Building a Cyber Resilient Workforce

Texas Department of Information Resources

Information Security Forum 2023

Ioana V. Bazavan
Security Sr. Managing Director,
Accenture

2023 State CIO Top Ten Policy and Technology Priorities

Cybersecurity is the #1 Priority

STATE CIO TOP 10 PRIORITIES

Priority Strategies, Management Processes and Solutions for 2023

01 **Cybersecurity and Risk Management:** governance; budget and resource requirements; security frameworks; data protection; training and awareness; insider threats; third-party risk

02 **Digital Government / Digital Services:** framework for digital services; state portals; improving and digitizing citizen experience; accessibility; identity management; digital assistants; privacy

03 **Workforce:** preparing for the future workforce and reimagining the government workforce; transformation of knowledge, skills and experience; more defined roles for IT asset management, business relationship management, and service integration

04 **Legacy Modernization:** enhancing, renovating, replacing, legacy platforms and applications; business process improvement

05 **Identity and Access Management:** supporting citizen digital services; workforce access; access control; authentication; credentialing; digital standards

06 **Cloud Services:** cloud strategy; selection of service and deployment models; scalable and elastic services; governance; service management; security; privacy; procurement

07 **Consolidation/Optimization:** centralizing; consolidating services; operations; resources; infrastructure; data centers; communications and marketing "enterprise" thinking

08 **Data and Information Management:** data governance; data architecture; master data management; open data; sustained access to government data; data portals; enhancing the role of data; information and intelligence, knowledge management; data integration; data management strategy; roles and responsibilities; DataOps

09 **Broadband / Wireless Connectivity:** strengthening statewide connectivity; implementing rural broadband expansion; 5G deployment

10 **Customer Relationship Management:** internal customer service strategies; building customer agency confidence and trust; collaboration; service level agreements (demand planning)

STATE CIO TOP 10 PRIORITIES

Priority Technologies, Applications and Tools for 2023

01 **Identity and Access Management:** Identity proofing; multi-factor authentication

02 **Legacy Application Modernization/Renovation**

03 **Cloud Solutions:** selection of service and deployment models; cloud migration strategies; cloud architecture

04 **"X" as a Service:** software-as-a-service; infrastructure-as-a-service; platform-as-a-service

05 **Security Enhancement Tools:** CDM, advanced analytics, digital forensics

06 **Artificial Intelligence / Robotic Process Automation:** including chatbots, virtual assistants

07 **Data Analytics:** business intelligence and business analytics; applications; big data

08 **Low Code / No Code Software Development**

09 **Enterprise Resource Planning (ERP)**

10 **Business Process Integration Tools**

Source: State CIO Top Ten Policy and Technology Priorities for 2023

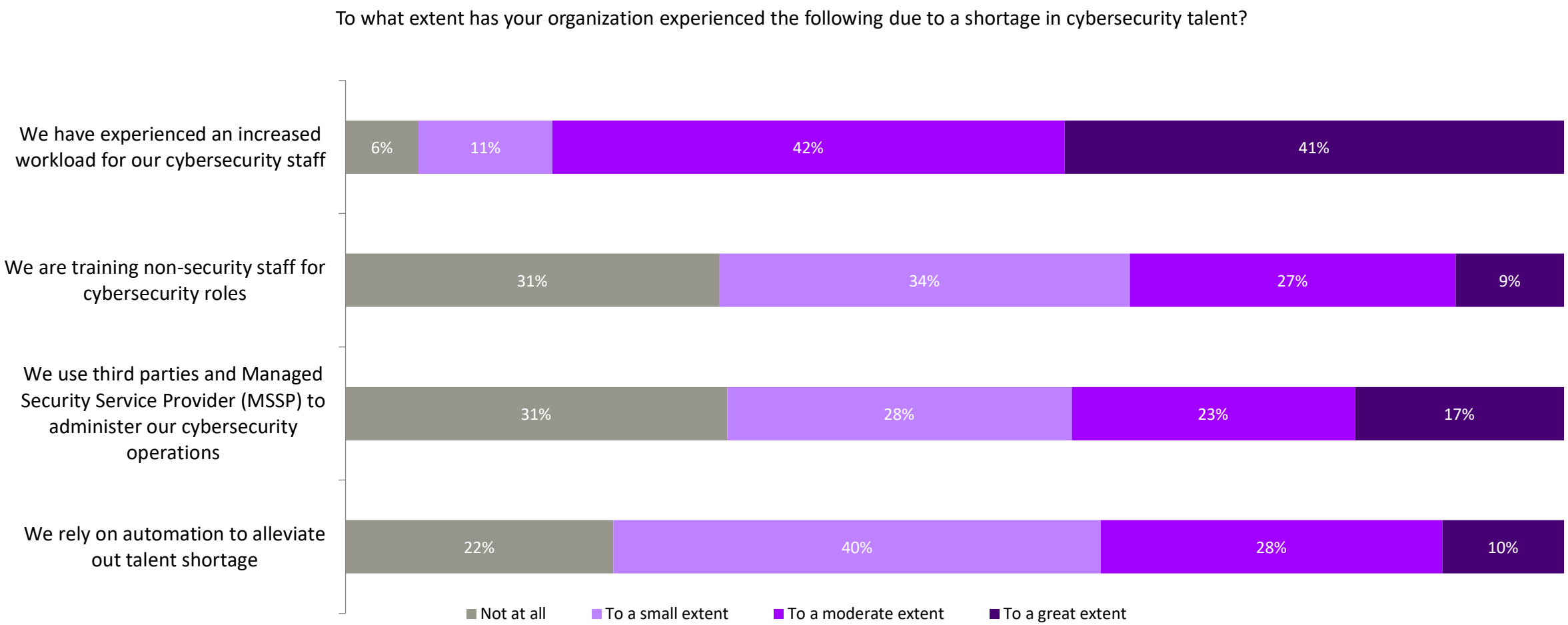
- The National Association of Chief Information Security Officers (NASCIO) conducts a survey of the state CIOs to identify and prioritize the top policy and technology issues facing state government
- The CIOs top ten priorities are identified and used as input to NASCIO's programs, planning for conference sessions, and publications
- **Workforce is the #3 Priority**

What we're hearing from clients across North America

State CISOs are vocalizing needs across the entire National Institute of Standards & Technology (NIST) cybersecurity lifecycle (i.e., Identify, protect, detect, respond, and recover). Key themes are:

1. **Cyber Strategy & Running the Cyber PMO**
2. **Cyber Workforce Strategy & Workforce Development**
3. **Cyber Governance Risk and Compliance**
4. **Cyber Detection, Incident Response and Recovery Services**
5. **Cloud, Platform, and Application Security**
6. **Managed Security Services**

41% of respondents feel they have experienced an increased workload for their staff due to shortage in cybersecurity talent



Source: 2023 NACo & Accenture - Research on Cybersecurity of County Governments

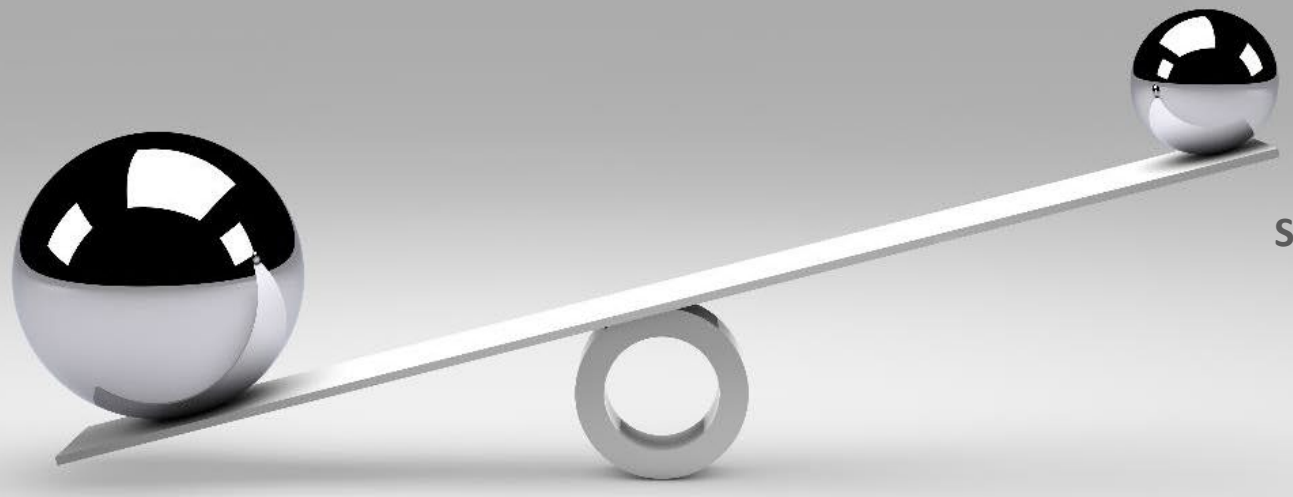
IN THE RACE FOR CYBER RESILIENCE, PEOPLE ARE AT THE CENTER

WHAT'S THE ANNUAL COST OF CYBER CRIME? $6 TRILLION IN 2021

ALL ORGANIZATIONS NEED TO **LEVEL THE PLAYING FIELD** AGAINST THREAT ACTORS BY **REDUCING HUMAN RISK** THROUGH **FUNDAMENTAL CULTURE CHANGE** AND TRANSFORMING EMPLOYEES INTO **CYBER CHAMPIONS**

INCIDENTS ATTRIBUTED TO HUMAN FALLIBILITY:

95%



SECURITY SPEND INVESTED IN THE HUMAN FIREWALL:

<5%

TODAY'S CULTURE	TOMORROW'S CULTURE
IT is responsible for cybersecurity	**EVERYONE** is responsible for cybersecurity
Only Executives have sensitive information that should be protected	**ALL Employees** have information that must be protected
Only businesses can be harmed by cyber threats	**ANYONE**, including families, friends, clients, and contractors can be affected by cyber threats

CYBER RESILIENCE BEGINS AND ENDS WITH OUR *PEOPLE*

ATTACKERS KNOW HOW TO EXPLOIT HUMAN FLAWS:

88% OF DATA BREACHES CAUSED BY EMPLOYEE NEGLIGENCE*

*Source: Stanford University and Tessian Security 2020 (The Psychology of Human Error)

BUILD A ‘HUMAN FIREWALL’ THROUGH A CYBERSECURITY PROGRAM THAT FOCUSES ON:

ENGAGEMENT

With **compelling content** that targets relevant threat scenarios to move beyond mere compliance.

ENABLEMENT

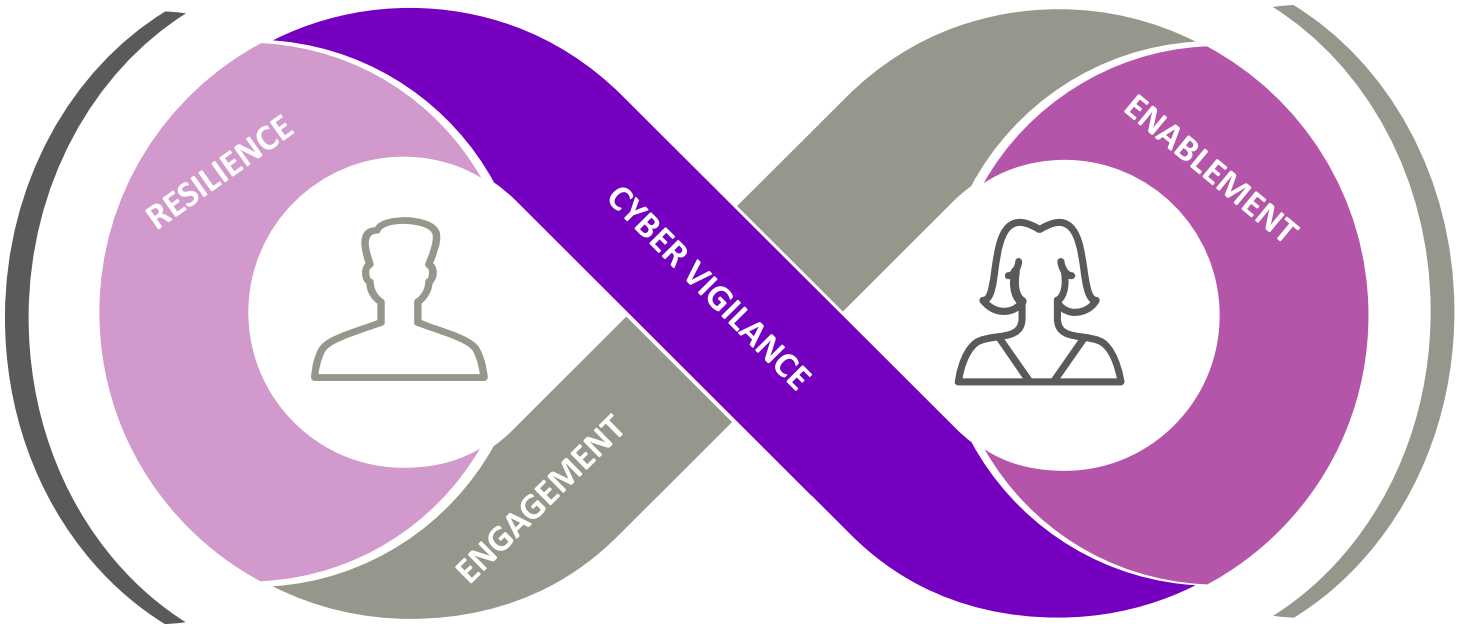
Converting knowledge and practice into behaviors that are embedded into ‘ways of working’ to reduce operational costs, penalties and breaches.

CYBER VIGILANCE

With **awareness and understanding** about role and industry specific threats that is backed by hands-on experience.

RESILIENCE

With a **security-embedded culture** that takes proactive steps in detecting and preventing suspicious incidents.



WHEN WE THINK ABOUT BUILDING A HUMAN FIREWALL, WE THINK ABOUT FIVE PILLARS:

1 CYBERSECURE BEHAVIORS AND CULTURE CHANGE

Transforming the enterprise wide culture and elevating capabilities to drive 'security first' ways of working with insights

- **Cyber Behaviors Assessment & Risk**
- **Behavior Change Program Transformation**
- **Managed Security Awareness & Training,** e.g., Phishing as-a-Service, & Off the shelf Digital Learning

2 CYBERSKILLS & SPECIALIZED LEARNING

Educating your Technology and Cybersecurity talent to become more responsive to threat

- Immersive learning w/ **Persona-based (technical audience)** learning paths design
- Upskilling for IT/ OT, Security, Developers
- **Orchestrated App Sec Training** & Vulnerability Management for Developers

3 CYBERSECURITY TALENT MANAGEMENT

Attracting, onboarding, developing and retaining top Cybersecurity Talent to your organization

- Cybersecurity **Workforce& Talent Strategy**
- **Operating Model and Org Design**, aligned to industry framework and future skills
- **Leadership Development** for Cyber and Business Leaders

4 HUMAN-CENTERED CHANGE FOR SECURITY IMPLEMENTATIONS

Supporting change for Security (Technology, Process) implementations, promoting adoption and embedding change

- Organizational Change Management (OCM) for **Digital Identity, Cloud, IRM, & Compliance Programs**
- Mobilization and Governance

5 MEASURE & ASSESS

Elevate Security

IMMERSIVELABS

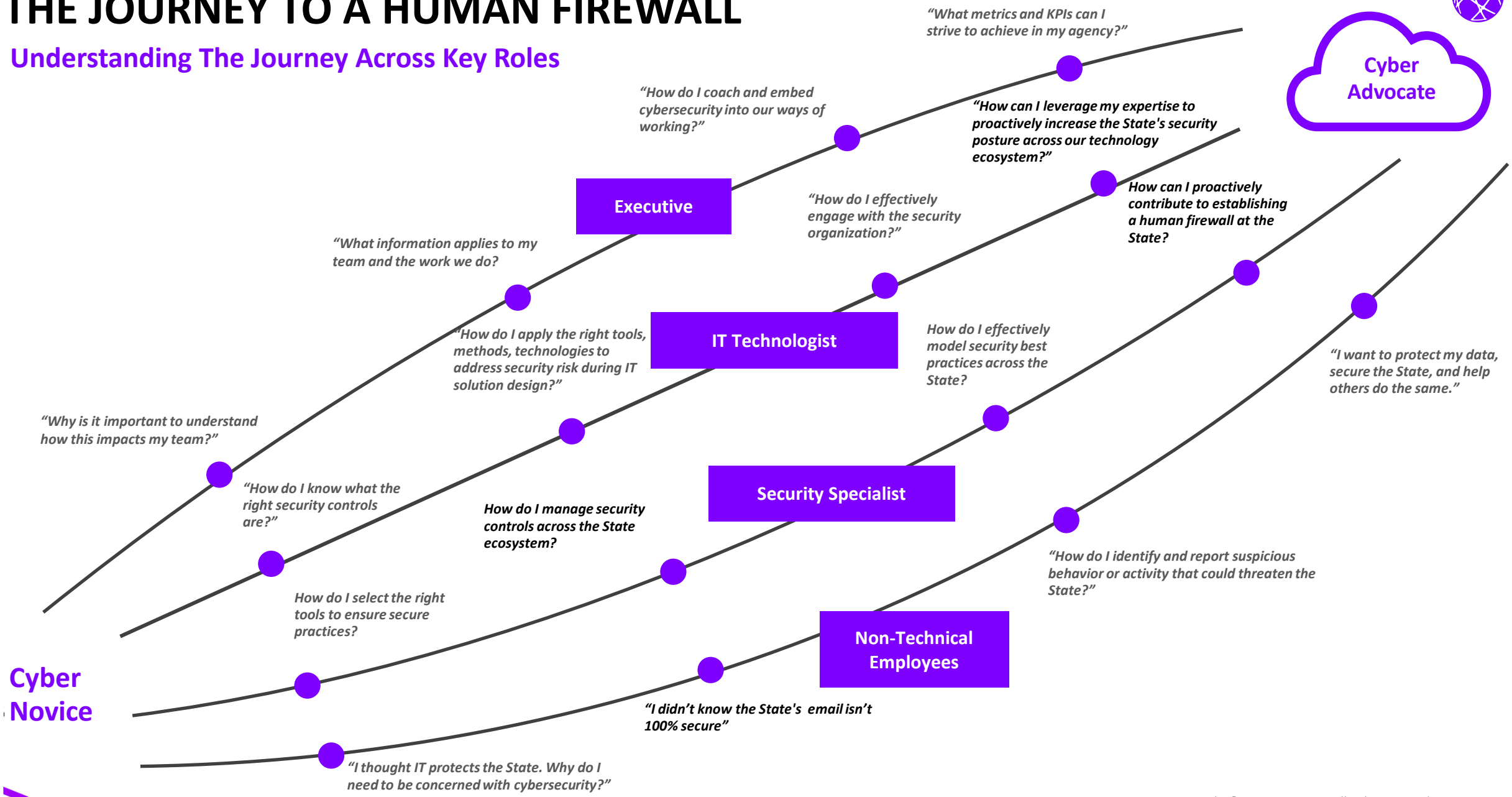
TRANSFORMATION GPS 2.0

Build and Transform Services

Managed Services

THE JOURNEY TO A HUMAN FIREWALL

Understanding The Journey Across Key Roles



EFFECTIVE CYBERSECURITY TRAINING & AWARENESS
70-20-10 MODEL FOR LEARNING

We recommend a proven, 70-20-10 model when delivering cybersecurity training and awareness programs across 3 key stages: **Foundational, Focused,** and **Role-based training**

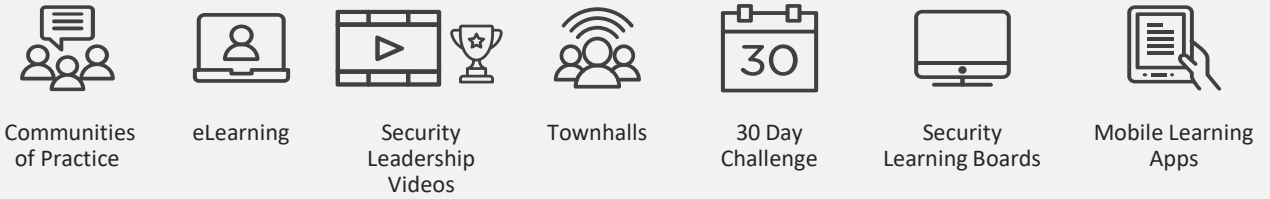
STAGE 1
FOUNDATIONAL
- General Users
- Agency Leadership

STAGE 2
FOCUSED
- Security Operations
- Threat Hunt
- Risk Management

STAGE 3
ROLE BASED
- Privileged Users
- Authorizing Officials
- ISSOs

Learning All The Time- 70%

Embed security learning into day-to-day experience to promote adoption, build community, and practice new behaviors.



Communities of Practice | eLearning | Security Leadership Videos | Townhalls | 30 Day Challenge | Security Learning Boards | Mobile Learning Apps

Learning From Others- 20%

Encourage collaboration and relationship building to reinforce learning.

Workplace Collaboration Board | Security Conferences | "Share Your Story" Contest | Partnering with Our Vendors

Formal Training- 10%

Embrace high-touch, hands-on learning for new skill building.

Virtual Classroom | Lunch & Learns | Instructor-Led Sessions | Speaker Series

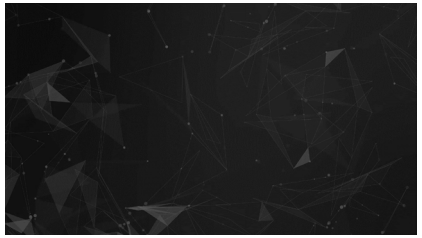
ILLUSTRATIVE CYBERSECURITY PROGRAM OUTPUTS

KEY OUTCOMES

- ✓ Cybersecurity Program Strategy & Execution Plan
- ✓ High-level Stakeholder Analysis
- ✓ Cybersecurity Champion Network
- ✓ Cybersecurity Learning & Awareness Package
- ✓ Cybersecurity Program Brand Identity
- ✓ Behavior Change Measurement Approach & Interventions

SAMPLE CYBERSECURITY LEARNING & AWARENESS ITEMS

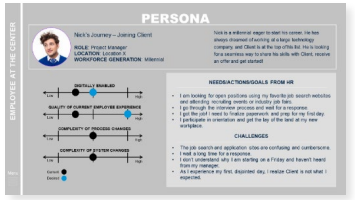
Infographics



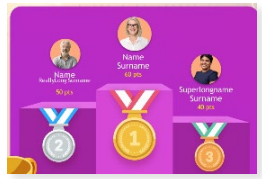
Bite-sized Videos

Digital Postcards

Digital Posters



Persona + Journey Map



Recognition Templates

Digital Newsletters

Key Takeaways
Building a Cyber Resilient Workforce

- The growing cybersecurity talent shortage is real and will not be resolved anytime soon
- Our people are the foundation for cyber resilience
- Security training and awareness decreases the workload on dedicated security experts
- Cybersecurity talent management is essential for developing an effective junior workforce
- Building a comprehensive training program is a significant operational undertaking

Thank You

For additional information, please reach out to Ioana V. Bazavan or Michele Myauo:

ioana.v.bazavan@accenture.com

michele.lynn.myauo@accenture.com