EXTREME MAKEOVER: METRICS ADDITION
BIOGRAPHY

• Certified Information Systems Security Professional (CISSP);

• More than 20 years of information security, information technology and legal experience;

• A former Special Agent for the FBI;

• Served as the Information Systems Security Officer, in addition, to investigating cybercrime;

• Graduate of Xavier University in Cincinnati, Ohio with a B.S.B.A in Information Systems;

• A licensed attorney in the State of Texas.

Mary N. Chaney, Esq., CISSP
THE PAST
HISTORICALLY

• Metrics = Quantitative measure
• Theoretically target audience get their specific metrics
• Dashboards, charts, presentations, etc. all showing a lot of “stuff”
WHAT HAS BEEN THE RESPONSE?

W = Who
G = Gives
A = A
S = Shhhhh!!
WHY HAVE THINGS CHANGED?

• Security in obscurity
• Lost in Translation
• Metrics need to “Make Business Sense”
• Don’t let your message get lost in the numbers!
VARIOUS VIEWS:

Executives – How are we doing?
Stakeholders – Guidance?
Risk Management – What’s our risk posture?
Compliance – Are we complaint?
SOC – WTH?
WHAT IS YOUR MESSAGE?

Metrics have different purposes depending on maturity.

1. Actionable
2. Informative
3. Health Metrics
NEW DAY, NEW WAY

3 high risk areas:

1. Application
2. Database
3. 3rd Party Supplier
SCORECARDS

Application
1. Vulnerabilities
2. Coding (OWASP)
3. Access
4. Logging/Monitoring/Alerting
5. Stakeholder Engagement

Database
1. Vulnerabilities
2. Access
3. Logging/Monitoring/Alerting
4. Stakeholder Engagement

3rd Party Supplier
1. Vulnerabilities
2. Access
3. Logging/Monitoring/Alerting
4. Stakeholder Engagement
BASE DEFINITIONS

What makes up the score for each component:

1. What is a vulnerability? (Patches, AV, etc.)
2. Who has access? (End user, HPA user, customer, etc.)
3. Logging/Monitoring/Alerting (standard logs, active monitoring, SLA defined alerts)
4. Engagement (Set threshold/SLA for response times based on criticality)
DO THE MATH:

SCORE = 100%
(Each component makes up a percentage of the score)

Database

1. Vulnerabilities = 25%
2. Access = 25%
3. Logging/Monitoring/Alerting = 25%
4. Stakeholder Engagement = 25%
QUESTIONS?