Talent Management & Workforce Development

Building and Sustaining the Workforce

Learning Tree® International
Optimizing IT Workforce Performance

AFCEA
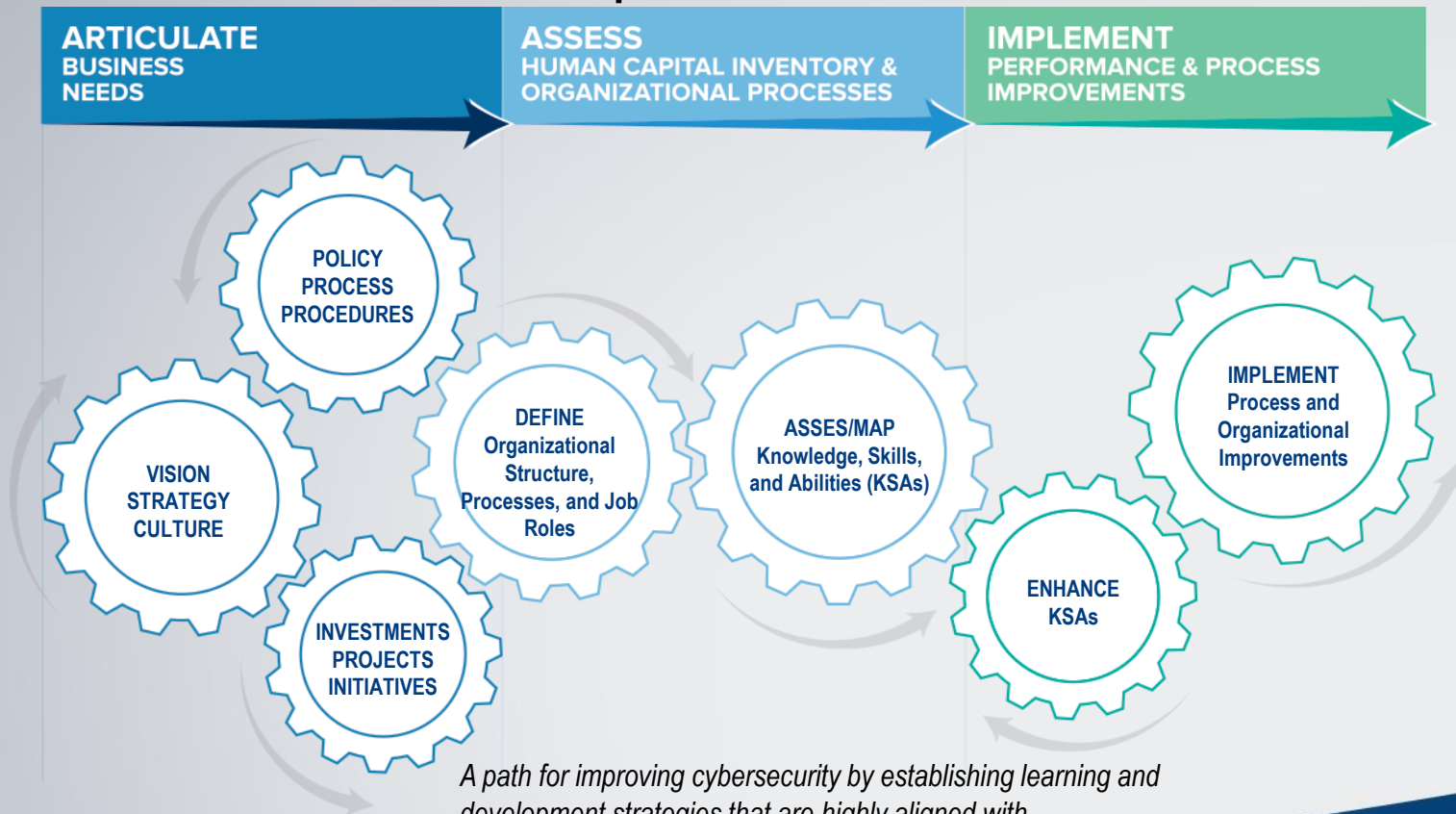Connecting people, ideas and solutions globally

CERTS 2019 AFCEA

Framing the Problem: *Trust & Cost*

➢ More Devices, Connections and Vulnerabilities are created each day…

➢ Cybercrime will cost the global community in excess of **$6T** annually by 2021 (Cybersecurity Ventures)

➢ Global spending on information security products / services will reach more than **$124B** in 2019 (Gartner)

➢ The avg. cost of a cyber attack is **$5M**, which includ**1.25M** for system downtime (Ponemon)
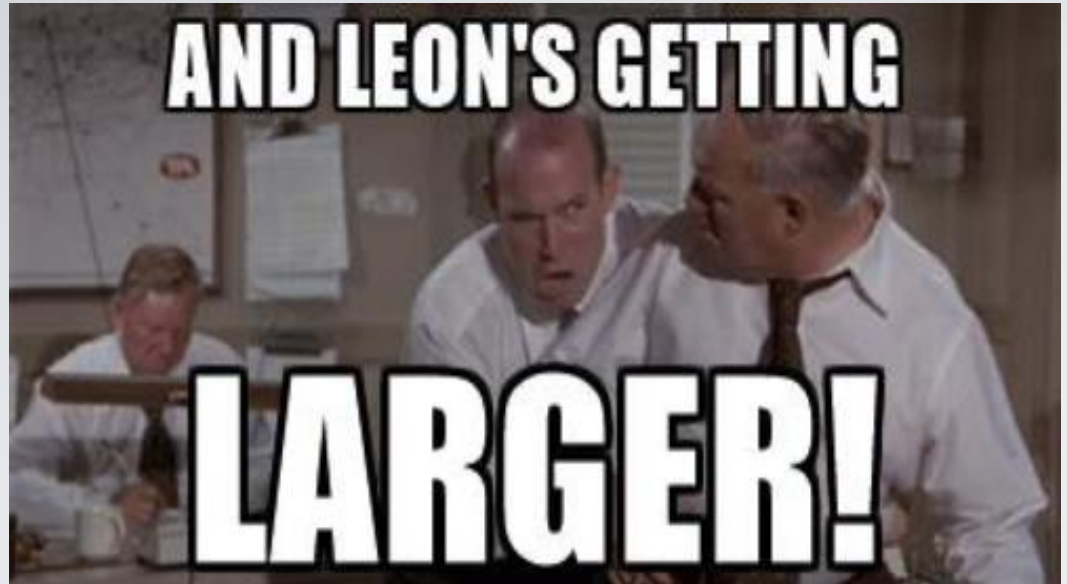
CYBER WORKFORCE OPTIMIZATION
Creating Alignment Between Organizational Needs, Human Capital & Performance

ARTICULATE BUSINESS NEEDS

ASSESS HUMAN CAPITAL INVENTORY & ORGANIZATIONAL PROCESSES

IMPLEMENT PERFORMANCE & PROCESS IMPROVEMENTS

- POLICY PROCESS PROCEDURES
- VISION STRATEGY CULTURE
- INVESTMENTS PROJECTS INITIATIVES
- DEFINE Organizational Structure, Processes, and Job Roles
- ASSES/MAP Knowledge, Skills, and Abilities (KSAs)
- ENHANCE KSAs
- IMPLEMENT Process and Organizational Improvements

A path for improving cybersecurity by establishing learning and development strategies that are highly aligned with organizational goals and objectives.

Our Challenge

PURPOSE: share in a relevant and interactive collaboration examining:

1.) *decisions creating organizational trust & agility*
2.) *actions fostering a problem-solving mindset*
3.) *efforts encouraging commitment and growth*

GOAL: capture and share portable ideas, actions and disciplines that are maturing cybersecurity acumen across an enterprise.

Focus of our Collaboration

Enabling *security responsibility* across the entire enterprise starts with *creating broad and relevant awareness*. Extending the responsibility of *system and data protection* outside of IT and into the primary department functions of an organization increases *threat awareness*, *institutional integrity* and *personal responsibility*. Achieving sustainable results in this action requires a formal commitment across all *People* in the organization, supported by *Process* and *Technology*.

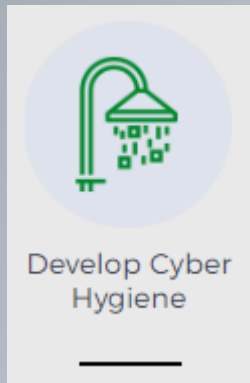|				
Develop Cyber Hygiene	Adopt NIST & NICE Cybersecurity Frameworks	Establish Risk Management Posture	Build a Multidisciplinary Program	Continuous Recruitment & Retention Process

Develop
Cyber Hygiene

The National Security Agency (**NSA**) identified Cyber Hygiene as a substantial priority for any organization, as several of the network and data breaches on record could have been prevented with basic cyber hygiene.

According to **Forbes**, cyber hygiene disciplines occur over **three phases – *planning, execution*** and ***check***. These disciplines include, but not limited to, hardening techniques, patching, network segmentation, security of both protocols and authentication credentials. This effort is a continuous process as adversaries are always innovating.

Adopt
NIST & NICE Cybersecurity
Framework

Adopt NIST & NICE Cybersecurity Frameworks

The National Institute of Standards and Technology (**NIST**) – an agency of the Department of Commerce – has released one of the most comprehensive, and widely adopted, frameworks that provides guidance in assessing organizational maturity across five functional areas for cybersecurity – ***Identify, Protect, Detect, Respond & Recover***.

Furthermore, the National Initiative for Cybersecurity Education (**NICE**) established a framework identifying common cybersecurity functions, specialty areas and job roles; highlighting the knowledge, skills and abilities to effectively protect organizational assets.

Establish
Risk Management Posture

Establish Risk Management Posture

The biggest risk to protecting information and information systems in modern business operations are untrained employees and corrupt inside actors. Modern cybersecurity strategies now employ an **enterprise-wide risk management posture** across the entire organization, rather than isolating this strategy within IT.

As part of this posture, organizational leaders continually consult with internal and external cybersecurity experts to review their human capital talent and **critical thinking capabilities**, **business processes**, **system design**, **access management** and the **policies** and **safeguards governing organizational assets**.

Build
Multidisciplinary Program

Build a
Multidisciplinary
Program

To combat the forces of threat actors attempting to penetrate your systems and steal your data, an organization must **create an adaptive environment** in which the workforce must no longer operate in silos, but rather as **multidisciplinary, agile teams**.

Job functions and the **roles associated** with them must be able to rapidly adjust for the variable influences on their responsibilities. Further, the workforce needs the **flexibility of rapidly developing and integrating new skills and capabilities**, as the cyber landscape continues to evolve.

Continuous Recruitment & Retention Process

Continuous Recruitment & Retention Process

Given the war for cyber talent, HR and Employee Development departments must establish a **revised and continuous strategy for attracting and retaining these key hires**. Department leaders must encourage more enterprise-wide adoption of security awareness to not overly burden dedicated security personnel.

Also, HR professionals must also seek individuals that have the **innate skills**, but not necessary the technical degrees, and develop those individuals to help address the **cyber skills gap**.

AFCEA
Connecting people, ideas and solutions globally

CERTS 2019

CYBERSECURITY
TRAINING FRAMEWORK

Contact Us Today

The complex nature of protecting your most critical data and data networks is supported by the introduction of the **National Initiative for Cybersecurity Education (NICE)** and the Learning Tree International aligned training framework. The NICE Framework – produced by the **National Initiative for Cybersecurity Careers and Studies (NICCS)** – has been developed to clearly identify unique categories, specialty areas, work roles and related knowledge, skills and abilities (KSAs) required to perform in any given area or cybersecurity work role. Learning Tree has developed and sourced a world class curriculum that is specifically aligned with the NICE Framework. Training offerings are certification-based and practitioner aligned ensuring your staff has the right skills for the right role at the right level.

Analyze

Investigate

Oversee & Govern

Securely Provision

Collect & Operate

Operate & Maintain

Protect & Defend

Cloud Security Certification

Learning Tree International

AFCEA
Connecting people, ideas and solutions globally

CERTS2019