# Current Hot Topics in Risk Management

## Steven C. Holland
## Chief Risk Officer
## University of Arizona

*WACUBO-BMI 2019 – Track 3*

# *SELECTED HOT TOPICS FOR TODAY*

- *International Activity*

- *Protection of Minors*

- *Cyber Risk Exposure*

# Our Primary Areas of Risk

# *OTHER HOT TOPICS – FIELDER'S CHOICE*

- *Campus Speech and Climate Issues*
- *Foreign Student Tuition Revenue Loss*
- *Title IX Compliance*
- *Concussion/Traumatic Brain Injury*
- *Alcohol Service at Campus Events*
- *Student Organizations*
- *Intercollegiate Athletics/Sports Clubs*
- *Environmental Compliance*
- *Fleet Operations*
- *Deferred Maintenance*
- *Construction and Renovation*

## INTERNATIONAL TRAVEL – RISK SCENARIO

*A week-long academic field trip was arranged to visit Peru. One faculty member traveled with five students. One of the female students complained of severe abdominal pain, and was taken to a local hospital for evaluation, and was admitted for observation. The faculty member left her at the hospital to continue the itinerary with the remaining students to the next city.*

*While in the hospital, a surgical procedure was performed to remove the student's appendix. It was later determined that the surgery was not necessary. Also, while under anesthesia, the student was sexually assaulted by an unknown person or persons.*

*Key Issues*

- *Traveler Safety and Health*

- *Student Travel versus Faculty/Staff Travel*

- *Insurance Coverage and Emergency Management*

- *Traveler Tracking and Communication*

- *Hazardous Destinations*

- *Travel as an Revenue Source (running tours)*

*FY 18-19 International Travel Data*

*Faculty/Staff Travel:*     *3,457 trips*
        *114 countries*
        *54,182 person days abroad*

*Top Five Destinations in Order:*
*Mexico, Canada, China, United Kingdom, France*

*Student Travel:*     *1,100 registered for Study Abroad*
        *> 200 programs offered through SASE*
        *40-50 faculty led trips per year*
        *Independent Study Travel*

## *Traveler Safety and Health*

- *Transportation Risks – number one source of injury abroad*
  - *rental and private cars, buses, taxi-cabs, rail, air, boat, charter services*

- *Victim of Crime – property theft, corruption, assault, kidnapping*

- *Lodging Choices – selection process, fire safety, security*

- *Communications – international cell phone, wellness check-in*

- *Emergencies – medical, natural disaster, political unrest*

- *Medical Insurance – coverage limitations, family members*

## *Considerations for Student Travel*

- *Vetting of study abroad programs and program providers*

- *Challenges and benefits with international partners*

- *Planning requirements for faculty led programs – Training!!!*

- *Policy regarding excursions from program location/activity*

- *Mental health issues – medication, treatment, self-harm*

- *Sexual assault and harassment:*
  - *Title IX implications, local law enforcement deficiencies, internal vs. external, privacy, student code of conduct, judicial process, departure from program.*

- *Being arrested or detained for drugs or other legal problems*

When you're down by the sea and an eel bites your knee

That's a Moray
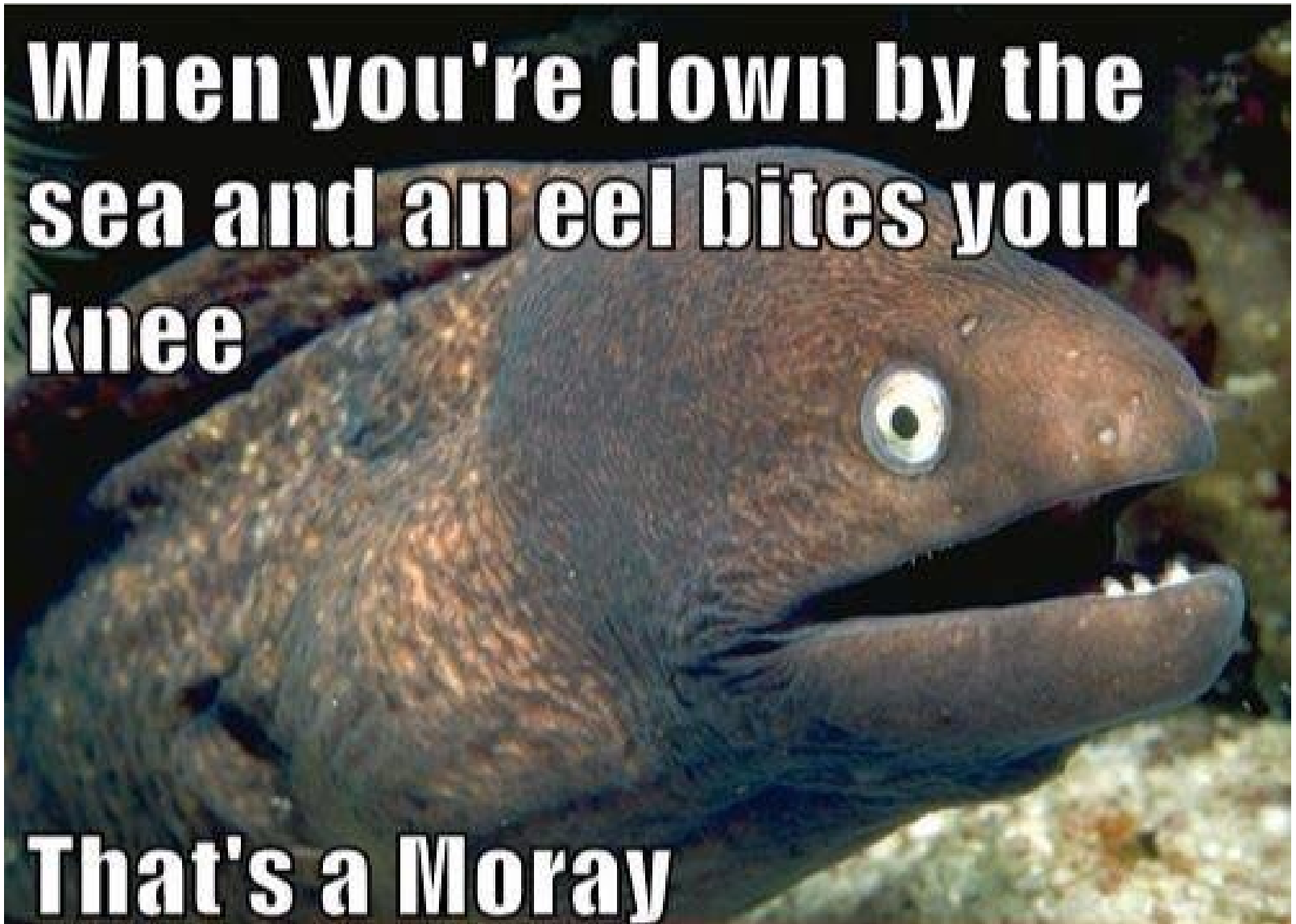
## *Insurance Coverage and Assistance Services*

- *International insurance programs – scope of medical coverage, general and professional liability, auto, traveler assistance, emergency evacuation – medical vs political vs disaster.*

- *Is medical coverage for work related injury only (i.e. worker's compensation) or full medical care?  Traveler usually responsible for existing conditions, prescriptions, etc.*

- *Employee coverage often different from student coverage – consider requiring that faculty led student trips all have the same insurance provider – try to avoid the bus accident scenario with multiple victims and multiple insurance providers.*

- *Specialty Coverages:  Defense Base Act, Kidnap/Ransom*

- *Check coverage exclusions for countries under economic sanction, war zones, in-country citizenship.*

## *Emergency Evacuation and Security Issues*

- *Included in travel assistance programs, but check limitations*

- *Typically requires advance notice and approval from carrier*

- *Medical evacuation may not be to US, but to nearest competent medical treatment location.*

- *Political unrest evacuation MAY be included, but may have high triggers for coverage to kick in, or be with a separate carrier.*

- *Natural disaster evacuation is usually excluded!  This is a significant potential coverage gap.*

- *Kidnap and Ransom coverage will be a separate carrier, and must be kept confidential.  Need to authorize key internal officials who can request coverage and trigger response assistance.*

## *Traveler Tracking*

- *Duty of Care – knowing where your people are, being able to communicate with them, and connect them to needed services.*

- *Registration Systems – itinerary details, collect online with external software or internal systems.  Critical when you have travelers from multiple units in an area when crisis arises.*

- *Combining travel registration with authorization or reimbursement*

- *Tracking services may be available from insurance provider.*

- *Consider requiring STEP registration:* https://step.state.gov/step/

- *Traveler profile, emergency contacts domestic and abroad.*

## *Travel to Hazardous Destinations*

- *Define hazard levels that trigger additional review/approval*
  - *US State Department warnings and alerts*
  - *https://travel.state.gov/content/travel/en/international-travel.html*
  - *Consider ranking hazardous locations – elevated, high, or extreme risk*

- *Expectations for traveler competency, training needs, local resources*

- *Policy scope - applicable to students only, faculty/staff, or everyone traveling under university program or business?*

- *Export Control – federal licensing, ITAR, EAR, OFAC regulations*

- *Don't forget health hazards – http://wwwnc.cdc.gov/travel/*

- *Evaluate insurance coverage exclusions for war zones, areas of political instability, and countries under US government sanction.*

## PROGRAMS FOR MINORS – RISK SCENARIO

*A summer volleyball camp for high school kids is held in a large athletics complex that includes courts, weight training facilities, offices, and an aquatics center.  Participants are housed in a nearby residence hall.*

*After organized events end for the day, participants are allowed to use the courts on their own to practice their volleyball skills.  Several players sneak into the aquatics center, and dare each other to jump into the pool from the 10 meter platform.  While horsing around on the platform, one of the players is knocked off balance, and falls to the pool deck below, where he suffers fatal injuries.*

# PROTECTING MINORS AND OTHER VULNERABLE POPULATIONS

- *Inventory of programs that work with children – you will be surprised how many you have*

- *Program design and management requirements, minimum staffing, participant safety, transportation, medical emergencies*

- *Training of employees, students, volunteers*

- *Review of statutory reporting obligations*

- *Background screening of workers*

- *Requirements for outside users of facilities, worker screening, insurance and indemnification, operational requirements, facility use agreement*

## *Types of Programs Serving Minors*

- *4-H Youth Programs – wide variety, tons of volunteers*

- *Camps – science, computer, music, art, sports, recreation*

- *Athletic Coach Camps – facility use, can be residential*

- *Music instruction – individual instruction, private rehearsal rooms*

- *Campus facilities and events open to the public*

- *Off-campus groups bringing minors to campus (school groups)*

# *Often Overlooked Programs Serving Minors*

- *Internships/Externships*

- *High School Honors Programs*

- *Mentoring programs*

- *Community service activities (staff and/or students)*

- *Student/Greek Organization sponsored programs/events*

- *Partnerships with local K-12 schools*

- *Overnight Admissions visits*

- *Tutoring/babysitting on campus*

## *Survey to Identify Existing Programs Serving Minors*

*Before you start – consider the following:*

1. *Clearly define who is a "minor" under policy – such as….*
   - *Under age of majority but matriculated (Doogie Howser, MD)*
   - *Dually enrolled high school students*
   - *Employed by the college or university*

2. *Specify what will be considered "a program"*
   - *What about 3rd party programs held in campus facilities?  Does the policy apply to them?  How will it be enforced?*

## *Survey to Identify Existing Programs Serving Minors*

- *Programs may have been in existence for many years with excellent track record and no problems – but may not be operated in accordance with best practices.*

- *A registration system that tracks program activities and locations at any given time is critical, especially in the event of an emergency that requires connecting kids with parents.*
  *UA Link:  https://youthsafety.arizona.edu/university-sponsored-youth-program-registration*

- *Programs with national affiliations (i.e. 4-H) often have well developed procedures and training, but still need to be consistent with institutional policy.*

- *Policy development and adoption needs senior leadership and widespread stakeholder involvement.*

## *Program Design and Management Requirements*

- *Staff qualifications – background screening requirements – how fast?*

- *Staffing ratios by gender and program type – are there benchmarks or national standards?*

- *Staff training – reporting obligations, emergency procedures, records*

- *Facility and transportation safety – License, Rentals, Personal Vehicles*

- *Emergency planning – incidents affecting individual and group*

- *What about parents and volunteers in the program?*

- *Behavioral issues – bullying, violence, sexual misconduct/assault*

## _Notes about Background Screening_

- *Fewer than 5% of offenders have criminal backgrounds*

- *Criminal records of student employees exclude juvenile offenses*

- *Background checks used as the sole method of screening and selection is poor practice.  Background checks MUST be paired with standardized applications, in-person interviews and thorough reference checks.*

## *Best Practices on Staffing Ratios*

*The American Camp Association's adult-to-minor ratios are considered best practice and have been adopted as minimum standards by many institutions that host youth programs on their campus.*

| Ages | Staff-to-Camper Ratio for Overnight Programs | Staff-to-Camper Ratio for Day Programs |
|---|---|---|
| 4 to 5 | 1:5 | 1:6 |
| 6 to 8 | 1:6 | 1:8 |
| 9 to 14 | 1:8 | 1:10 |
| 15 to 17 | 1:10 | 1:12 |

## *Considerations about Staff Training*

*Training must be required before granting access to minors, annually with reinforcement and following an incident or close call.  At a minimum the following topics should be included:*

- *Overview of policy requirements*
- *How offenders operate/identify grooming behaviors*
- *How to recognize red-flag and high risk behaviors*
- *How to prevent peer-to-peer abuse and false allegations*
- *How to report suspicions and concerns*
- *How to recognize and respond to signs of abuse*

## Outside Users of Institutional Facilities

- *Facility Use Agreements – require, require, require.*

- *Minimum insurance requirements*
  - *Commercial General Liability, Commercial Auto, Worker's Compensation*
  - *Sexual Misconduct is EXCLUDED unless CGL is separately endorsed*
  - *Worker's Compensation is state law for all employees. Do not allow outside user entities to dodge this by making their workers independent contractors.*

- *Consider requiring outside users to follow all applicable institutional policies concerning staff screening, safety procedures, etc.*

- *Consider requiring outside users to conduct background checks, but it is not recommended for the institution to get involved in hiring decisions or to set acceptability standards.*

- *Coach's Camps – Despite the affiliation, these are usually private events using institutional facilities, and should meet the same requirements as other outside users. Lines between camp and institution can blur easily.*

## ONLINE PLANNING RESOURCES

*Auburn University Ad Hoc Committee Report*

https://www.auburn.edu/academic/provost/pdf/Final%20Report-%20Committee%20to%20Review%20and%20Establish%20University%20Policies%20Regarding%20Minors%20on%20Campus.pdf


"Best Strategies for Protections Minors: Shaping the Future with Lessons from the Past,"

https://learn.uvm.edu/wordpress_3_4b/wp-content/uploads/Best-Strategies-for-Protecting-Minors.pdf


"The Best Practices for Managing Minors on Campus," Marsh Risk Consulting

http://www.ucop.edu/risk-services/_files/pubs/appendix_a.pdf


Higher Education Protection Network - HEPNet

https://www.higheredprotection.org/

# CYBER RISK MANAGEMENT – RISK SCENARIO



*A phishing email is sent to a group of targeted faculty members, advising them to click a link in the message to review new information security guidance, and verify their credentials for access to the university network. The link in the email opens a very authentic-looking webpage, branded with the university logo, and providing a second link to confirm access credentials. The links are fake, and directs those who click on them to a fake website that looks authentic.*

*About a dozen faculty members click the link and enter their login credentials, which are captured by the hackers. Later, right before payroll processes, the hackers use the stolen credentials to login to the online employee self-service website, alter their direct deposit information, and re-route their pay to an off-shore account. As soon as the deposits are made, the hackers log back in, and restore their direct deposit information to its original status.*

*The theft goes unknown until faculty members notice they did not receive their direct deposit pay advice.*

# CYBER RISK MANAGEMENT

- *Decentralized IT culture is common on campuses, making compliance a challenge.*

- *Personal data is everywhere. The more you look, the more you find.*

- *Breach notification statutes have increased the compliance risk exposure dramatically.*

- *Cyber risk insurance is now widely available, but with high deductibles, hefty premiums, and extensive application and underwriting processes.*

- *Reputational risk exposure is real.*

# *Resistance is futile….?*

Gartner analysts predict that "in 2020, enterprise systems will be in a state of continuous compromise.

[Organizations] will be unable to prevent advanced targeted attacks from gaining a foothold on their systems."

•Gartner. "Prevention is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence." **30 May 2013**.

| | |
|---|---|
| **Economic Espionage** | • Theft of intellectual property |
| **Organized Crime** | • Financial gain |
| **Hactivists** | • Disruption and political statements |
| **Pass-through Attacks** | • Exploit resources for further attacks |
| **Destructive Attacks** | • Disrupt operations and destroy data |

# *CYBERSECURITY IS ASYMMETRIC*

- *Defenders must succeed 100% of the time and invest heavily to design robust solutions*

- *Attackers only need one win!  A single successful phishing email can get the attacker inside the system, regardless of the amount invested in perimeter defenses*

## *Sources of Cyber Liability and Risk Exposure*

- *Collection, storage, transmission, handling of personal information*

- *E-commerce – PCI-DSS protocols, P-Card controls*

- *Mobile devices – laptops, phones, tablets, portable drives, remote PCs*

- *Publishing, hosting online original copyrighted material*

- *IT resources compromised and re-purposed for unauthorized purpose*

- *Old systems, homegrown applications or inadequately evaluated commercial applications with poor to non-existent security protections*

- *Spear Phishing – Targeted attacks seeking access to systems*

- *Compromised credentials are used in more than 95% of data breaches*

"Your new password is incorrect. You must use at least one capital letter, a special symbol, an umlaut, an N-dash, two tildas, a Latin phrase from one of James Joyce's works, and at least three consecutive numbers in the Fibonacci series."

## *Possible Implications of System Intrusion and Data Breach*

- *Denial of service attacks*

- *Mandated notification of owners of personal records breached*

- *Financial loss to those affected – institutional liability, or expensive lesson for the victim*

- *Business interruption – loss of revenue, current and future*

- *Reputational damage, loss of client base*

- *Hardware taken out of service by law enforcement*

*What is personal information?*

Most state statutes now define personal information as:

First name or first initial and last name AND any one of the following:

- SSN and/or

- Driver's license or non-operating identification license and/or

- financial account number and/or

- credit card PLUS security code, access code or password that would allow access to individual's account

## How is a breach defined; how do you know when it's happened?

*Check your state statutes, but per ARS §44-7501, breach means:*

- *Unauthorized acquisition and access, -*
- *involving unencrypted or un-redacted computerized data including personal information, -*
- *that materially compromises the security or confidentiality of personal information, -*
- *that is maintained by a person as part of a database of personal information regarding multiple individuals, -*
- *that causes or is reasonably likely to cause substantial economic loss to an individual*

*Encrypted or Redacted information means:*

- *Data is rendered unreadable or unusable without a confidential process or key*
- *Data is truncated or altered so that no more than last 4 digits of SSN, driver's license, non-operating identification license, account number or credit card number is accessible as part of personal information*

## *Preventative Measures*

- *Limit collection or storage of personal data unless necessary*

- *Control transfer of sensitive data to mobile devices*

- *Two factor authentication – password plus a validation code*

- *Password policies – make them strong and changed regularly*

- *Rapid reporting – breach conditions do not get better if you wait*

- *Encryption protocols – consider institutional solution*

- *Educate users about phishing and personal data security*

- *Control downloads – limit administrative privileges*

## *Information Security Steering Committee*

- *Establishes priorities and policies for campus information security*
- *Investigates and determines response to breach notifications*

- *Typical campus representation includes:*
  - *Information Security Officer*
  - *Chief Information Officer*
  - *Human Resources*
  - *Export Control*
  - *Privacy Officer*
  - *Financial Services*
  - *Risk Management*
  - *Academic/Faculty Representative*
  - *University Registrar*
  - *University Police Chief*
  - *Chief Auditor*
  - *Office of General Counsel*
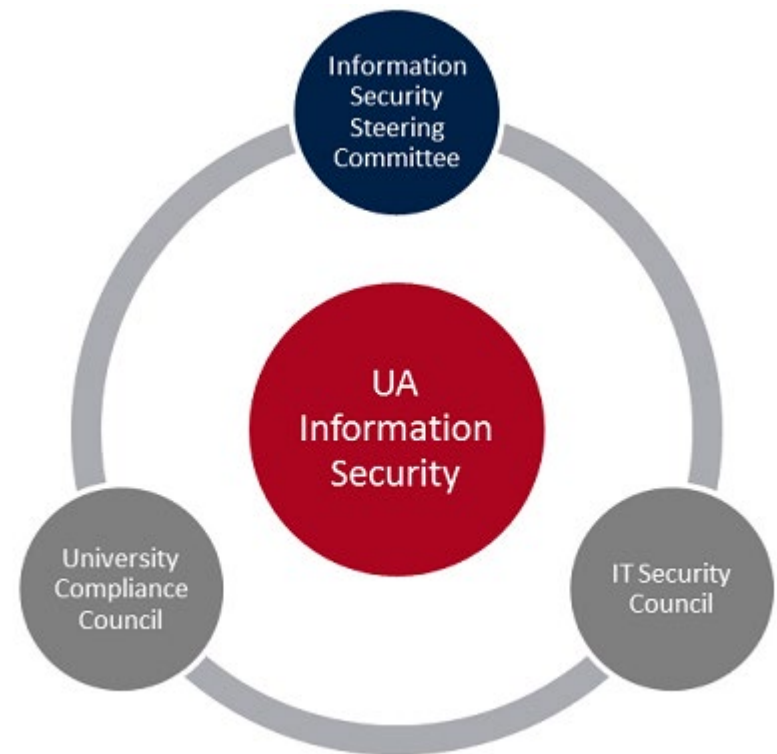
# *Who are key partners in cyber risk management?*

- *Senior Leadership – President, Provost, VPs, CFO*

- *Chief Information Officer, Information Security Officer*

- *General Counsel*

- *Chief Risk Officer*

- *College and Departmental Leadership & IT Staff*

- *Contracting Officials*

- *Procurement*

- *Law Enforcement*

- *Software Vendors*

- *External Resources*

- *Compliance Office*

- *Cyber Insurance Provider*

## *Resources for Cyber Security*

- *Payment Card Industry Standards*
    - *https://www.pcisecuritystandards.org/security_standards/*

- *Red Sky Alliance – consortium of corporate IT security professionals*
    - *http://redskyalliance.org/*

- *US Department of Homeland Security – Cybersecurity*
    - *http://www.dhs.gov/topic/cybersecurity*

# *OTHER HOT TOPICS – FIELDER'S CHOICE*

- *Campus Speech and Climate Issues*
- *Foreign Student Tuition Revenue Loss*
- *Title IX Compliance*
- *Concussion/Traumatic Brain Injury*
- *Alcohol Service at Campus Events*
- *Student Organizations*
- *Intercollegiate Athletics/Sports Clubs*
- *Environmental Compliance*
- *Fleet Operations*
- *Deferred Maintenance*
- *Construction and Renovation*

Questions?
Thank you!

Steve Holland
520-621-1790

sholland@email.arizona.edu