



Homeland
Security



Managing Risk Against Cyber Uncertainties: Using the Dashboard

Federal Network Resilience Division

October 31, 2017

Webinar Objectives

- To Remind Ourselves of the Rationale for Continuous Monitoring
- To Explore Federal Cybersecurity Operators' Use of Security-Based Performance Dashboards, Over Time
- To Review the Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) Program
- To Understand How the (CDM) Dashboards Will Work, In Real Time



About Today's Speaker

Dave Otto is the Risk Scoring Lead within the Office of Cybersecurity and Communications' Federal Network Resilience Division.

Prior to joining the Department of Homeland Security, Dave was the Enterprise Secure Configuration Manager for the Department of Justice (DOJ). At DOJ, Dave and his team spearheaded the effort to implement endpoint management and continuous monitoring across the entire enterprise.

Dave has a diverse background in law enforcement, counseling psychology, and cybersecurity. He brings extensive experience with physical and cybersecurity, human factor studies, system design, and secure configuration management to his work with risk management and continuous monitoring.



Disclaimer For This Webinar

Dave will share his views of what has worked and what has not worked, based on his professional experiences.

There are multiple paths to success!



A Trip Down Memory Lane

Cyber style.....

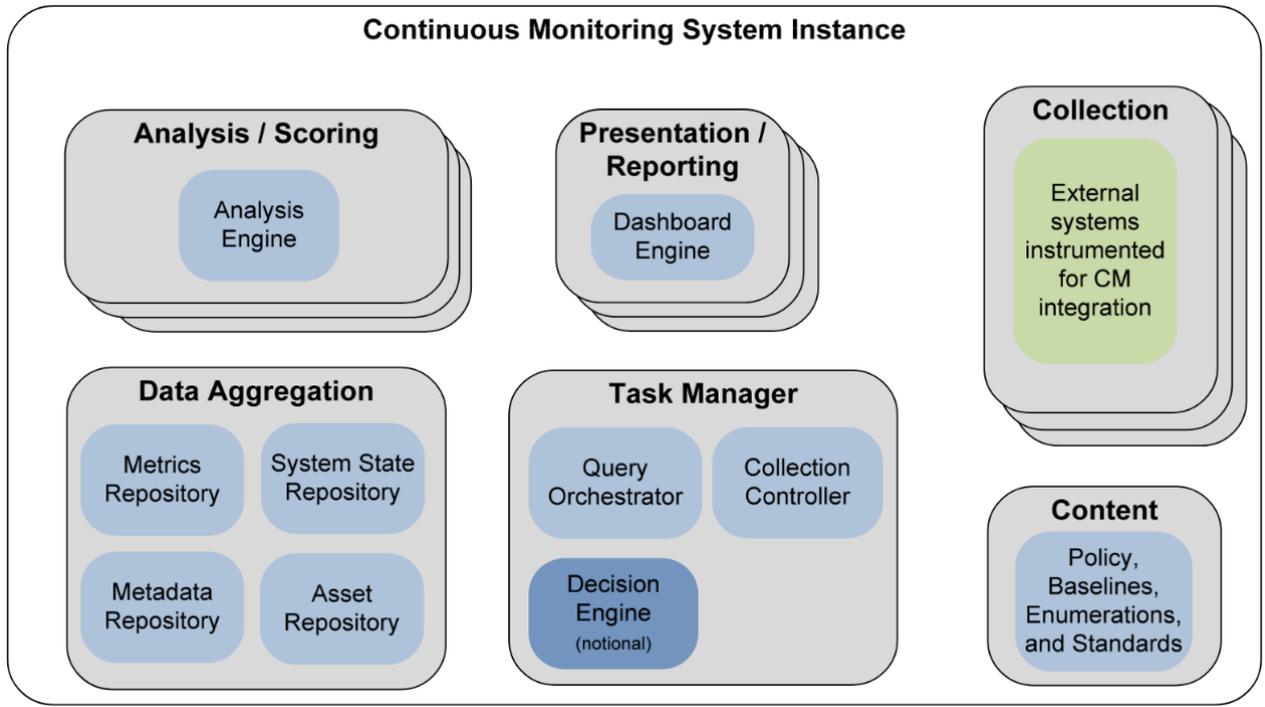


Homeland
Security

Federal Network Resilience
Cybersecurity & Communications

Before There Was Continuous Diagnostics and Mitigation...

There was the **Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS)** Reference Architecture.



CAESARS was a good foundation. DHS expanded upon its framework to address the limitations and add additional capabilities.



Then Came the CAESARS Framework Extension (FE)

The goal of this document was to facilitate **enterprise continuous monitoring** by presenting a reference model that enables organizations to aggregate collected data from across a diverse set of security tools, analyze that data, perform scoring, enable user queries, and provide overall situational awareness.



NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



2010

The Federal Information Security and Identity Management Subcommittee (ISIMC) initiates a joint DHS, NSA, and NIST research initiative to develop the CAESARS Framework Extension (FE).

2011

NIST and DHS co-publish the CAESARS Framework Extension (NISTIR 7756): *An Enterprise Continuous Monitoring Technical Reference Model.*



Homeland
Security

We Pushed for Continuous Monitoring Because

Continuous monitoring allowed for:

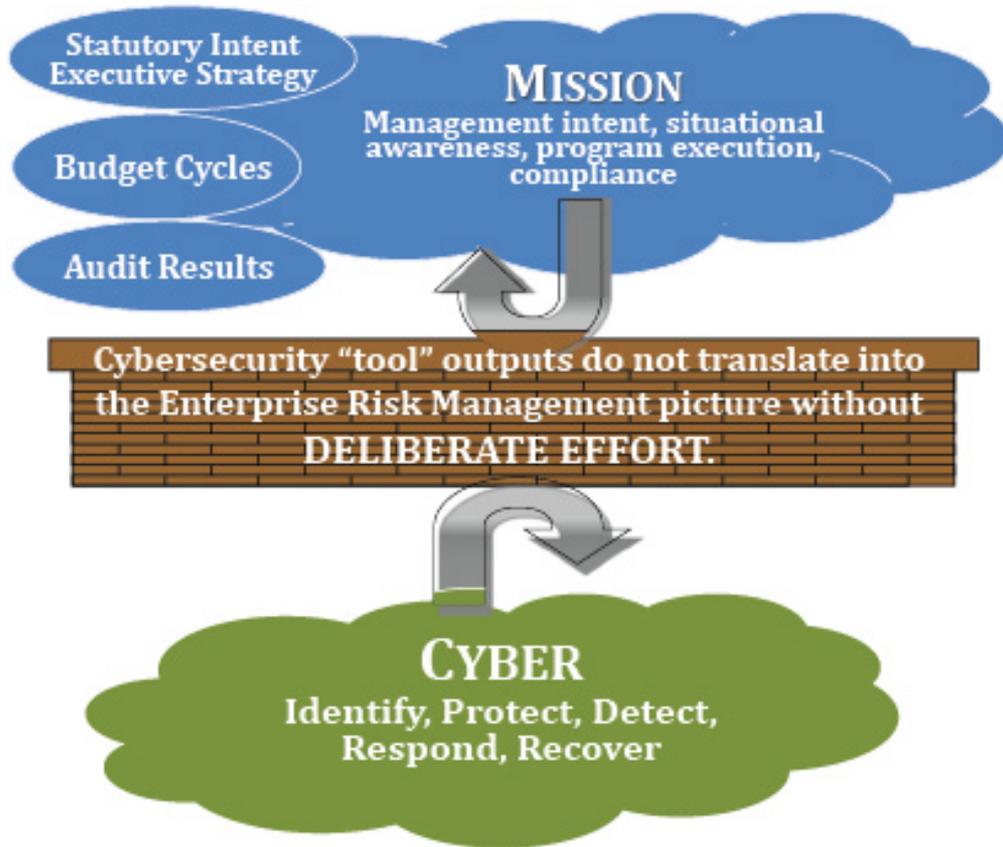
1. Ongoing **observance and analysis** of the operational states of systems; and
2. Provisioning of decision support regarding situational awareness and **deviations from expectations.**

Continuous monitoring is ongoing observance with intent to provide warning.*

*MITRE, in support of the National Security Agency.



There Was/Is Obstruction in the Cybersecurity Value Chain

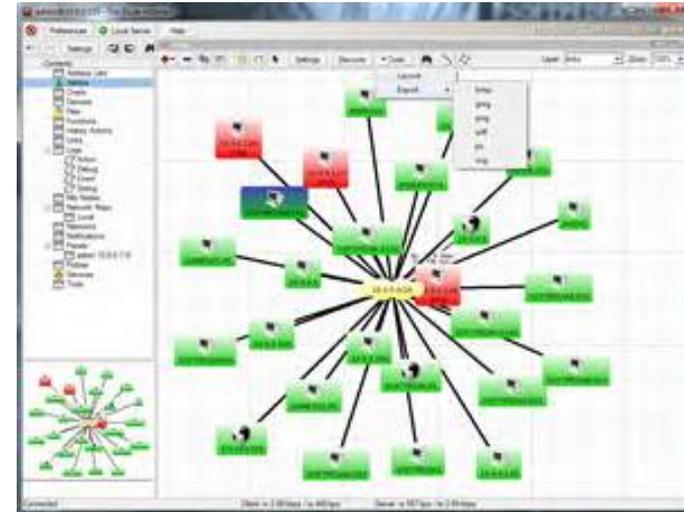
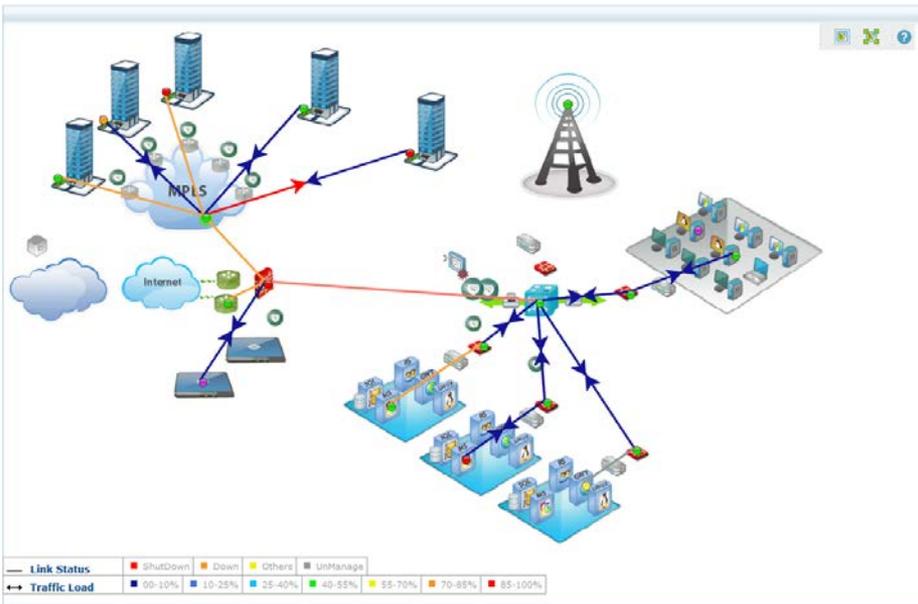


Ineffective support for:	
Congress <ul style="list-style-type: none">• Safety of constituents' data	Committee Members & Staff OMB <ul style="list-style-type: none">• Proper execution of authorities• ROI on taxpayer funds• Compliance
National Security Council <ul style="list-style-type: none">• Effects on ability to exercise elements of national power	Authorizing Officials CISO <ul style="list-style-type: none">• Tying security outcomes to mission/business success• Effective resource utilization
Federal CIO Council NCCIC <ul style="list-style-type: none">• Producing actionable information• Identifying best practices	

Disjointed collection and use of data inhibits effective governance, decision-making, and action.



Jetting Back to The Here and Now



RSA Archer eGRC
with RSA Security
Management Extensions

Enterprise Governance, Risk and Compliance

Executive | Policy Management | Policy Center | Enterprise Management | Risk Management | Compliance Management | Business Continuity Management | Incident Management | More

Search Control Procedures | Add New Control Procedure | Open Findings Report

Dashboard: Compliance Management | Welcome, System Administrator | Options

Compliance Summary

Authoritative Sources Compliance Summary

Source Name	Compliance Rating	% of Non Compliant Controls	Criticality	Source Type
COBE 4.1.620071	██████████	17%	Key	Common Practice
EU Privacy Act	██████████	17%	Key	Law/Regulation
FACT Act "Red Flag" Guidelines, November 2007	██████████	14%	Key	Law/Regulation
GLBA	██████████	12%	Key	Law/Regulation
HRSA Privacy	██████████	2%	Key	Law/Regulation
ISO/IEC 27001:2005	██████████	18%	Key	Common Practice
NIST SP 800-53 (August 2005)	██████████	17%	Key	Common Practice
Payment Card Industry Data Security Standard v2	██████████	18%	Key	Industry Standard
U.S. State Privacy Laws	██████████	17%	Key	Law/Regulation

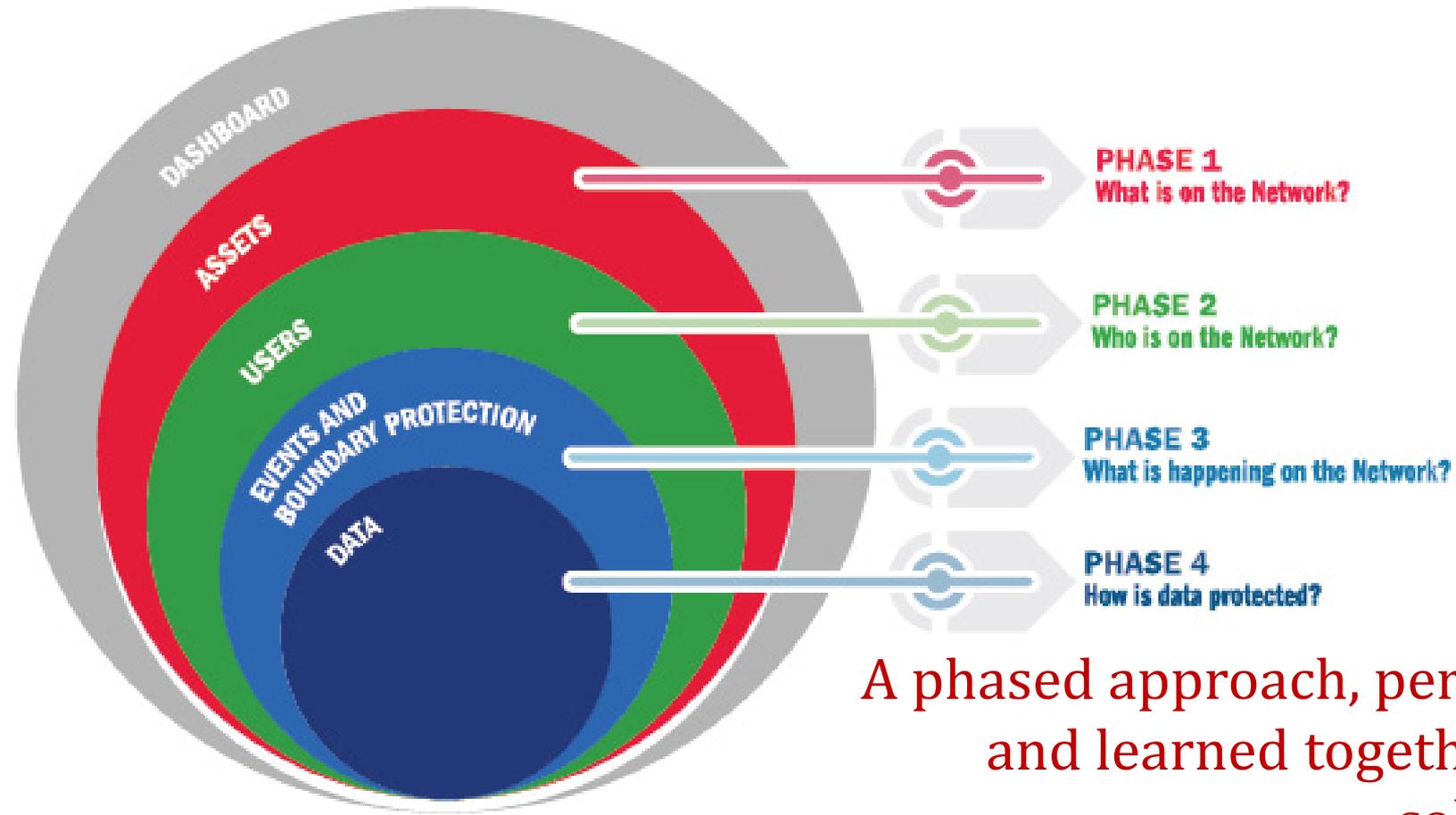
Overall Compliance: Control Procedures By Compliance Status

Technical Control Compliance: Overall Configuration Compliance



The Continuous Diagnostics and Mitigation Method

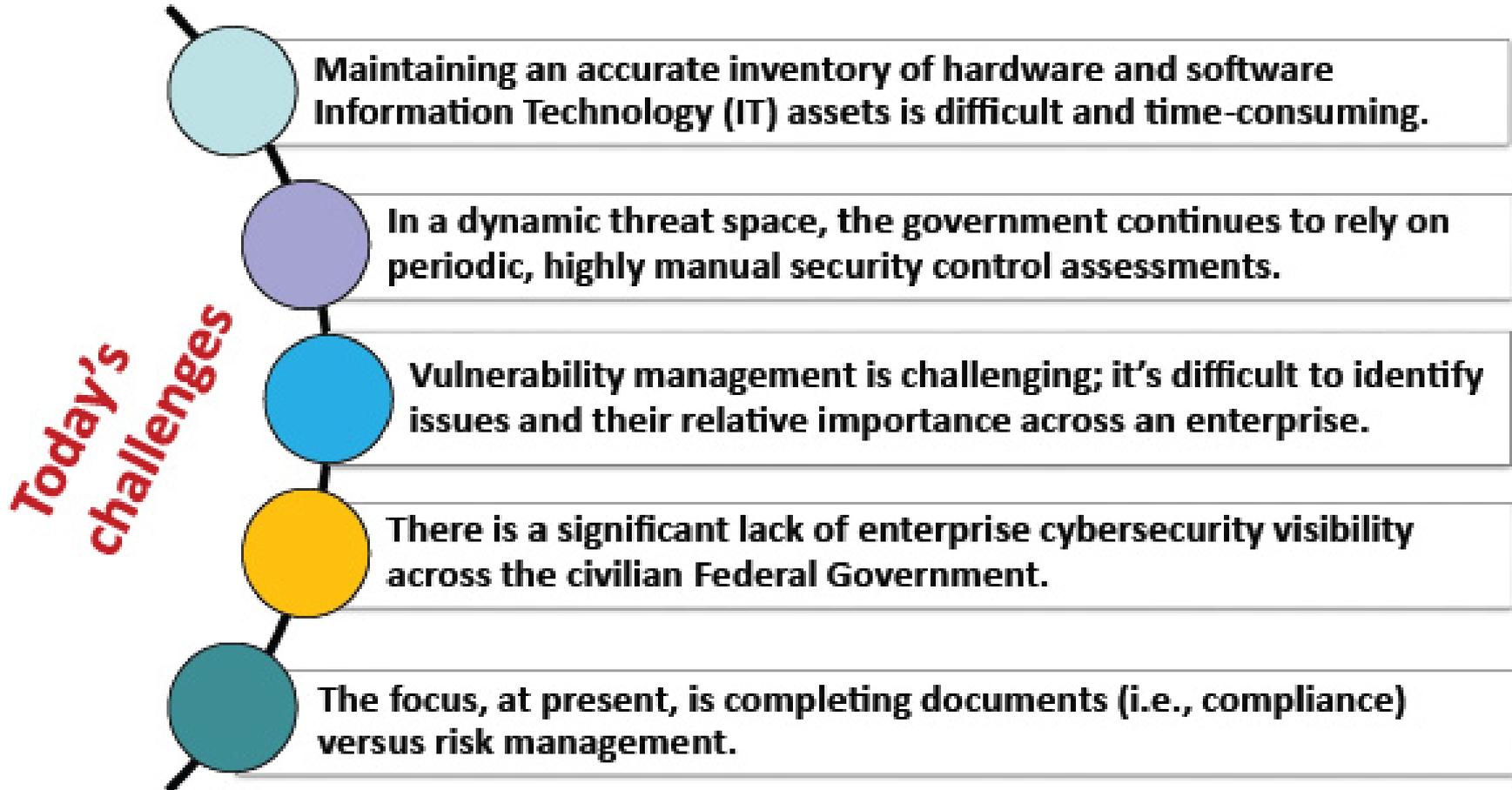
Do you know where your cyber risks are?



A phased approach, performed and learned together, by a collective.



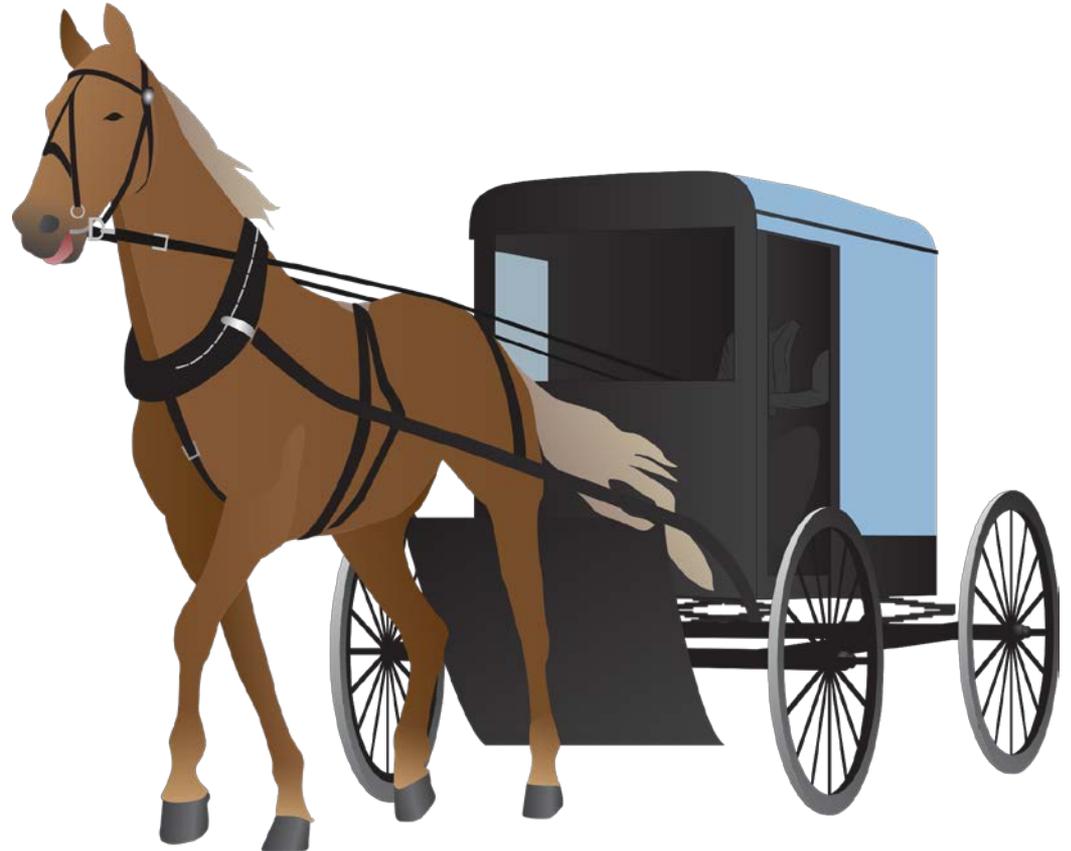
Current Cybersecurity Gaps



Bring on the Dashboards!

Noun

1. An upturned screen of wood or leather placed on the front of a horse-drawn carriage, sleigh or other vehicle that protected the driver from mud, debris, water, and snow thrown up by the horse's hooves.
2. A panel under the windscreen of a motor car or aircraft, containing indicator dials, compartments, and sometimes controls.



Why Are Dashboards Useful?

At the tactical and agency level, they:

- Showcase key details and provides insights, squelching noise.
- Track progress and performance through consistent measures, over time.

At the strategic and enterprise level, they:

- Make situational understanding congruent amongst all.
- Ensure clear and consistent communications.
- Make decision-making more effective.
- Make prediction possible.



A Dashboard's Value Proposition

- Maintain an accurate picture of an organization's security risk posture;
- Have visibility into assets;
- Leverage use of automated data feeds to measure security;
- Ensure effectiveness of security controls; and
- Enable prioritization of mitigation and remediation.



I Have a Dashboard. Now I Know All Risks, Right?

If the highest aim of the captain were to preserve his ship, he would keep it in port forever.
- Thomas Aquinas



Laying the Foundation for Structured Sense-Making

**Innovative approaches
to governance needed!**



Dashboards: Just The Facts

- Dashboards provide situational awareness of a standard set of measures across NIST's Risk Management Framework (RMF) Tiers and all CDM acquisition-centric groupings of agencies.
- Dashboards **are not** comprehensive tools for analysis, decision making, or management.
- Dashboards **do not** peek around corners.
- Cybersecurity tools at the operational level **do not** calculate risk.



Continuous Diagnostics and Mitigation Dashboard Hierarchy

What can we see now that we could not see before?

Are we better able to manage and mitigate cyber risk?



Adversaries Exploit Easy Stuff First: We See It



Common Exploit Framework: It's On The Internet



Brower Exploitation Framework (BeEF)



Penetration Testing



Social Engineering Toolset (SET)



Web Vulnerability Scanner



Network Mapper



Penetration Tools



Password Cracking

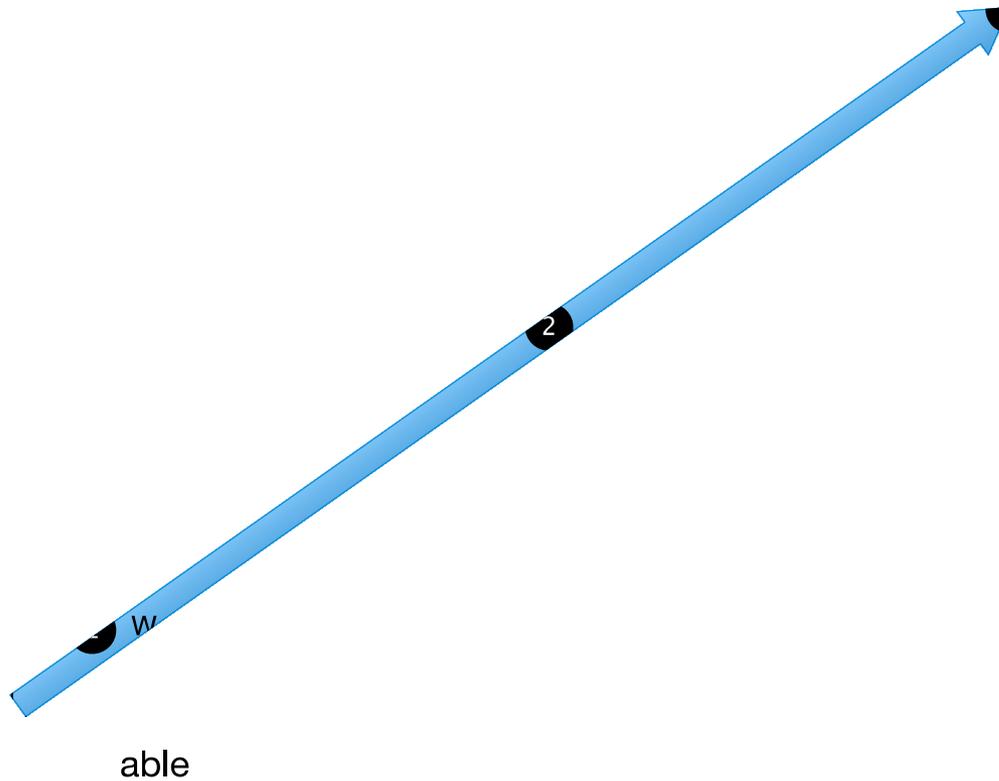


Hacking Tool Repository

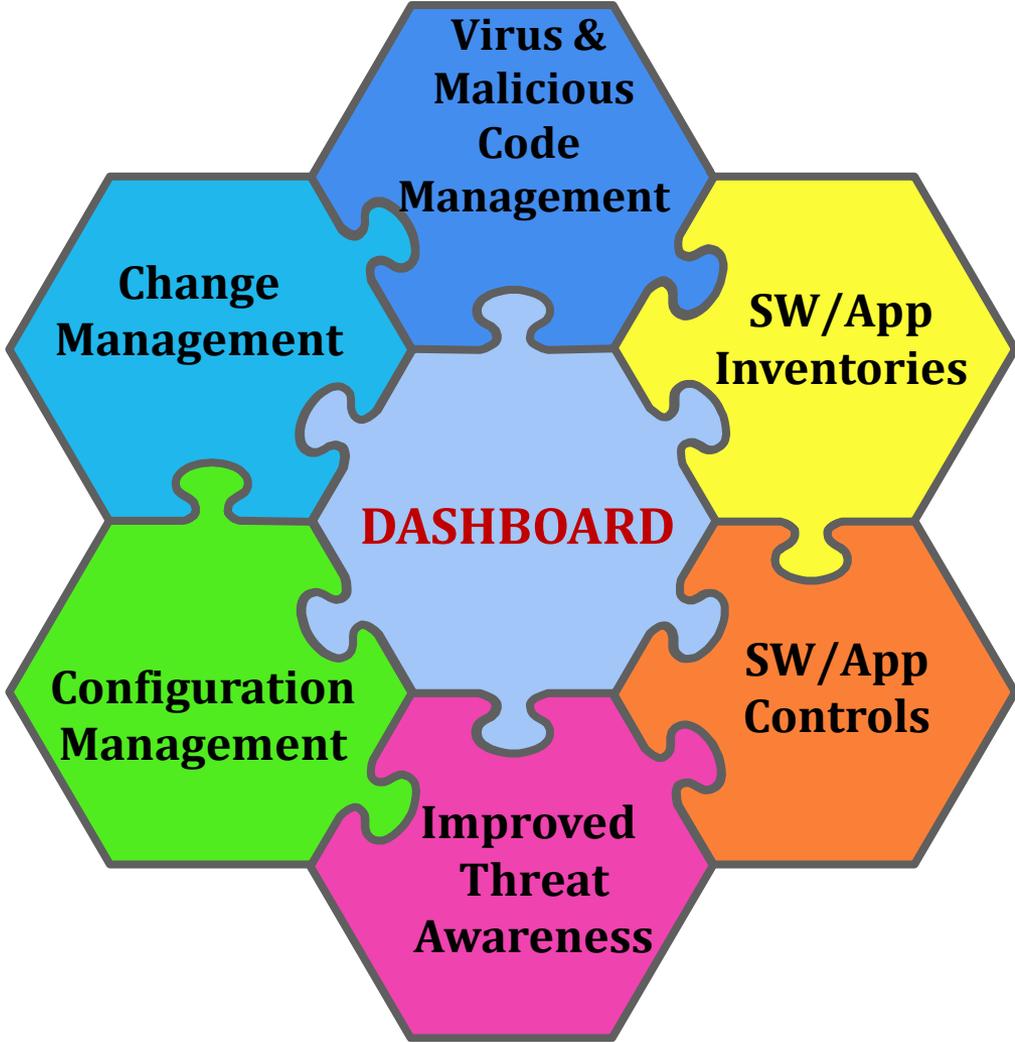
Our adversaries use **low-cost** attack capabilities to exploit common vulnerabilities.

The information provided above is a sampling. DHS does not endorse any non-government websites, companies or applications.

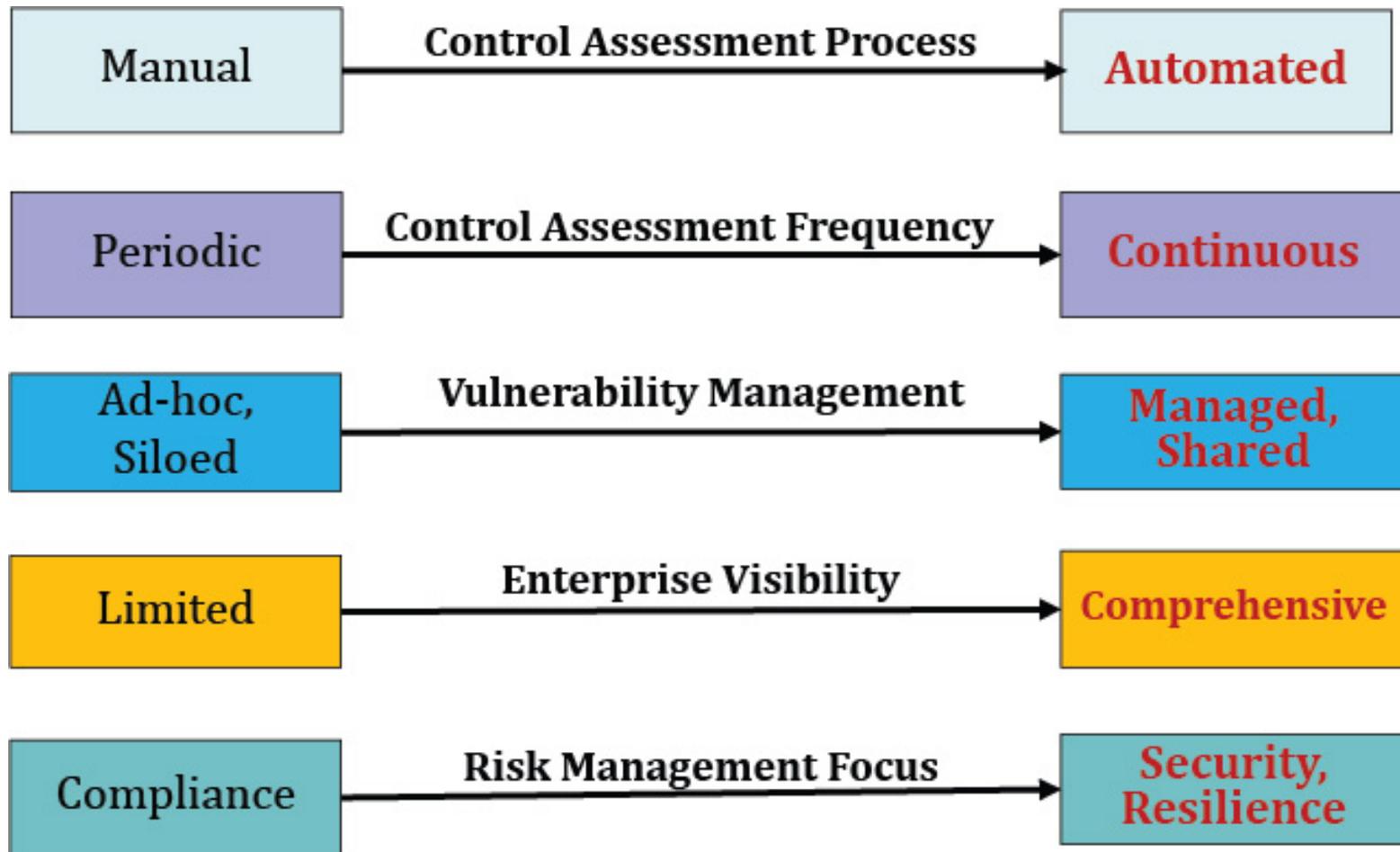
Cyber Risk, By The Numbers



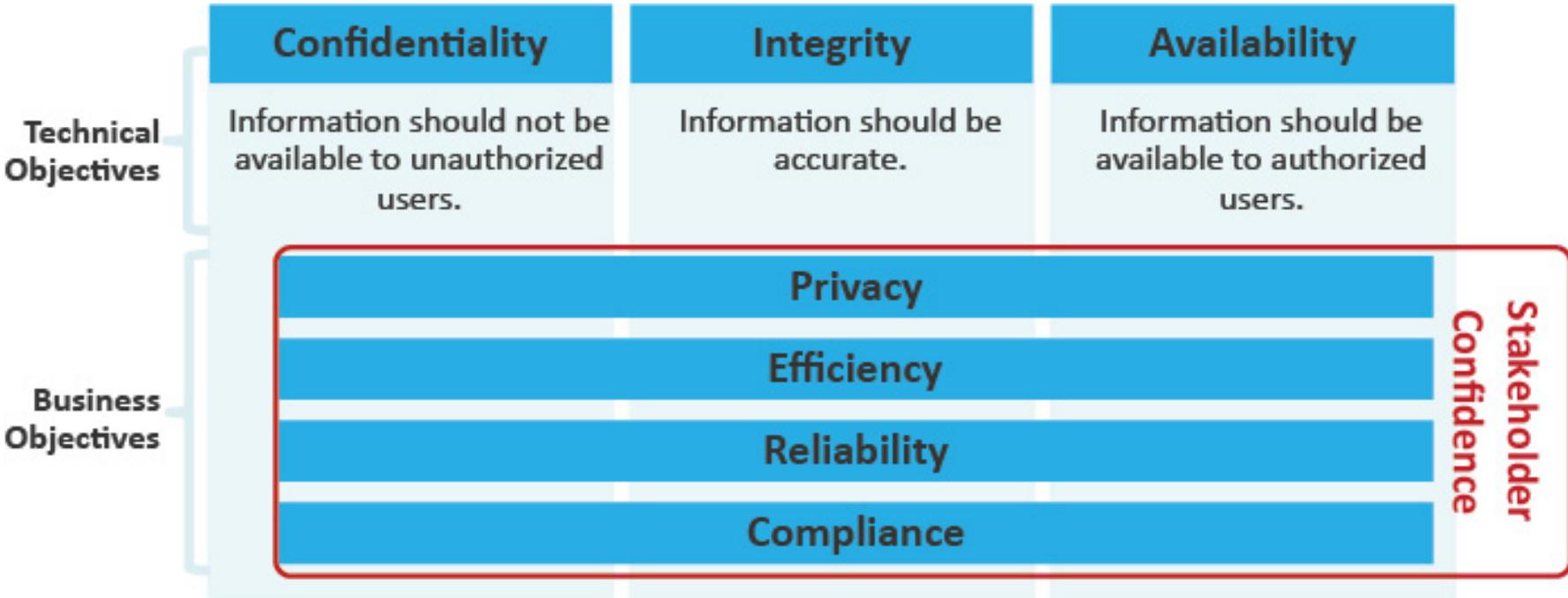
Enabling Improved Vulnerability Management



Dashboards Are a Tool of Governance, Driving Change



What Are We Aiming For?



Success at the Point of Execution

1. First why, then what.

2. Leverage enablers at the proper organizational level; avoid the “2,000-mile screwdriver.”
3. Tier 2 sets the direction through governance facets; Tier 3 executes through disciplined project management.
4. Avoid numerous, rapid changes that cause enterprise turbulence.
5. Tie actions to expected outcomes and expected timeframes; socialize and communicate expectations.
6. Set decision points to check progress against expectations.
7. Build knowledge base to make for faster and more effective Observe, Orient, Decide, and Act (OODA) loop.



Look At Current Events For The “Why?”

4,149 data breaches reported in 2016
[Risk Based Security]

4.2 Billion records exposed in data breaches in 2016
[Risk Based Security]

56% YoY increase in healthcare data breaches
[HHS]

\$445 Billion Economic impact of cyber risks in 2016
[World Economic Forum]

\$402 Cost to victim organization per breached PHI record
[IBM]

\$4m Average cost of data breach to victim organization
[IBM]

\$2,528 Average amount each victim spent as a result of medical identity theft
[Accenture]

U.S. SEC Exploit in EDGAR led to illicit trading gains
[IdentityForce]

Equifax 143 Million consumers impacted by PII breach
[IdentityForce]

FAFSA: IRS Data Retrieval Tool - 100 K privacy records
[IdentityForce]



Success at the Point of Execution

1. First why, then what.
- 2. Leverage enablers at the proper organizational level; avoid the “2,000-mile screwdriver.”**
3. Tier 2 sets the direction through governance facets; Tier 3 executes through disciplined project management.
4. Avoid numerous, rapid changes that cause enterprise turbulence.
5. Tie actions to expected outcomes and expected timeframes; socialize and communicate expectations.
6. Set decision points to check progress against expectations.
7. Build knowledge base to make for faster and more effective Observe, Orient, Decide, and Act (OODA) loop.



Success at the Point of Execution

1. First why, then what.
2. Leverage enablers at the proper organizational level; avoid the “2,000-mile screwdriver.”
- 3. Tiers 1 and 2 set the direction through governance facets; Tier 3 executes through disciplined project management.**
4. Avoid numerous, rapid changes that cause enterprise turbulence.
5. Tie actions to expected outcomes and expected timeframes; socialize and communicate expectations.
6. Set decision points to check progress against expectations.
7. Build knowledge base to make for faster and more effective Observe, Orient, Decide, and Act (OODA) loop.



A Comparison, In Brief: Operations vs. Governance

	OPERATIONS (RMF Tier 3)	GOVERNANCE (RMF Tiers 1, 2)
Scope	Individual networks, systems, users, organizations	Multiple networks, systems, user bases, organizations
Timescale	Immediate to 6 months	6 to 36 months
Level of Abstraction	Transactional	Trends, aggregations
Management Impact	Direct interaction	Context setting



Success at the Point of Execution

1. First why, then what.
2. Leverage enablers at the proper organizational level; avoid the “2,000-mile screwdriver.”
3. Tier 2 sets the direction through governance facets; Tier 3 executes through disciplined project management.
- 4. Avoid numerous, rapid changes that cause enterprise turbulence.**
5. Tie actions to expected outcomes and expected timeframes; socialize and communicate expectations.
6. Set decision points to check progress against expectations.
7. Build knowledge base to make for faster and more effective Observe, Orient, Decide, and Act (OODA) loop.



Success at the Point of Execution

1. First why, then what.
2. Leverage enablers at the proper organizational level; avoid the “2,000-mile screwdriver.”
3. Tier 2 sets the direction through governance facets; Tier 3 executes through disciplined project management.
4. Avoid numerous, rapid changes that cause enterprise turbulence.
- 5. Tie actions to expected outcomes and expected timeframes; socialize and communicate expectations.**
6. Set decision points to check progress against expectations.
7. Build knowledge base to make for faster and more effective Observe, Orient, Decide, and Act (OODA) loop.



Success at the Point of Execution

1. First why, then what.
2. Leverage enablers at the proper organizational level; avoid the “2,000-mile screwdriver.”
3. Tier 2 sets the direction through governance facets; Tier 3 executes through disciplined project management.
4. Avoid numerous, rapid changes that cause enterprise turbulence.
5. Tie actions to expected outcomes and expected timeframes; socialize and communicate expectations.
- 6. Set decision points to check progress against expectations.**
7. Build knowledge base to make for faster and more effective Observe, Orient, Decide, and Act (OODA) loop.



Success at the Point of Execution

1. First why, then what.
2. Leverage enablers at the proper organizational level; avoid the “2,000-mile screwdriver.”
3. Tier 2 sets the direction through governance facets; Tier 3 executes through disciplined project management.
4. Avoid numerous, rapid changes that cause enterprise turbulence.
5. Tie actions to expected outcomes and expected timeframes; socialize and communicate expectations.
6. Set decision points to check progress against expectations.
7. **Build knowledge base to make for faster and more effective Observe, Orient, Decide, and Act (OODA) loop.**



Thank You For Joining Us!



Dave Otto, CISSP

Federal Network Resilience Division

Office of Cybersecurity and Communications

CyberLiaison@hq.dhs.gov



Homeland
Security