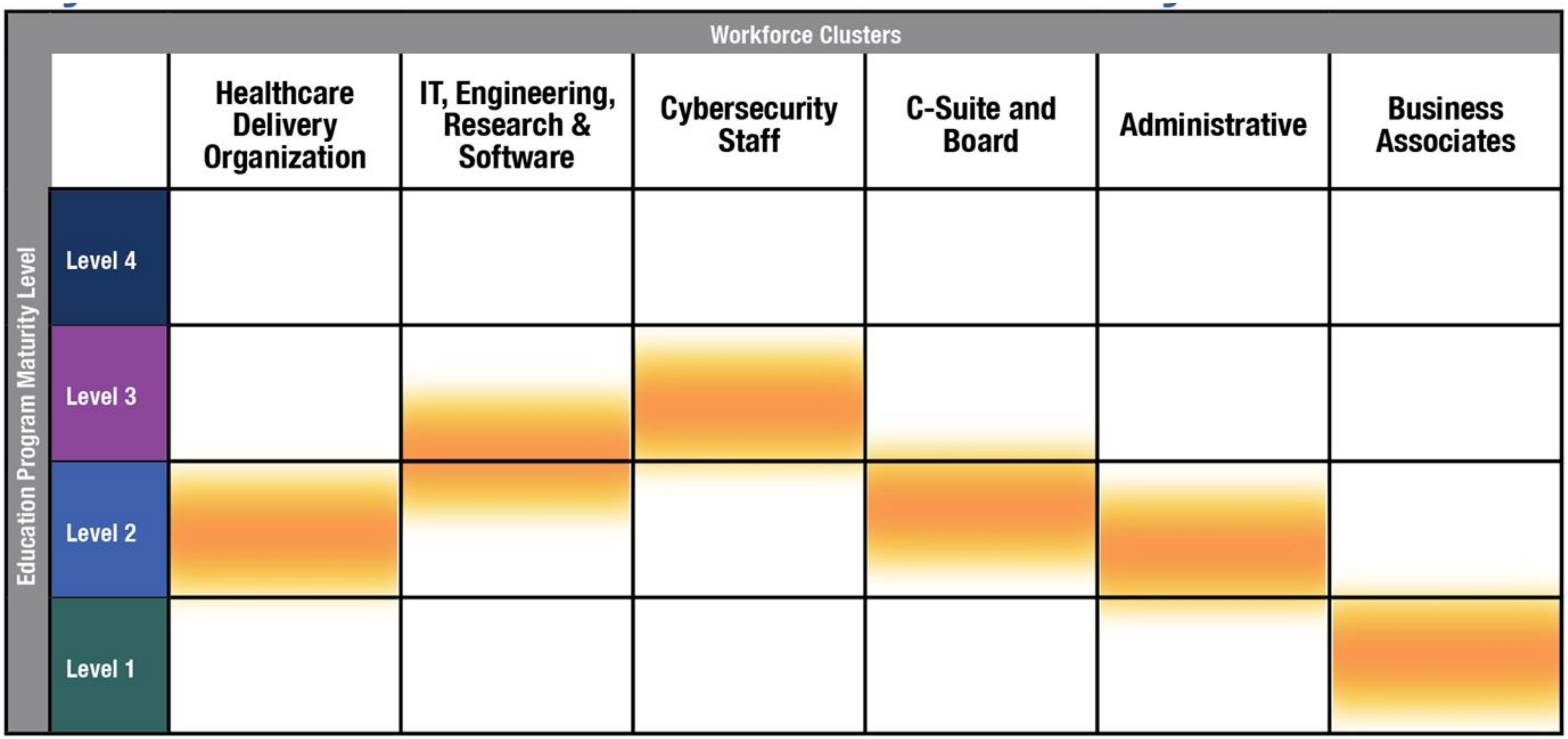
Cybersecurity Staff

C-Suite and Board

Administrative,Finance, Legal

Business Associates

		Workforce Clusters					
		Healthcare Delivery Organization	IT, Engineering, Research & Software	Cybersecurity Staff	C-Suite and Board	Administrative	Business Associates
Education Program Maturity Level	Level 4						
	Level 3						
	Level 2						
	Level 1						



Education Program Maturity Level	Workforce Clusters					
	Healthcare Delivery Organization	IT, Engineering, Research & Software	Cybersecurity Staff	C-Suite and Board	Administrative	Business Associates
Level 4						
Level 3		●	●			
Level 2	●	●		●	●	
Level 1						●

- Security is one of many training topics
- Only 15% of training can be recalled after 30 days

To affect behavior:
Training needs to be reinforced

- Posters, cafeteria signs, screensavers, etc.
- Monthly phishing
- Table-top exercises
- Gamification

- Time is of the essence for many employees
- Jobs are complicated
- Employees sneak in personal activities on work equipment

To affect behavior:
It needs to be simple

- No administrative access
- Provide automatic software & browser patch updates
- Password lockers
- Separate browser & email for personal activities
- Device trackers, full storage encryption

Toby Gouker, PhD, GSLC
tgouker@fcp.com
(443) 570-0466

Improving Security Culture to Reduce Human Error

Darren Lacey – Chief Information Security Officer and Director of IT Compliance, Johns Hopkins University and Johns Hopkins Medicine

Kevin Crain – Chief Information Security Officer and Director of IT Security, University of Maryland Medical System

Roundtable Discussion
Q&A

THANK YOU!

MHCC MARYLAND HEALTH CARE COMMISSION

HSCRC Health Services Cost Review Commission

HIMSS MARYLAND Chapter

Maryland Hospital Association