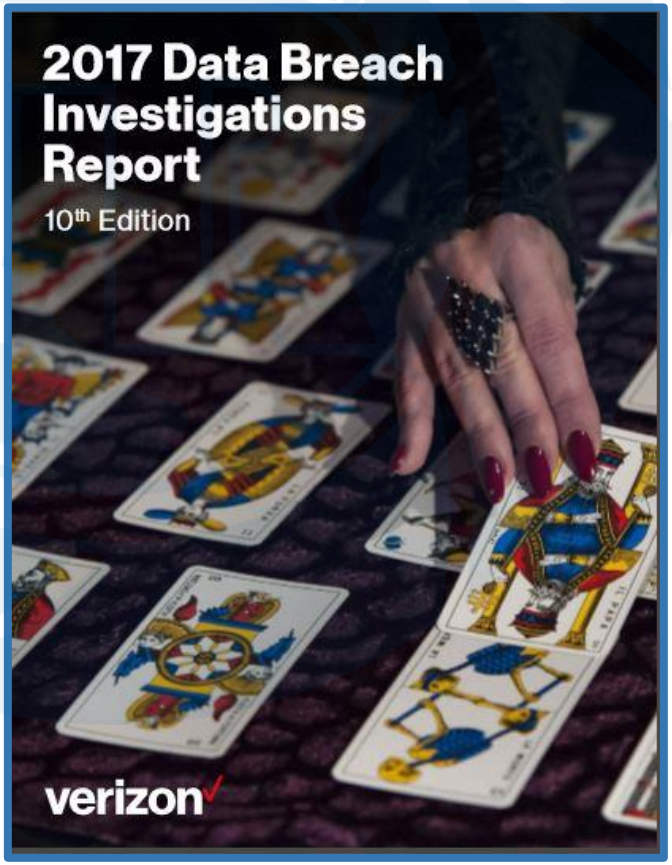
Your Workforce—is the Key to Cyber Resilience

R. “Montana” Williams, CWDP
President
Titan Rain Cybersecurity, LLC

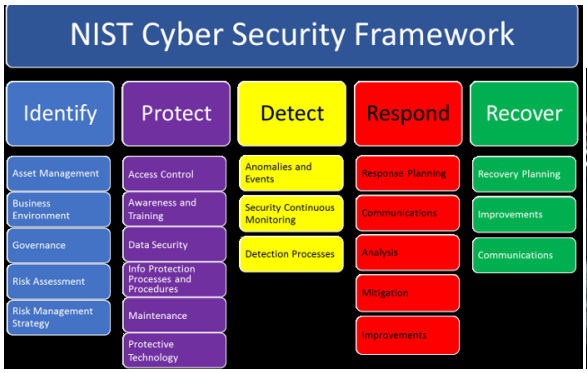
The State of Global Cyber Resilience

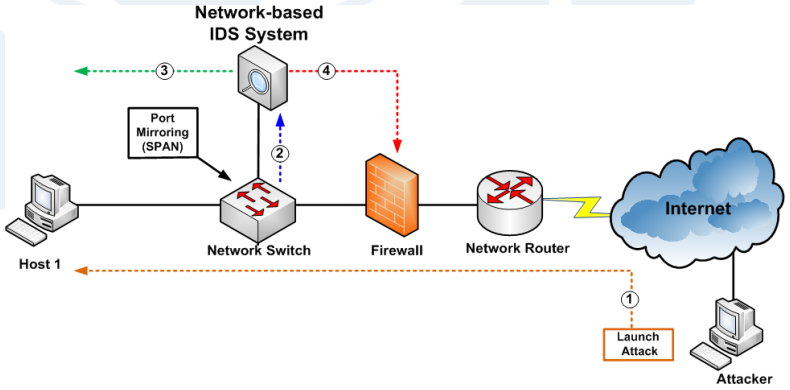
- Summary of the Verizon Report
  - 75% involve external actors
  - 51% involve criminal groups
  - 81% involve stolen credentials or weak passwords
  - 43% involve social attacks (social engineering/phishing
  - 66% involve malware installation via attachments
  - 73% are financially motivated
- Cost of Cyber Attack
  - $6T annually cost of cybercrime thru 2012 (Forbes)
  - Cost of per breach has declined from $4M to $3.6M
    - Technology—Analytics, SIEM, encryption, ISAOs
    - Implementation of governance, risk, compliance



Cause(s) of Failure

- Is it our Technology?
- Is it our processes, regulations, or policies?
- Is it our ***people***?





People—the Chain's Weakest Link

- Organizational culture
- Catching Phish & Click'itis
- Lack of Policy & Accountability
- Workforce Development

Global Cybersecurity Resiliency Crisis—It's a People not Technical Problem

Cyber Resiliency—Start Here

- Organizational Cybersecurity Culture
  - From the Boardroom to the Breakroom
    - Leaders: Make yourself available
    - Make it Real
    - Make it a Team Effort
    - Make it a Priority
    - Make it Safe to ask Questions
    - Make it Personal
    - Make it transparent
    - Make it easy to come clean
    - Make it Plain
  - Espoused vs. Actual Values
  - Understand Cybersecurity's Return on Investment

Cyber Resiliency—Start Here

- Catching Phish & Click'itis
  - Overcoming Cognitive Bias—if it is too good to be true
  - Awareness Training—Beyond the Once a Year Model
    - Recency
    - Model
      - Brief
      - Frequent
      - Focused

STOP | THINK | CONNECT™

Cyber Resiliency—Start Here

- Lack of guidance (policy) & Accountability
  - If all you do is comply—you have lost
  - Touhill's Great Cyber Policies
    - Acceptable Use
    - Computer Ethics
    - Password Protection
    - Clean Desk
    - Use of Internet
    - Employee Monitoring & Filtering
    - Technology Disposal
    - Physical Security
    - Electronic Mail
    - Removable Media
    - Remote Access
    - Mobile Device
    - Software
    - Access Control
    - Network Management

Cyber Resiliency—Start Here

- DHS Workforce Development Toolkit
  - **Prepare** Assess Your Organization's Cybersecurity Workforce Planning Readiness
  - **Plan** Tools on How to Plan for Your Cybersecurity Team
  - **Build** What Should a Cybersecurity Team Look Like
  - **Advance** Develop Your People

Cyber Resiliency—Start Here

PREPARE

- Workforce Management Lifecyle

Cyber Resiliency—Start Here

PLAN

- Workforce Planning Diagnostic Tool
  - Risk Exposure
  - Risk Tolerance

Risk Exposure Values

	Non- Federal Risk Exposure	YES	NO
Non-Federal Risk Exposure	1. Can your organization account for all its attack surfaces?		
	2. Does your organization have regular cybersecurity hygiene training for all its employees?		
	3. Does your organization protect access by granting graduated levels of clearances for employees?		
	4. Does your organization document and track successful and unsuccessful cybersecurity breaches?		
	5. Does your organization change its security posture once an attack/intrusion (regardless of success) occurs?		
	6. Does your organization require employees to undergo background checks?		
	7. Does your organization employ foreign nationals?		
	8. Does your organization's mission require you to maintain sensitive data?		
	9. Does your organization have specialized operational cybersecurity workforce?		
	10. Does a part of your workforce possess unique cybersecurity skills, beyond those needed for cyber hygiene and information assurance, like malware analysis, digital forensics, reverse engineering, threat actor identification, or ethical hacking?		

Risk Tolerance

	RISK TOLERANCE	YES	NO
Risk Tolerance	1. Has your organization identified specific threats/attacks that it can absorb (rather than address or mitigate) without damaging mission or business imperative?		
	2. Does your organization choose to plan for only some cybersecurity threats or risk?		
	3. Is there some data that your organization is willing to have breached as a cost to performing necessary business operations?		
	4. Does your organization make trade-offs (in allocation of resources to increase market share or profitability) rather than building more sophisticated cyber defenses?		
	5. Does your organization engage with external partners/entities (despite increased exposure to cyber-attacks or intrusions as a result of these dealings)?		
	6. Does your organization deliberately choose to be out of compliance with government/industry regulations because these regulations are more costly/inconvenient to follow than penalties for non-compliance?		
	7. Has your organization's cybersecurity infrastructure ,more or less, stayed the same for the last five years?		
	8. Has your organization's cybersecurity workforce (i.e., size and expertise level) more or less remained constant over the last five years?		
	9. Do you know what types of attacks present the greatest risk to your business / mission operations and success?		
	10. Is your cyber workforce prepared to "fight through" / address those attacks?		
	11. Does your workforce have the training to address those attacks?		
	12. Does your organization have a continuity of operations plan (COOP) plan for "fight through" / mission continuation, or under degraded conditions?		

Cyber Resiliency—Start Here

BUILD

- National Cybersecurity Workforce Framework
- Task-based KSAs

Cyber Resiliency—Start Here

Security Provision	Information Assurance Compliance	Software Engineering	Enterprise Architecture	Technology Demonstration	Systems Requirements Planning	Test and Evaluation	Systems Development
Operate & Maintain	Data Administration	Info System Security Mgt	Knowledge Mgt	Customer & Tech Support	Network Services	System Administration	Systems Security Analysis
Protect & Defend	Computer Network Defense (CND)	Incident Response	CND Infrastructure Support	Security Program Mgt	Vulnerability Assessment & Mgt		
Analyze	Cyber Threat Analysis	Exploitation Analysis	All-source Analysis	Targets			
Operate & Collect	Collection Operations	Cyber Operational Planning	Cyber Operations				
Oversight & Development	Legal Advice & Advocacy	Strategic Planning & Policy	Education & Training				
Investigate	Investigation	Digital Forensics					

Establishing National Standards

Job

Task/Workrole

Knowledge, Skills, and Abilities (KSA)

Cyber Resiliency—Start Here

ADVANCE

- Transition from Knowledge-based only to Experiential-based education & training
  - Centers of Academic Excellence
  - Certifying bodies—labs and performance-based assessments

Shifting the Model to Exceed Global Standards

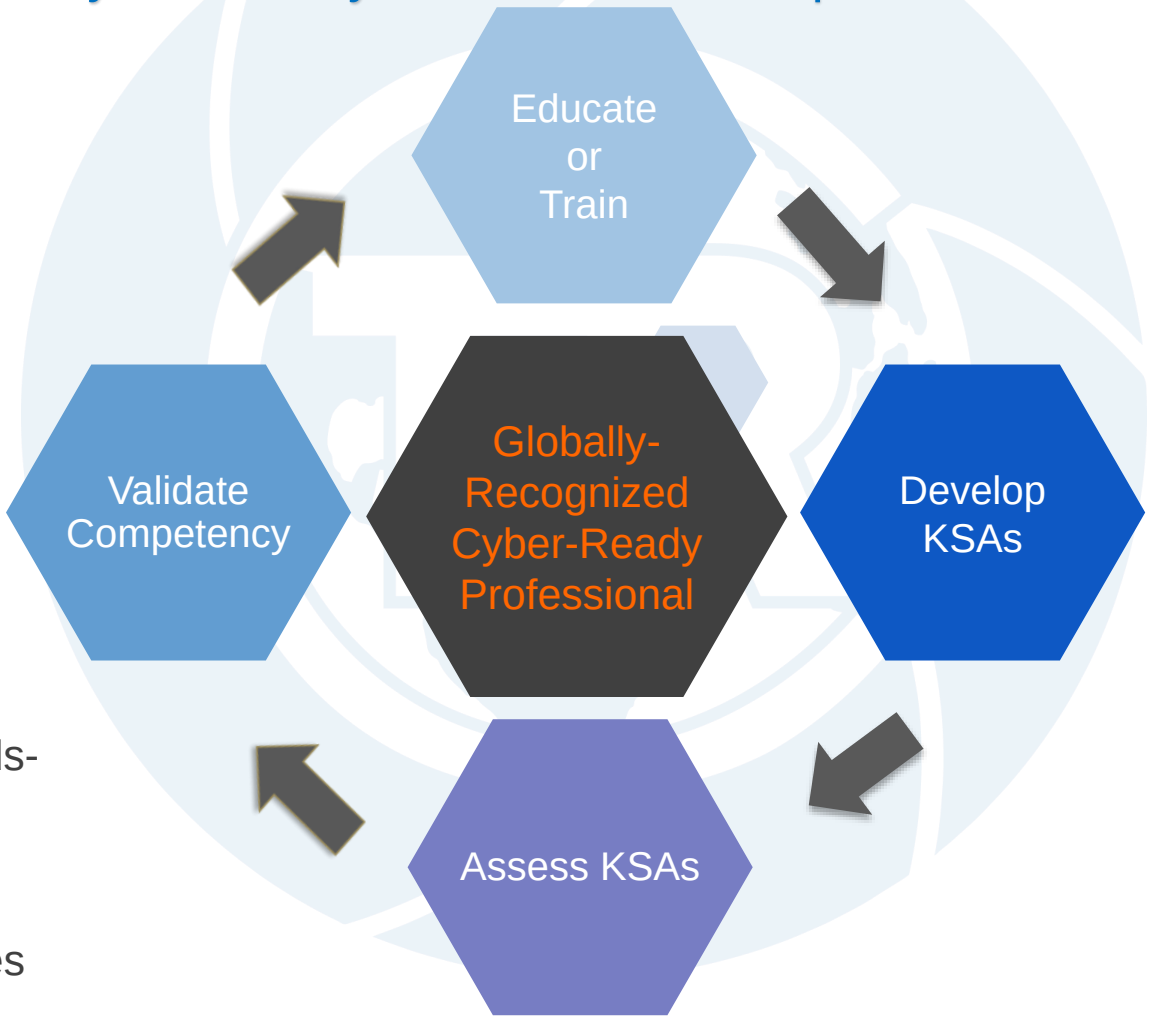
Educate or Train—World Class Trainers Delivering Globally Recognized Certification Content

Develop Knowledge, Skills, & Abilities—Combining Knowledge-based Instruction with Experiential-based Labs & Scenarios

Assess Knowledge , Skills , & Abilities—Assessing KSAs Via Hands-on Assessments

Validate Competency—Education, Development, & Assessment Validates Competency

Cybersecurity Workforce Development Model



Recommended Role Aligned Certs

Network Technicians

Novice	Journeyman		Master
CompTIA A+	CompTIA Network+	CompTIA Security+	CompTIA CASP

Incident Responders

Novice	Journeyman		Master
CompTIA Security+	CSX P	C|ND Certified Network Defender	Titan Rain Cybersecurity

Advanced Incident Response

Recommended Role Aligned Certs

Forensics

Novice

CEH Certified Ethical Hacker

Journeyman

CHFI Computer Hacking Forensic INVESTIGATOR

Fundamentals of Malware Analysis

Master

Network Forensics

Advanced Malware Analysis

Network Security Engineers

Novice

CISCO CERTIFIED CCNA ROUTING & SWITCHING

CISCO CERTIFIED CCNA SECURITY

Journeyman

CISCO CERTIFIED CCNP ROUTING & SWITCHING

CISCO CERTIFIED CCNP SECURITY

Master

CISCO CERTIFIED CCIE Security

CCSP

Recommended Role Aligned Certs

Identification and Access Management

Novice

Journeyman

Master

Vulnerability Management (Pen Testing)

Novice

Journeyman

Master

Pen Testing & Network Exploitation
Advance Malware Analysis

Recommended Role Aligned Certs

Compliance/Risk

Novice

Journeyman

Master

Project Management/Leadership

Managers

Directors

Executives

About Titan Rain Cybersecurity

- **History:** It's Roots are secured by expertise gained from the earliest cyber intrusions across the globe—thus its name
- Services Provided
  - Consulting
    - Organizational Policy & Strategy Development
    - Governance, Risk Management, & Compliance (GRC)
    - Cybersecurity Workforce Development
  - In-Person Training
    - Individual
    - Team
    - Executive/Boardroom Training

QUESTIONS????

Presenter

R. “Montana” Williams is the President & Founder of Titan Rain Cybersecurity, LLC, in Las Vegas, NV. He leads an emerging business focused on global cybersecurity strategy, policy, risk management, governance, workforce development consulting & expertise across the critical infrastructure sectors. He is a Certified Workforce Development Professional with over 25 years experience delivering training, running training organizations, creating and delivering cybersecurity workforce strategy internationally within government, academia, and industry. He lead the U.S. Department of Homeland Security’s Cybersecurity Education & Awareness Branch, commanded the USAF Cyber Red Team, & is adjunct college professor. Mr. Williams is a globally recognized expert in cyber risk, governance, threat analysis, cyber education, training, & workforce development, the architect of the NICE National Cybersecurity Workforce Framework, Federal Virtual Training Environment, & the first cyber workforce development tool kit.

montana.williams@titanraincybersecurity.com