# Cybersecurity – the Human Factor

**Prioritizing *People Solutions* to improve the cyber resiliency of the *Federal* workforce**

fissea

Federal Information Systems Security Educators' Association

AWARENESS • TRAINING • EDUCATION

HAVE YOU
**CONSIDERED AND ADDRESSED**
THE HUMAN FACTORS OF CYBER?

ARE YOUR PEOPLE
**TRAINED AND ENABLED**
TO IDENTIFY AND AVOID CYBER THREATS?

IS YOUR ORGANIZATION
**PROPERLY COORDINATED**
IN THE EVENT OF A CYBER ATTACK?

WOULD YOUR TEAM
**COMMUNICATE AND RESPOND**
TO CYBER INCIDENTS?

DOES YOUR WORKFORCE UNDERSTAND AND ADOPT
**KEY CYBERSECURIY BEST PRACTICES?**

ARE YOUR PEOPLE
**AWARE OF THEIR ROLES & RESPONSIBILITIES?**

ARE YOUR SECURITY TEAMS AS
**UNIFIED IN THEIR MISSION**
AS THE ATTACKERS ARE IN THEIRS?

# Today's Presenters

Emile Walker

Emile Walker is the Manager, Cybersecurity Awareness & Training at the U.S. Postal Service. Prior to this, Walker has had a broad range of cybersecurity experience including Information Systems Security Officer (ISSO), DoD CERT Incident Handler/Analyst, Unix/Linux Systems Administrator, Vulnerability Assessment Analyst, Site Security Reviewer, Websense Administrator and other related cybersecurity responsibilities.

Dave Witkowski

Dave Witkowski is a managing director at Deloitte Consulting LLP, advising federal IT executives on cybersecurity workforce strategy. Focusing on key issues in the cyber workforce such as the gap between talent demand and supply and the evolving nature of cyber threats. His expertise includes leadership assessment, workforce planning, training and awareness, competency modeling, hiring sourcing strategies, and organizational change management.

Sarah Benczik

Sarah Benczik is a Senior Manager at Deloitte Consulting LLP. She advises government leaders on people-focused strategy to improve mission and business results. Her recent work has focused on cybersecurity workforce planning and management, integrating talent management processes with employee engagement to improve employee experience, and designing organization and governance structures for cyber organizations.

Pilar Jarrin

Pilar Jarrin is a Manager at Deloitte Consulting LLP. Ms. Jarrin specializes in managing change in complex operational environments and currently leads teams at United States Postal Service (USPS) to drive stakeholder and leadership engagement efforts that enable cyber compliance, including Sarbanes Oxley (SOX), Payment Card Industry, and OIG audit compliance within the CIO environment.

It is no longer enough to create a secure infrastructure for information. Organizations must also address the *human factors* of cybersecurity by cultivating an informed and proactive workforce.

# The Human Factors of Cyber Risk

Cybersecurity is a growing problem in our new digital economy with the **cost of a data breach up 15%** over the last year.

| Major Cyber Risks | Root Cause |
|---|---|
| **$400 BIL** Estimated cost of cyber attacks on organizations globally | Organizations rarely invest in and plan for the **human component of cybersecurity** until **after** a breach has occurred. For major breaches, this can cost the organization **millions of dollars.** |
| **35%** of data breaches were attributed to human error or negligence | Types of cyber threats and methods of prevention change each day. Instilling a culture of cyber **interest** and **awareness** equips an organization to **better handle changing cybersecurity threats**. |
| **47%** of IT professionals describe collaboration between security risk management and business as poor or nonexistent | Many executives have the **mindset that cybersecurity is the responsibility of IT**; **rather it is everyone's responsibility**. Employee awareness should be the first line for **defense** of an organization's digital assets. |

Countering cyber threats requires a focus on ***people and behaviors***, not just technology.

# Key Strategies to Address the Human Factors Underlying Cyber Risk

## Human Factor Strategies

### Cyber Workforce Development

Build a cyber workforce, capable of rising up to the challenge of cybersecurity through recruiting and retaining efforts.

### Training & Awareness

Take a fresh look at information security training & awareness efforts; provide immersive learning opportunities to reinforce behavior change.

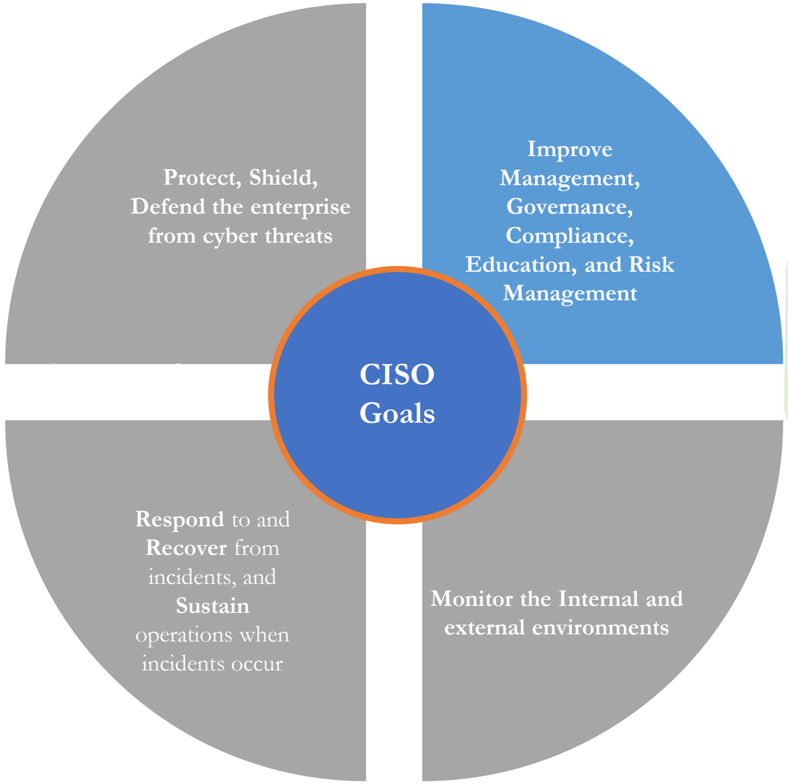
### Stakeholder & Leadership Engagement

Set up partnerships with leadership across organizations and ensure that leadership engage and support cybersecurity programs.

# Mitigating Cyber Risk through People Solutions

The USPS Chief Information Security Officer (CISO) organization strategically included people-focused programs into their enterprise-wide cybersecurity function.

## The Goals of a CISO Program



Protect, Shield, Defend the enterprise from cyber threats

Improve Management, Governance, Compliance, Education, and Risk Management

CISO Goals

**Respond** to and **Recover** from incidents, and **Sustain** operations when incidents occur

Monitor the Internal and external environments

## CISO People Programs

**Cyber Workforce:** Develop the strategy for predicting and managing their cyber workforce, focusing on key stages in employee's careers to help guide workforce development and to increase engagement and retention. hiring, onboarding, and training cyber experts and leaders.

**Governance:** Establish cybersecurity program governance, charting out roles & responsibilities for key groups and personnel.

**Training & Awareness:** Develop and provide cybersecurity training programs, awareness campaigns, and behavior change initatives for CISO personnel and impacted employees.

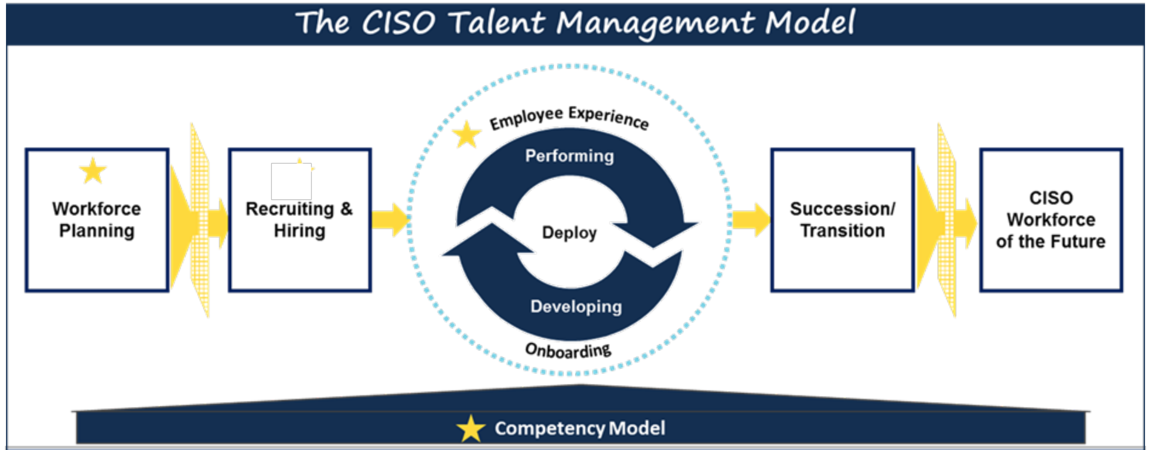
**Stakeholder and Leadership Engagement:** Engage and communicate with cross-organizational executives and impacted stakeholders to ensure the continuous prioritization of cybersecurity activities and efforts.

# Developing the Cyber Workforce

To address the cyber talent gap, USPS CISO created a ***cyber workforce development plan*** to recruit and develop strong performers both internal and external to the agency.

USPS CISO has a dedicated cyber initiative focused on CISO **workforce strategy and talent management**

The CISO Talent Management Model



CISO Talent Management focuses on stages in employees' careers to help guide workforce development and increase engagement and retention.

## *Current CISO Cyber Workforce Priorities:*

1) Development of a **Cyber Competency Model** based on the NICE framework, executive interviews, CISO Position Descriptions, HR processes, and stakeholder feedback. This serves as foundation for next steps like workforce skills assessments, performance goals, hiring strategies, and learning and development plans.
2) Development of a **Cyber Workforce Plan** to outline the short- and long-term talent needs to ensure the right number of people with the right skills are in the right jobs at the right time (through 2021).
3) Improving the **CISO employee experience** through a series of quarterly engagement sprints and beginning **Leadership Development** activities.

# Training for Cyber

USPS CISO's *Training & Awareness* program provides targeted role-based education to cyber professionals and trains the entire organizations' employees, suppliers, and customers on key cybersecurity best practices.

The USPS CISO **Awareness & Training** team launched an initiative to enhance information security awareness across the organization, using industry leading practices across key areas of engagement.

## *Program Objectives*

- Design and implement a strong cybersecurity awareness and training program to increase the organization's and the enterprise's ability to safeguard its information.
- Improve employee, supplier, and customer awareness of cyber threats and educate them on the key role they play in helping to protect against these threats.

## Key Engagement Areas

### Communications

- Enterprise-wide corporate communications

### Online Comms.

- Intranet online presence

### Training

- Awareness-level education
- Role-based training

### Anti-Phishing

- Monthly phishing tests to two groups of 15K
- Enhanced Anti-phishing education

### Creative

- Awareness videos
- Visual training aids
- Posters/Flyers/ Mailers

USPS CISO provides its employees - as well as its suppliers - with comprehensive information security ***awareness & training***, improving the overall ***cybersecurity posture*** of the enterprise.

# Aligning Stakeholders and Leadership Around Cyber

*Cybersecurity is everyone's responsibility*. Through its stakeholder engagement efforts, USPS CISO encourages collaboration with other business units, enabling the execution of interdependent programs and activities.

Through the development of its Strategic Initiative Support team, USPS CISO has stood-up a customized engagement plan for each key stakeholder group based on its priority level and the specific feedback provided in interviews.

## Stakeholder and Leadership Engagement Program:

- Builds on momentum around cybersecurity by continuously engaging organization personnel to address their cybersecurity needs.
- Improves communications and collaboration with stakeholders involved in cybersecurity activities, efforts, or programs.
- Identifies opportunities for improving CISO's ability to collaborate effectively organizational leadership.
- Executes targeted solutions to align CISO's objectives with the goals of other business units.

Effective stakeholder engagement is critical to USPS CISO's success, as its programs are. USPS CISO continually strives to execute programmatic efforts to engage personnel at the staff and executive levels.

Organizations must address the *human element* cybersecurity if they want to prepare and protect their organization from future cyber threats.

Questions?

# References

The following sources informed the preceding discussion of cybersecurity and talent:

http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/key-findings.html

https://www.kpmg.com/BE/en/IssuesAndInsights/ArticlesPublications/Documents/Harvey-Nash-CIO-survey-2015-new.pdf

http://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf

http://www2.deloitte.com/global/en/pages/risk/articles/Global-Cyber-Briefing.html

http://cybersecurityventures.com/cybersecurity-market-report/

http://www.securityweek.com/employees-not-following-policy-biggest-threat-endpoint-security-it-pros-say

http://cybersecurityventures.com/cost-per-breach/

http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy_2014.pdf

http://www.cgma.org/magazine/news/pages/cyber-security-talent-threats-201512263.aspx?TestCookiesEnabled=redirect

http://www-03.ibm.com/security/data-breach/