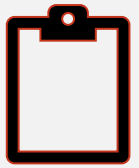
MHEC SECURITY SERVICES SERIES WEBINAR:

Building a Culture of Information Security

April 12, 2022

Resources available on the MHEC website post-event.

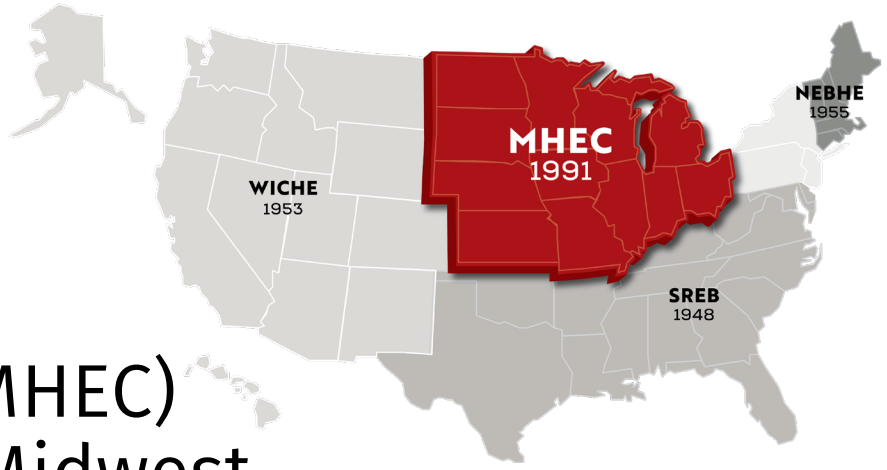
Submit questions in the Q&A.



Please complete our survey.

MIDWESTERN HIGHER EDUCATION COMPACT

About MHEC



- Midwestern Higher Education Compact (MHEC) was legislatively created and serves the Midwest census region (12 states)
- One of four regional higher education compacts (MHEC, WICHE, SREB, NEBHE)
- MHEC offers programs for post-secondary education institutions in areas such as property insurance, student health, military credit, open educational resources, research, policy analysis, and technology.

MIDWESTERN HIGHER EDUCATION COMPACT

MHEC Technologies Community

Contact: Deb Kidwell
Dir of Technology Initiatives
612-677-2770
debk@mhec.org

- Engages IT innovators and specialists from services areas for technology, academia, students, and administration
- Provides strategic guidance to MHEC on technology-related topics in support of the mission of higher education institutions, and helps identify opportunities for contracts to serve higher education needs
- Learn more about the MHEC Technologies Community: MHEC.org/policy-research/technologies

MIDWESTERN HIGHER EDUCATION COMPACT

MHEC Technology Contracts

Contact: Nathan Sorensen
Dir of Govt Contracts
(612) 677-2767
nathans@mhec.org

- Sustain and advance affordable, high-quality educational opportunities through cost-savings initiatives
- Known and used by higher education IT and procurement offices
- Encompasses contracts that might not traditionally be considered 'technology'
- Learn more about MHEC Contracts: MHEC.org/contracts

MIDWESTERN HIGHER EDUCATION COMPACT

MHEC SECURITY SERVICES WEBINAR SERIES:

- January 26, 2022: *Improving Your Cybersecurity Posture*
- February 14, 2022: *Educator's Guide to Outsmarting the Puppet Master*
- March 16, 2022: *Ransomware Trends: The Evolution of the Threat*
- **April 12, 2022: *Building a Culture of Information Security***
  - Presented in partnership with BerryDunn
  - MHEC Contract #MHEC-06042021-BD
    - Consulting Services
    - Competitively bid solicitation
    - Available to all higher education institutions within the MHEC region, both public and private not-for-profit

MIDWESTERN HIGHER EDUCATION COMPACT

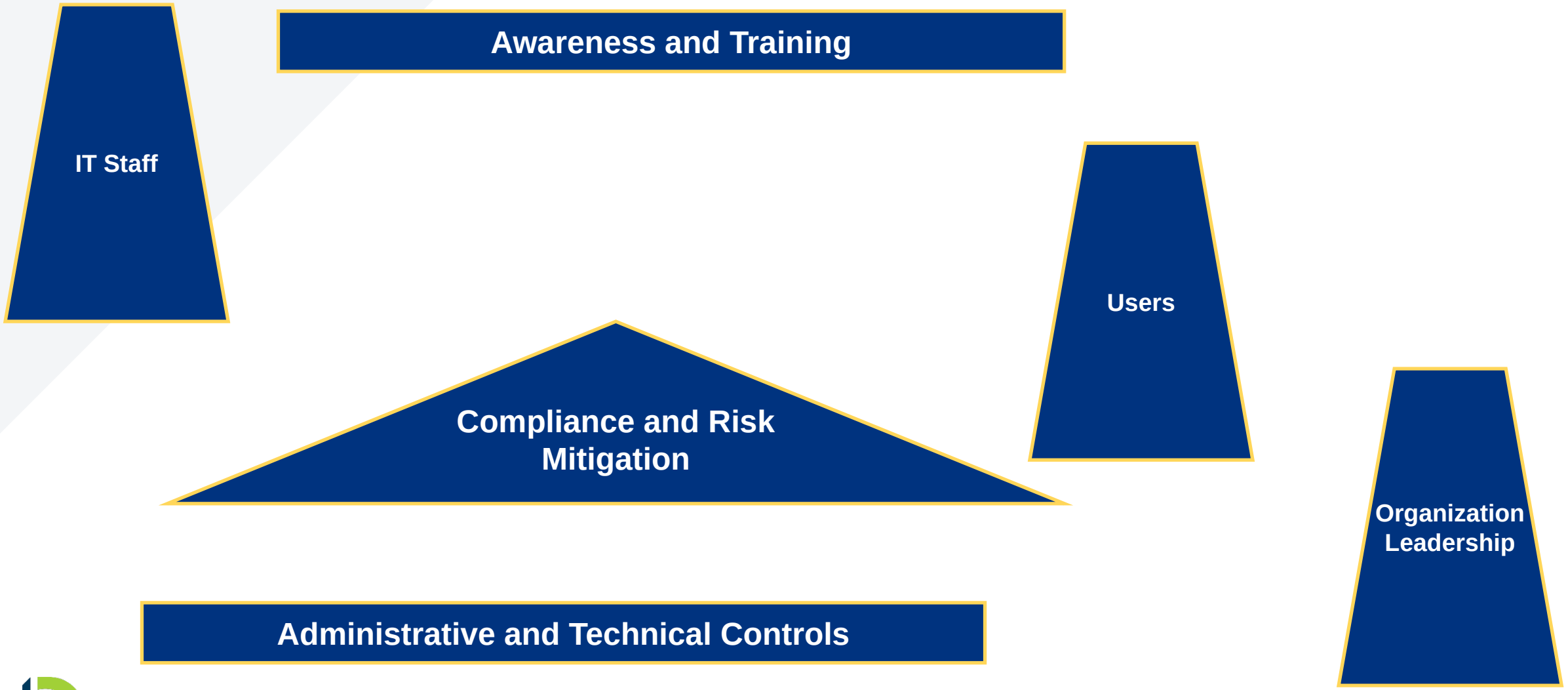
Building a Culture of Information Security

Joe Traino, Brian Hadley, Vienna Morrill, Tyler Bartlett

BerryDunn

April 12, 2022

What does a culture of information security look like?



Agenda

1. Selecting Standards
2. Assessing Risk
3. The Importance of Wellbeing

1

Selecting Standards

Cybersecurity Frameworks

- National Institute of Standards and Technology (NIST)
  - CSF, 800-53, 800-171
- International Standards Organization (ISO)
  - 27000, HEISC
- Center for Information Security (CIS)
- Cybersecurity Maturity Model Certification (CMMC)

Polling Question #1

Customization

- NIST
  - Security Assurance Level
- ISO
  - 27002 Clause 5 through 18 controls
- CIS
  - Implementation Group
- CMMC
  - Level

Function	Category	Subcategory	Relevant Control Mappings[2]
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	• CCS CSC 4 • COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 • ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 • ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.316(b)(2)(iii)

DHHS Office for Civil Rights | *HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework*

Security Awareness Training

Awareness and Training

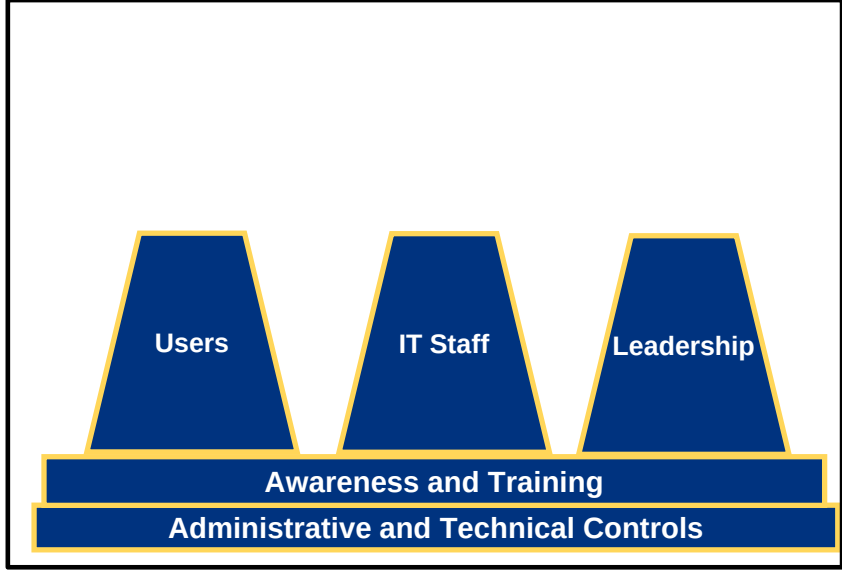
Administrative and Technical Controls

2

Assessing Risk

Assessments

- Internal
  - Annually
- External
  - Periodically to verify the results of internal assessments



Polling Question #2

Example Assessment Outcomes

NIST SP800-53 R4 CA-6	Security Assessment and Authorization/ Security Authorization	Risk level: Moderate
Findings: (1) [redacted] systems are not authorized before being placed into operations, nor on a defined frequency, nor when significant changes occur. (2) A [redacted] senior official does not sign and approve the security accreditation. (3) The security authorization is not updated on a defined frequency.		
Recommendations: Before being entered into a production environment, [redacted] systems should be put through an accreditation process to verify the functionality of the system and its security controls/features. The [redacted] should designate a senior official to sign and approve these security accreditations, authorizing entry to the production environment. The [redacted] should review and annually update these authorizations.		
Standard: The organization: a. Assigns a senior-level executive or manager as the authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization [Assignment: organization-defined frequency].		

Example Assessment Outcomes

Table 1: Priority CIS Control Compliance

✓ Fully compliant − Partially compliant ✗ Not compliant

IG 1 Sub-Controls	IG 2 Sub-Controls	IG 3 Sub-Controls

Control 6 Maintenance, Monitoring, & Analysis of Audit Logs		Control 12 Boundary Defense		Control 17 Implement a Security Awareness Training Program		Control 20 Penetration Testing & Red Team Exercises	
6.1	Utilize Three Synchronized Time Sources ✓	12.1	Maintain an Inventory of Network Boundaries −	17.1	Perform a Skills Gap Analysis ✓	20.1	Establish a Penetration Testing Program −
6.2	Activate Audit Logging −	12.2	Scan for Unauthorized Connections across Trusted Network Boundaries ✓	17.2	Deliver Training to Fill the Skills Gap ✓	20.2	Conduct Regular External and Internal Penetration Tests −
6.3	Enabled Detailed Logging ✓	12.3	Deny Communications with Known Malicious IP Addresses ✓	17.3	Implement a Security Awareness Program ✓	20.3	Perform Periodic Red Team Exercises ✗
6.4	Ensure adequate storage for logs ✓	12.4	Deny Communication over Unauthorized Ports −	17.4	Update Awareness Content Frequently ✓	20.4	Include Tests for Presence of Unprotected System Information and Artifacts ✗
6.5	Central Log Management ✓	12.5	Configure Monitoring Systems to Record Network Packets −	17.5	Train Workforce on Secure Authentication ✓	20.5	Create Test Bed for Elements Not Typically Tested in Production ✗
6.6	Deploy SIEM or Log Analytic tool ✓	12.6	Deploy Network-Based IDS Sensors −	17.6	Train Workforce on Identifying Social Engineering Attacks ✓	20.6	Use Vulnerability Scanning and Penetration Testing Tools in Concert ✓
6.7	Regularly Review Logs ✓	12.7	Deploy Network-Based Intrusion Prevention Systems −	17.7	Train Workforce on Sensitive Data Handling ✓	20.7	Ensure Results are Documented Using Open Standards ✗
6.8	Regularly Tune SIEM ✓	12.8	Deploy NetFlow Collection on Networking Boundary Devices −	17.8	Train Workforce on Causes of Unintentional Data Exposure ✓	20.8	Control and Monitor Accounts Associated with Penetration Testing ✗
		12.9	Deploy Application Layer Filtering Proxy Server −	17.9	Train Workforce on Identifying and Reporting Incidents ✓		
		12.10	Decrypt Network Traffic at Proxy ✗				
		12.11	Require All Remote Login to Use Multi-Factor Authentication −				
		12.12	Manage All Devices Remotely Logging into Internal Network −				

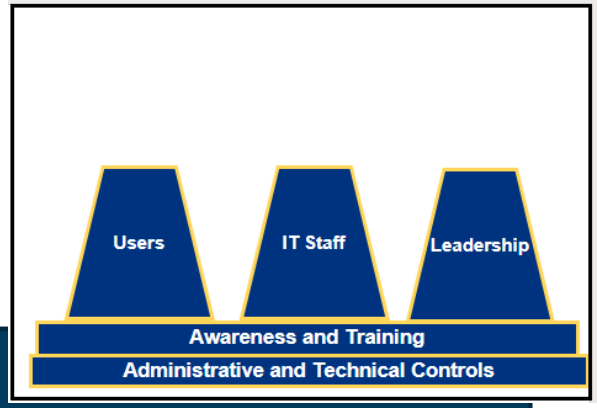
Example Assessment Outcomes

Implement Security Control			
Question Identifier:			
Question Text:			
Importance:	High	Resolution Date:	30-Apr-2022
Issue:	System X is not adequately protected		
Impacts:	Business processes A, B, C would be impacted if the system is down		
Recommendations:	Develop security control, test security control, implement security control		
Vulnerabilities:	System X is vulnerable to Attack Y		
Contacts:	John Doe		

3

The Importance of Well-being

What does well-being have to do with Information Security?



Well-being Defined

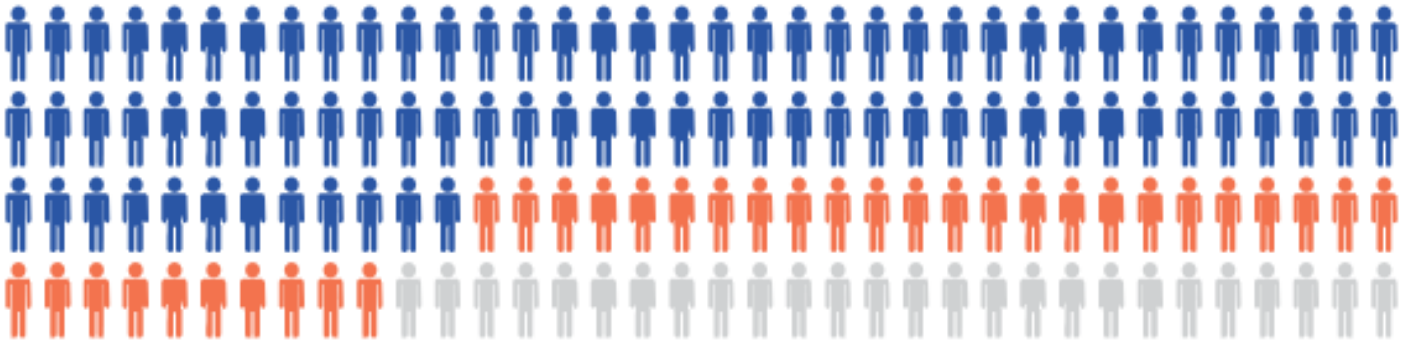
What you think and feel about your life; often influenced by a variety of factors including physical and mental health, social connectedness, financial wellness, and vocational satisfaction.

- Chronically low well-being can lead to disengagement and burnout.
- When people are disengaged and burned out... threats may go unnoticed, good security practices may slip, important steps may get left out, important communication may break down.

Polling Questions #3 and #4

“Unwell” users present challenges

Contributing Factors
- Fatigue
- Burn out
- Disengagement
- Distraction



The negligent insider is the root cause of most incidents.

A total of 3,807 attacks, or 56%, were caused by employee or contractor negligence, costing on average $484,931 per incident. This could be the result of a variety of factors, including not ensuring their devices are secured, not following the company's security policy, or forgetting to patch and upgrade.

Malicious insiders caused 26% or 1,749 incidents at an average cost per incident of $648,062.

Malicious insiders are employees or authorized individuals who use their data access for harmful, unethical or illegal activities. Because employees are increasingly granted access to more information to enhance productivity in today's work-from-anywhere workforce, malicious insiders are harder to detect than external attackers or hackers.

Source: 2022 Cost of Insider Threats Summary Report, Ponemon Institute

Contributing Factors
- Financial Distress
- Interpersonal Conflicts
- Distrust
- Feeling Unappreciated
- Lack of Belonging


Culture of Well-being
Programs ▪ Resources ▪ Benefits
Physical
Self-care is good and valuable
Mental
It's okay to not be okay
Career
Purpose drives growth
Financial
Transform hard work to goals
Social
You belong
Work Environment
Leadership sponsorship
Positive teams
Flexibility
Manager engagement
Built environment

Two Angles

IT Staff

- The individuals we rely on to identify, assess, respond to, and manage security risks.

Users

- The individuals we rely on to adhere to security policies and procedures.
- The individuals we rely on to identify and communicate threats.

Stress, Burnout, and Overall Well-being

- 80% of cybersecurity personnel said they're dealing with more stress in the wake of the pandemic than before it. (ITProPortal)
- 25% of CISOs said that their job has affected their mental and/or physical health. (CyberScoop)
- 65% of pros are thinking about leaving cybersecurity due to work-related stress. (Beta News)

https://blogs.cisco.com/security/mental-health-burnout-in-cybersecurity-tips-stories-and-insights

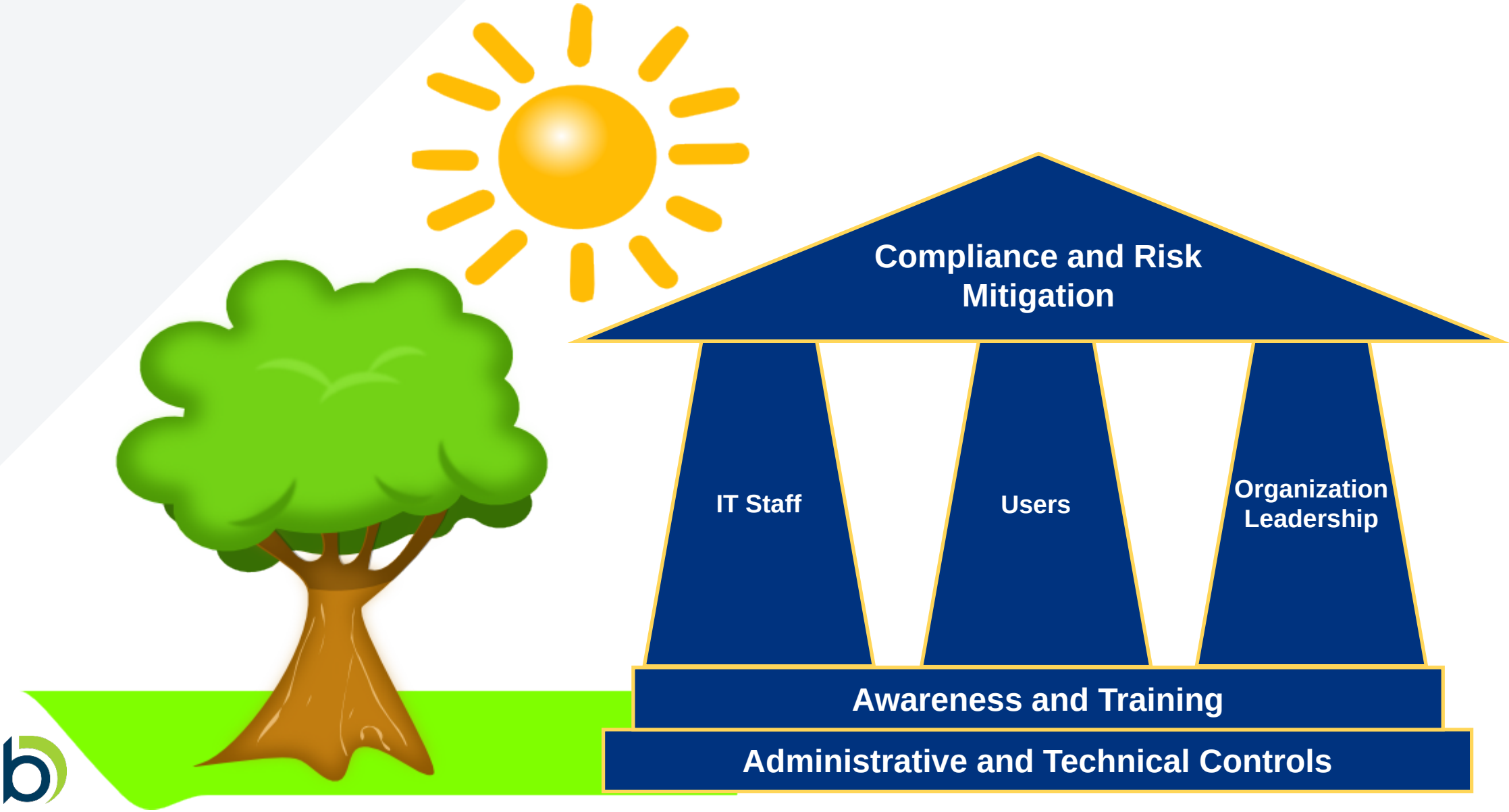
Supporting the Well-being of IT Personnel

- Set the tone with IT Leaders and Managers
- Meet people where they are at (use tools like surveys, facilitated team discussions)
- Understand and promote the programs, resources, and benefits available to your teams.
- Emphasize culture.
- Reduce Stressors. Ask employees. Are there opportunities to improve?
- Appreciate the value of retaining great people.

How IT Can Support the Well-being of Users

- Elevate the well-being discussion with the leadership team.
- Make the connection between well-being and enterprise risk.
- Consider well-being when planning IT changes and projects:
  - How does this change influence the well-being of users?
  - How might users react to this information?
  - How can we make information security, and technology in general, feel less "stressful?“
- Support research, planning, and implementation of well-being-related technology solutions

What does a culture of information security look like?



About BerryDunn

47
Years in Business

30+
Years of Advisory Services

145+
Colleges, Universities, and Systems

- Mature methodology
- Successful track record
- Focused on value

- Risk management programs
- IS maturity assessments
- Information security (IS) assessments
- HIPAA, NIST, GLBA and other compliance authority assessments
- Policy, program and procedure development
- Training and education

OBJECTIVE AND INDEPENDENT

97% Client satisfaction rating

Thank you

Joe Traino
jtraino@berrydunn.com

Brian Hadley
bhadley@berrydunn.com

Vienna Morrill
vmorrill@berrydunn.com

Tyler Bartlett
tbartlett@berrydunn.com

berrydunn.com