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

The cybersecurity workforce shortfall remains a critical vulnerability for companies and nations.
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
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

- Workforce Management Lifecycle
Cyber Resiliency—Start Here

- Workforce Planning Diagnostic Tool
  - Risk Exposure
  - Risk Tolerance
# Risk Exposure Values

<table>
<thead>
<tr>
<th>Non-Federal Risk Exposure</th>
<th>YES</th>
<th>NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can your organization account for all its attack surfaces?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does your organization have regular cybersecurity hygiene training for all its employees?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does your organization protect access by granting graduated levels of clearances for employees?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does your organization document and track successful and unsuccessful cybersecurity breaches?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does your organization change its security posture once an attack/intrusion (regardless of success) occurs?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does your organization require employees to undergo background checks?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does your organization employ foreign nationals?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does your organization’s mission require you to maintain sensitive data?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does your organization have specialized operational cybersecurity workforce?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Risk Tolerance

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

- National Cybersecurity Workforce Framework
- Task-based KSAs
# Cyber Resiliency—Start Here

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Operate &amp; Maintain</td>
<td>Data Administration</td>
<td>Info System Security Mgt</td>
<td>Knowledge Mgt</td>
<td>Customer &amp; Tech Support</td>
<td>Network Services</td>
<td>System Administration</td>
<td>Systems Security Analysis</td>
</tr>
<tr>
<td>Protect &amp; Defend</td>
<td>Computer Network Defense (CND)</td>
<td>Incident Response</td>
<td>CND Infrastructure Support</td>
<td>Security Program Mgt</td>
<td>Vulnerability Assessment &amp; Mgt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analyze</td>
<td>Cyber Threat Analysis</td>
<td>Exploitation Analysis</td>
<td>All-source Analysis</td>
<td>Targets</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operate &amp; Collect</td>
<td>Collection Operations</td>
<td>Cyber Operational Planning</td>
<td>Cyber Operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oversight &amp; Development</td>
<td>Legal Advice &amp; Advocacy</td>
<td>Strategic Planning &amp; Policy</td>
<td>Education &amp; Training</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Investigate</td>
<td>Investigation</td>
<td>Digital Forensics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Establishing National Standards**

**Knowledge, Skills, and Abilities (KSA)**

**Job**

**Task/Workrole**
Cyber Resiliency—Start Here

- 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

Educate or Train

Develop KSAs

Assess KSAs

Validate Competency

Globally-Recognized Cyber-Ready Professional
Recommended Role Aligned Certs

Network Technicians
- Novice
- Journeyman
- Master
  - CompTIA A+
  - Network+
  - Security+

Incident Responders
- Novice
- Journeyman
- Master
  - CSX P
  - CND
  - Advanced Incident Response

Advanced Incident Response
- CompTIA CASP

- Titan Rain Cybersecurity
Recommended Role Aligned Certs

Network Security Engineers

Novice
- CEH
- CCNA
- CCNA Security

Journeyman
- CHFI
- CCNP
- CCNP Security

Master
- CCIE
- CCSP
- CCSP Security

Forensics

Novice
- Fundamentals of Malware Analysis

Journeyman
- Network Forensics

Master
- Advanced Malware Analysis
Recommended Role Aligned Certs

Identification and Access Management

- Novice: CompTIA Network+, CompTIA Security+
- Journeyman: CompTIA CASP
- Master: Microsoft Certified Professional: Solutions Expert

Vulnerability Management (Pen Testing)

- Novice: CEH (Certified Ethical Hacker)
- Journeyman: EC-Council Certified Security Analyst, LPT MASTERCertified
- Master: Pen Testing & Network Exploitation, Advance Malware Analysis
Recommended Role Aligned Certs

**Compliance/Risk**
- Novice
  - CompTIA Security+
- Journeyman
  - CRISC
  - CGEIT
- Master
  - CISA

**Project Management/Leadership**
- Managers
  - PMI
  - CISSP
  - HCISPP
- Directors
  - CRISC
  - CISM
- Executives
  - CISO

Cybersecurity for Executives

Cybersecurity Risk for 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