As requested we have provided attendees of the 2019 NM Higher Education Symposium with a PDF copy of the presentation slides. With the exception of the Active Shooter presentation, due to size limitations; and Employment Practices and Current Trends, since it was a bullet point discussion.

Please keep in mind that the presentations are provided without notes or presenter explanation, should you have any questions or to request permission to use slides, we ask that you contact the presenter directly.

Note: If a presentation had special effects it will appear as though the text is doubled up.

NEW MEXICO

GENERAL SERVICES DEPARTMENT

Risk Management Division

Loss Prevention & Control Bureau

BASICS OF THE NEW MEXICO TORT CLAIMS ACT

Laura K. Vega

Cory M. McDowell

History of the New Mexico Tort Claims Act and sovereign immunity

- Up to 1975, the doctrine of sovereign immunity was based on the common law:
  - "It is a fundamental doctrine at common law and everywhere in America that no sovereign state can be sued in its own courts or in any other without its consent and permission" *State ex rel. Evans v. Field*, 27 N.M. 384, 201 P. 1059, 1060 (1921).

- 1975, NM Supreme Court rejects this notion.
  - "The original justification for the doctrine of sovereign immunity was the archaic view that 'the sovereign can do no wrong.'" *Hicks v. State*, 1975-NMSC-056.

History of the New Mexico Tort Claims Act and sovereign immunity

- New Mexico Legislature responds by enacting the Tort Claims Act (TCA)
  - NMSA 1978 sections 41-4-1 through 41-4-29.

- The purpose of sovereign immunity is to protect the public treasuries and to enable the government to function unhampered by the threat of time- and energy-consuming legal actions. *Garcia v. Albuquerque Public Schools Board of Education*. (1980) 95 NM 391.

When does the TCA Apply?

1. Governmental entity and any public employee
2. Acting with the scope of duty
3. Tort based in negligence

- NMSA 1978 Section 41-4-4

Exceptions to sovereign immunity (Waivers of the TCA)

- Other statutes
  - Inspection of Public Records Act (IPRA)
  - Whistleblower Act

Exceptions to sovereign immunity (Waivers of the TCA)

- Eight exceptions built into the TCA – Sections 44-4-5 through 44-4-12
    1. Operation or Maintenance of Motor Vehicles, Aircraft and Watercraft
    2. Buildings, Public Parks, Machinery, Equipment and Furnishings
    3. Airports
    4. Public Utilities
    5. Medical Facilities
    6. Health Care Providers
    7. Highways and Streets
    8. Law Enforcement Officers

Exception: Operation or Maintenance of Motor Vehicles, Aircraft and Watercraft

- Bodily Injury, wrongful death, property damage
- Negligence
- Public employee acting within the scope of the duties
- Operation or Maintenance

Exception: Buildings, Public Parks, Machinery, Equipment and Furnishings

- Bodily injury, wrongful death or property damage
- Negligence
- Public employees acting with the scope of their duties
- Operation or maintenance of any building, public park, machinery, equipment or furnishings

- NMSA 1978 44-4-6

Case Study: Espinoza v. Town of Taos

- 5-year old child enrolled in Taos Summer Day Camp Program.
  - Playing on the playground while waiting for parents to pick up children at the end of the day.
  - Child fell off the slide.

- Allegation is that the supervision was negligent.

Case Study: Espinoza v. Town of Taos

Case Study: Upton v. Clovis Mun. Scho. Dist.

Case Study: Bober v. New Mexico State Fair

Case Study: Encinias v. Whitener

Procedural Requirements

- Notice
  - 41-4-16
  - Written notice
    - Time, place and circumstances of the loss or injury
  - Within 90 days

- Statute of Limitations
  - 41-4-15
  - Commenced within 2 years after the date of the occurrence
  - Children under 7 years old have until their 9th birthday to file

Statutory Cap

- NMSA 1978 41-4-9
- Liability shall not exceed:
  - $200,000 for each legally described real property for a single occurrence
  - $300,000 for past and future medical expenses for a single occurrence
  - $400,000 for any number of claims arising out of a single occurrence for all damages other than real property and medical expenses
- Total liability shall not exceed $750,000 combined for a single occurrence

QUESTIONS?

Effective Safety Committee

Leland Frische - Sr. Risk Officer,
Central New Mexico Community College

PURPOSE OF A SAFETY COMMITTEE

- Improves Safety (Students, Staff & Visitors)
- Interaction of Employees and Management to Promote Safety
- ID Hazards
- Recommend and Implement Corrective Measures

BENEFITS OF AN EFFECTIVE SAFETY COMMITTEE

- A Safety Committee can benefit your organization in the following ways:
  - Gets employees involved
  - Creates interest in health and safety
  - Educates employees and managers
  - Promotes cooperation and coordination between departments; and
  - Promotes the exchange of ideas

ACTUALLY…

- Reduce number of workplace injuries and illnesses
  - Promotes Safety Awareness
  - Create a more enjoyable work environment
  - Reduce ancillary (“Hidden”) costs
  - Reduction of Insurance Cost

SAFETY COMMITTEE FORMATION

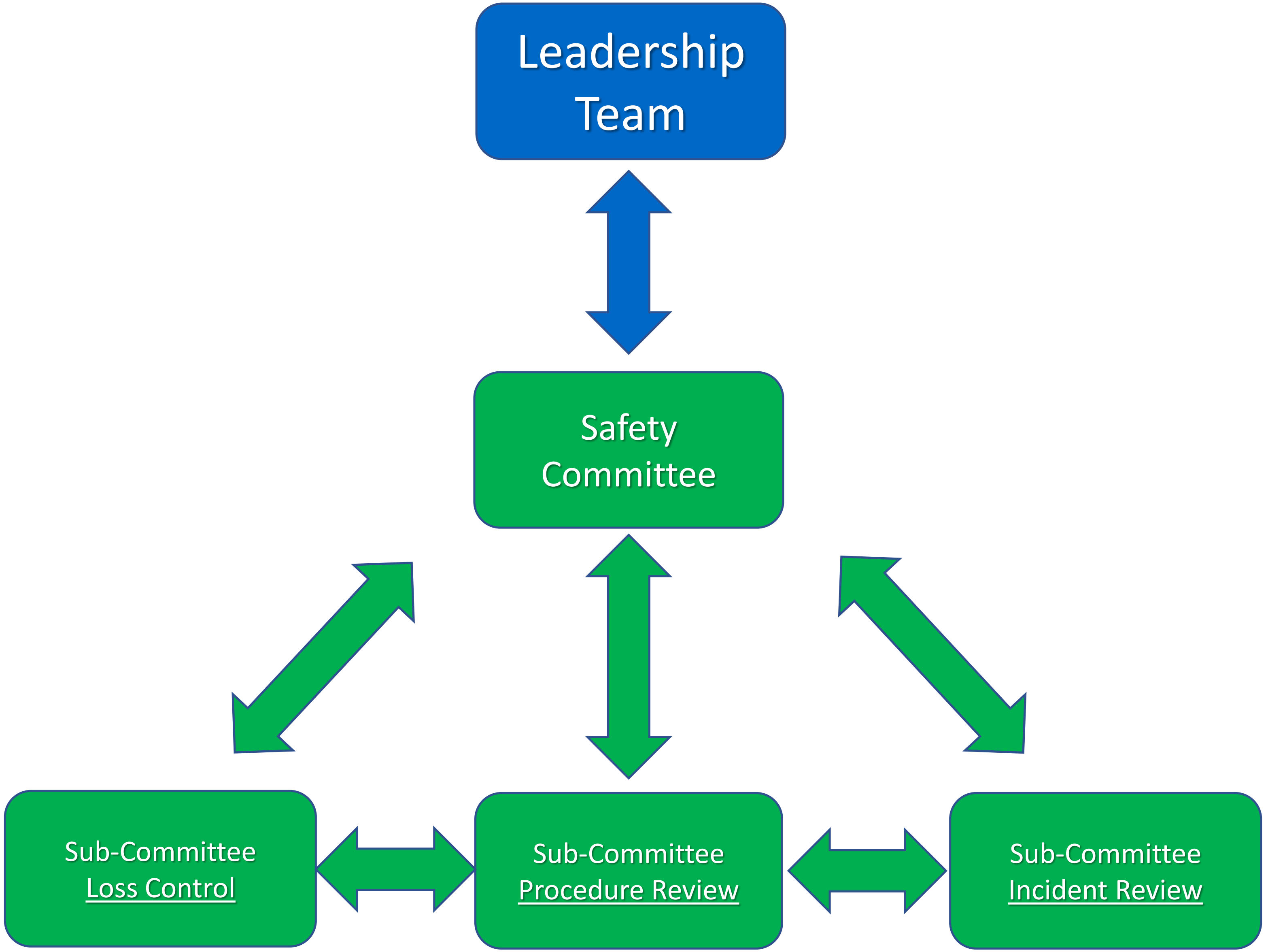
- Establish a Foundation
  - Common measurable goals
  - Commitment from Employees and Management
  - Trust
  - Communicate
  - Non-Adversarial Resolution

Questions for your organization

- Where are our injuries occurring?
- What are the predominant causes?
- Why are they occurring?
  - Are we following up on all injuries?
  - Do we complete root cause analysis?
  - Do we review training needs?
  - How are we communicating trends?

OBJECTIVE

Provide enhanced communication and increased understanding of processes which will allow us to consistently address safety issues to effectively reduce losses.



Leadership Team

Safety Committee

Sub-Committee Loss Control

Sub-Committee Procedure Review

Sub-Committee Incident Review

Safety Committee

- Recommendations to Leadership Team
- Recommendations from Leadership Team
- Safety Communication – Org Publication, Department Messages, Data Dashboard, Etc.

Loss Control Sub-committee

Reduce losses by establishing process for:

- Safety Assessments
- Training
- Mentorship
- Incentive

Procedure Review Sub-committee

Ensure consistent application of processes and procedures through a review of:

- Federal/State/City/County/School
- Departments
- Divisions
- Sections
  - Return to Work - Task Bank – no silos

Incident Review Sub-committee

Seek to understand incidents and provide constructive feedback through:

- Incident / Injury Review
- Root Cause Analysis
- Reinforcing Feedback
- Redirecting Feedback

Provide enhanced communication and increased understanding of processes which will allow us to consistently address safety issues to effectively reduce losses.

Thanks!

Questions?

Central New Mexico Community College

Protecting today. Safeguarding tomorrow.

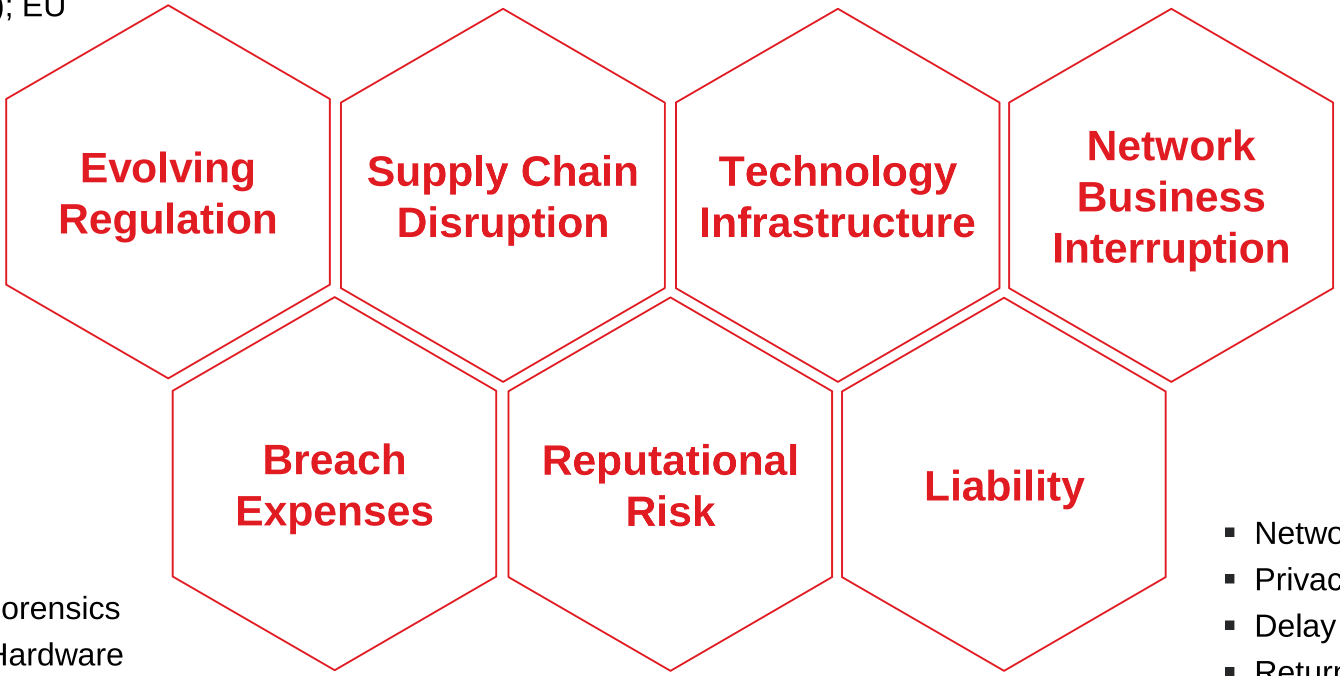
Aon's Cyber Solutions
New Mexico Higher Education Cyber Panel

Santa Fe, NM
March 29th, 2019

AON
Empower Results®

Higher Education and Cyber Risk

Cyber Risk Considerations – 2019



Evolving Regulation

- Varying State and Federal Regulations (NM and other States, HIPPA, FERPA etc.)
- Increasing privacy regulation – CCPA (effective 2020); EU GDPR

Supply Chain Disruption

- Dependent & Contingent Businesses
- Technology Dependencies

Technology Infrastructure

- Information Technology Platform
- IoT / Cloud / SaaS solutions
- Operational Technology

Network Business Interruption

- Technology Failures
- Extended Outages caused by malicious code
- Logistics
- Net Income Loss + Extra Expense

Breach Expenses

- Computer Forensics
- Software / Hardware Replacement
- Data Restoration
- Notification / Credit Monitoring

Reputational Risk

- Customer Erosion
- Public Relations Costs

Liability

- Network Security Liability
- Privacy Liability
- Delay in Delivery
- Return or Offset in Fees
- Contractual Liability / Liquidated Damages

Aon 2019 Cyber Security Risk Report: What’s Now and What’s Next

RISK 1 Technology

Embracing Digital Transformation Creates New and Unanticipated Risks

RISK 2 Supply Chain

Supply chain security wake-up calls grow more insistent

RISK 3 IoT

IoT is everywhere, and it is creating more risks than companies realize

RISK 4 Business Operations

Technology for operational efficiencies can lead to security deficiencies that disrupt organizations

RISK 5 Employees

Excess privileges and shadow IT increase employee risk

RISK 6 Mergers & Acquisitions

Vulnerabilities from deal targets increases as dramatically as M&A value

RISK 7 Regulatory

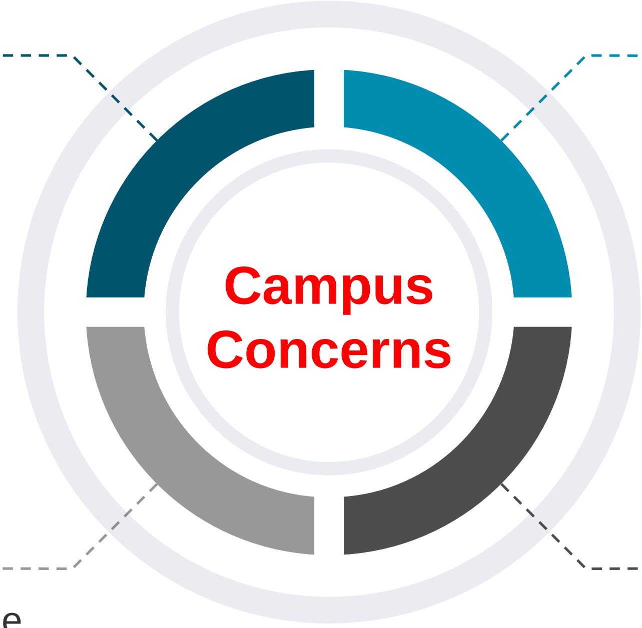
Managing the intersection of cyber security policy and enforcement

RISK 8 Board of Directors

Directors and Officers face growing personal liability relative to cyber security oversight

Aon
Empower Results®

Campus-Wide Drivers of Cyber Risk



Compliance

Institutions of higher education have broad reaching compliance requirements, potentially including FERPA, HIPAA, and GLBA among others.

Culture of Openness

Universities have a culture of openness and collaboration, which often conflicts with security needs.

Decentralization

Higher education campuses can be highly decentralized with separate departments controlling their own IT functions and data.

Desirable Data

- Student, faculty and staff personally identifiable information
- Financial aid and/or transaction data
- Protected healthcare information
- Intellectual property stemming from cutting-edge research

Colleges and Universities: Face Increasing Cyber Risk

Higher education institutions are facing cybersecurity incidents and breaches at an increasing frequency.

$154,000 – Average
$61,000 – Median
Total Breach Cost for Education 2013-2017

$166 Per record cost for breaches in the education sector in 2018

Higher Education is one of the sectors **most affected by W-2 fraud**

103% increase in breaches

>4000% increase in number of records in breaches

40% of breaches utilized phishing

50% of IT respondents indicate insider negligence is the likely cause of insider account compromise

Ponemon Institute, 2018 Cost of Data Breach Study, July 2018.
NetDiligence 2018 Cyber Claims Study'
Gemalto Breach level Index 1H 2017
Verizon. "2017 Data Breach Investigations Report 10th Edition". 2017.
Ponemon Institute LLC and Varonis. "Closing Security Gaps to Protect Corporate Data: A Study of US and European Organizations". 2016.

Colleges and Universities: See High Variety of Attacks

Nation-State Attacks on Higher Ed Institutions in Bulk

At the end of March, the U.S. Department of Justice and the U.S. Department of the Treasury announced law enforcement efforts in response to Iranian state-sponsored cyber-attacks on hundreds of universities around the globe, including more than 100 U.S.-based institutions.*

- China, Russia and others since the 1990’s****

Targeted Spear-Phishing

In January 2018, a successful spear-phishing attack at the University of Hawaii resulted in a data breach impacting approximately 2,400 faculty, staff, students, and student applicants.**

Computer Equipment Theft

Last summer, computer equipment theft at Washington State University resulted in the loss of personally identifiable information (PII) and protected health information (PHI) for approximately 1,000,000 individuals.***

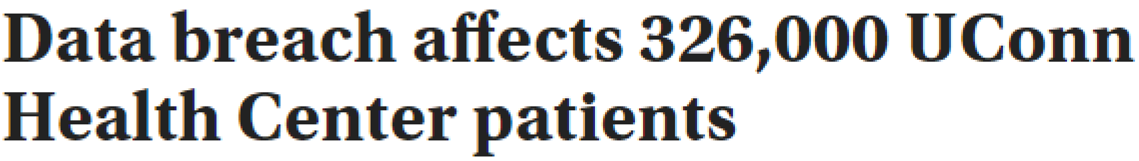
* Sources: Department of Justice, Office of Public Affairs, “Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps,” March 23, 2018; U.S. Department of the Treasury, Press Release, “Treasury Sanctions Iranian Cyber Actors for Malicious Cyber-Enabled Activities Targeting Hundreds of Universities,” March 23, 2018.
** Source: Tyne Phillips, “2,400 were exposed to phishing scheme, UH tells lawmakers,” , Honolulu Star Advertiser, January 25, 2018.
*** Source: Erik Lacitis, “WSU gets costly lesson in theft of hard drive with more than 1 million people’s personal data,” The Seattle Times, July 10, 2017.
****personal experience working the cases

Recent Higher Education Cyber Events

San Diego Unified data breach hits staff, plus as many as 500,000 students

Education Company Chegg Acknowledges Data Breach, Puts 40 Million Users on Notice

Oklahoma State University Center for Health Sciences Informs Patients of PHI Breach

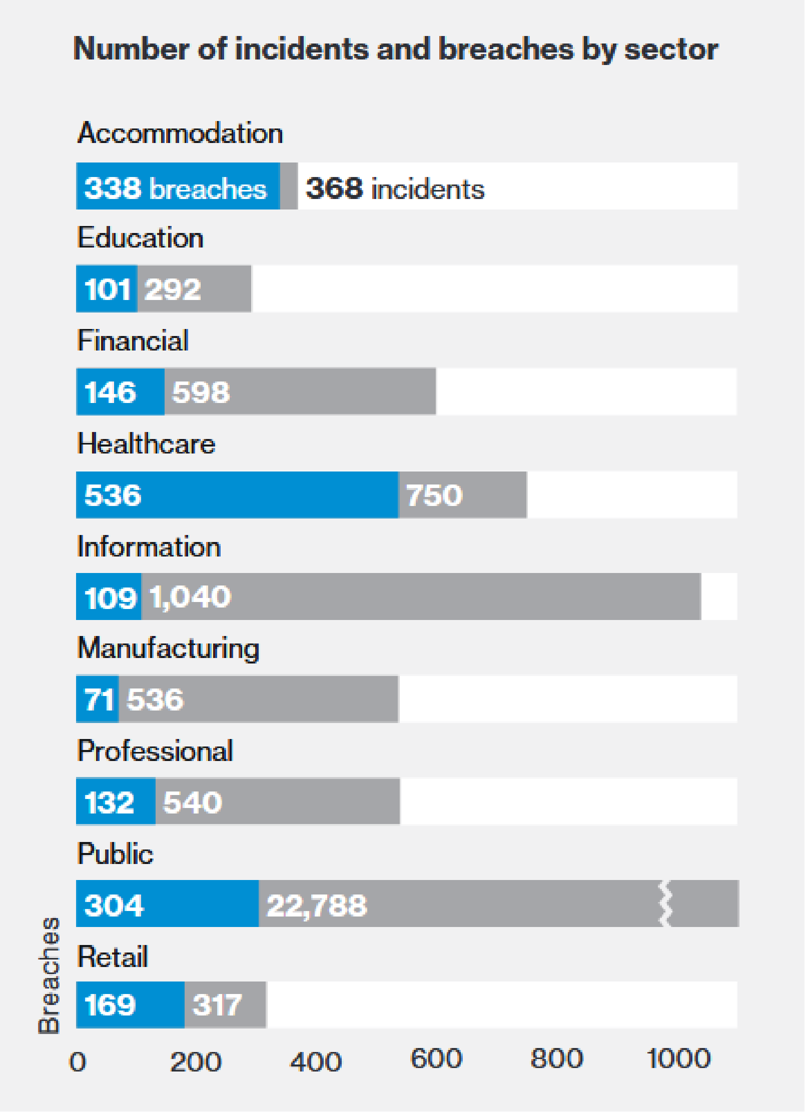


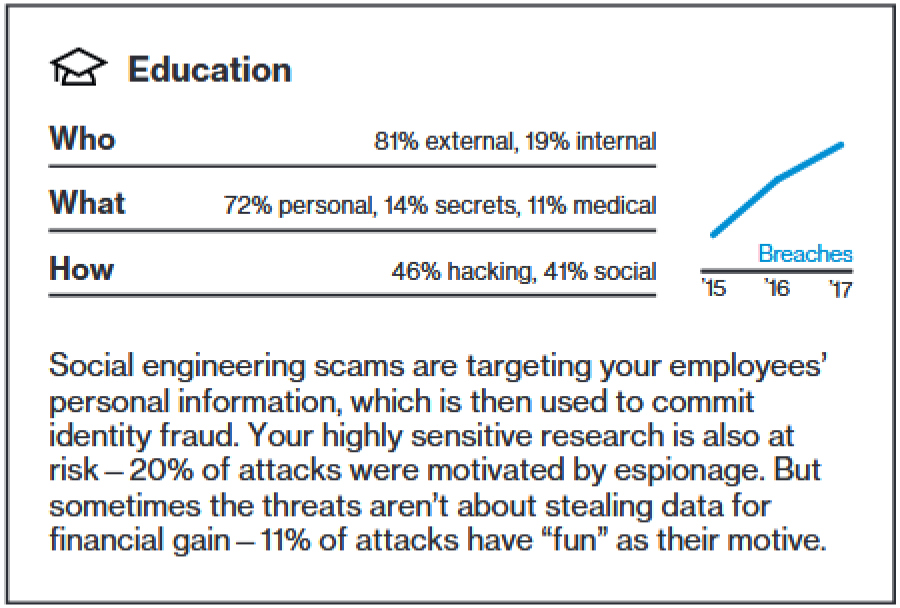
Data breach affects 326,000 UConn Health Center patients

Butler University data breach impacts 163,000

https://www.latimes.com/local/lanow/la-me-ln-san-diego-unified-data-breach-20181221-story.htmlhttps://www.twincities.com/2019/01/30/minnesota-department-of-human-services-reports-data-breach/
https://marketbrief.edweek.org/marketplace-k-12/tutoring-company-chegg-acknowledges-data-breach-puts-40-million-users-notice/
https://www.hipaajournal.com/oklahoma-state-university-center-health-sciences-phi-breach/
https://www.csoonline.com/article/2429410/butler-university-data-breach-impacts-163-000.html
https://www.law.com/ctlawtribune/2019/03/26/class-action-filed-over-uconn-health-data-breach-that-could-have-affected-326000-patients/?slreturn=20190229100558

Breach/Incidents for Higher Education





Education

Who 81% external, 19% internal

What 72% personal, 14% secrets, 11% medical

How 46% hacking, 41% social

Breaches
'15
'16
'17

Social engineering scams are targeting your employees' personal information, which is then used to commit identity fraud. Your highly sensitive research is also at risk – 20% of attacks were motivated by espionage. But sometimes the threats aren't about stealing data for financial gain – 11% of attacks have "fun" as their motive.

Ponemon/IBM:

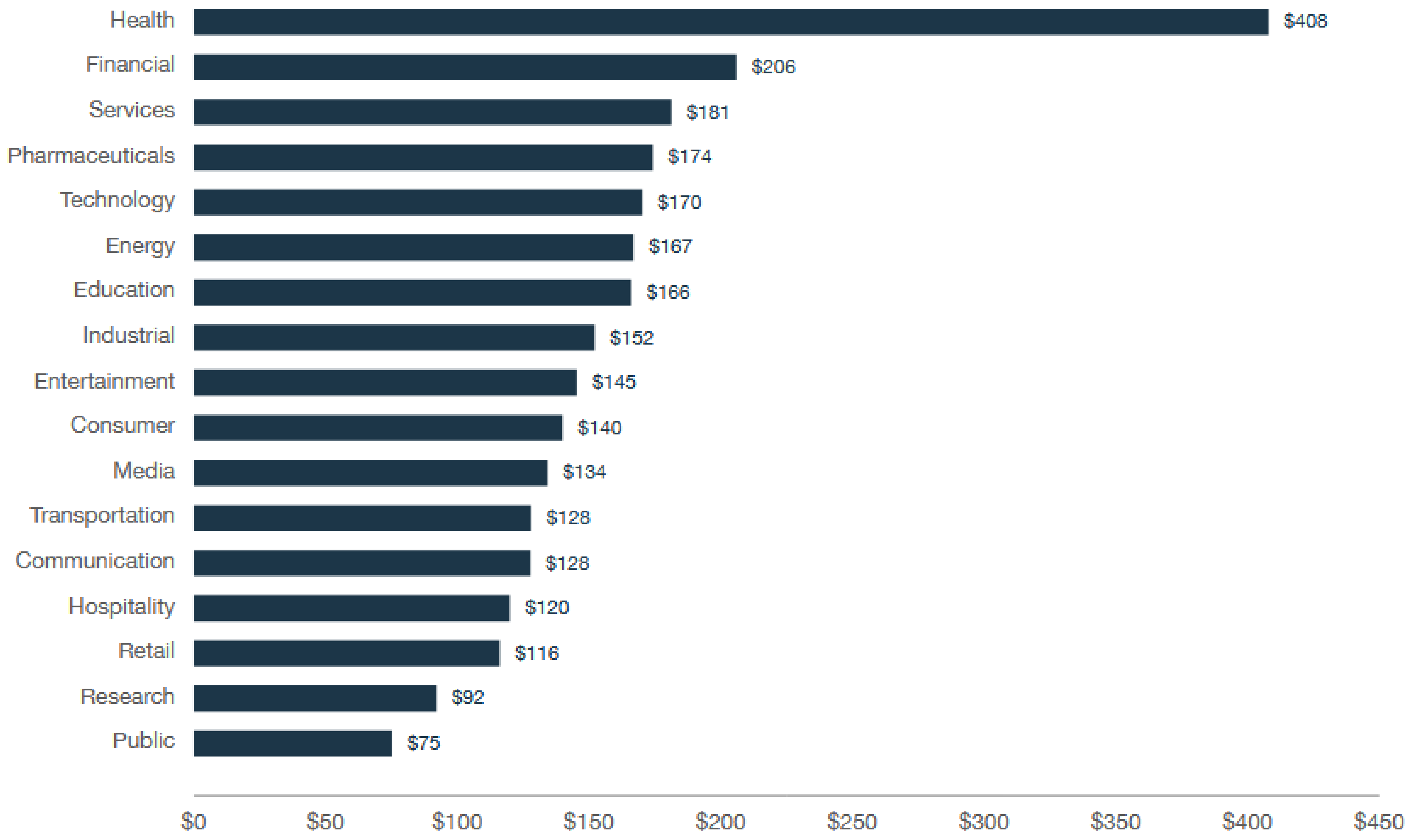
- $166 – cost per record (Higher Education)
- $7.91M – average total cost of a breach in the US
- $340K – savings per breach if entity has an Incident Response Plan
- 196 Days – average time to identify a data breach

Verizon. "2018 Data Breach Investigations Report – Executive Summary". 2018.
Ponemon Institute, 2018 Cost of Data Breach Study, July 2018.

Higher Education – Cost of a Breach

Figure 7. Per capita cost by industry sector

Measured in US$

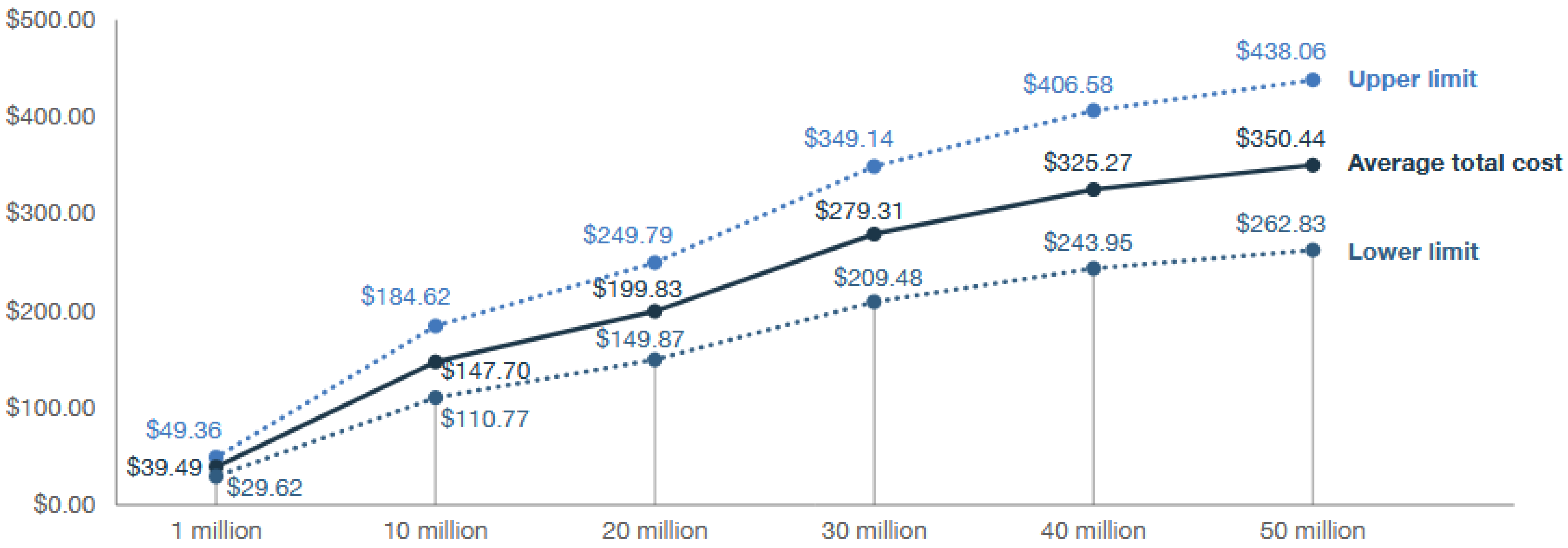


Ponemon Institute, 2018 Cost of Data Breach Study, July 2018.

Cost of a breach over 1M records

Figure 34. A more precise range of the total average cost of mega breaches

Measured in US$ millions



Number of breached records	Detection & escalation	Notification	Post data breach response	Lost business cost	Total cost
1,000,000	$ 11,682,870	$ 567,130	$ 12,225,694	$ 15,012,731	$ 39,488,426
10,000,000	$ 44,851,852	$ 1,878,009	$ 48,039,120	$ 52,926,157	$ 147,695,139
20,000,000	$ 62,481,481	$ 3,174,306	$ 67,170,833	$ 67,005,556	$ 199,832,176
30,000,000	$ 88,407,407	$ 4,151,389	$ 91,763,194	$ 94,989,352	$ 279,311,343
40,000,000	$ 102,537,037	$ 5,903,009	$ 106,411,343	$ 110,413,657	$ 325,265,046
50,000,000	$ 110,998,725	$ 6,498,576	$ 115,028,472	$ 117,919,213	$ 350,444,986

Ponemon Institute, 2018 Cost of Data Breach Study, July 2018.

Notable Data Breach / Privacy Commercial Impacts

Organization	Commercial Impact	Financial Components	Source
Anthem	$278 million	Gross Expenses ($148mm) Security Improvements ($115mm) HIPAA Settlement ($16mm)	Regulator Settlement U.S. District Court HHS OCR
Equifax	$430.5 million $514 million £500,000	Gross Expenses to Date Total Estimated Gross Expenses ICO Fine (DPA 1998)	Q3 2018 Earnings Release Q3 2018 Financials ICO Notice
Facebook	£500,000	ICO Fine (DPA 1998)	ICO Notice
The Home Depot	$298 million	Gross Expenses	10-K Filing 2017
Target Corporation	$292 million	Gross Expenses	10-K Filing 2017
Uber	$148 million €400,000 €600,000 £385,000	U.S. Attorney General Settlement French CNIL Fine Dutch DPA Fine ICO Fine (DPA 1998)	U.S. AG Settlement CNIL Notice Dutch DPA Notice ICO Notice
Yahoo! Inc. (Altaba Inc.)	$350 million $85 million $35 million $80 million $29 million £250,000	Reduced Acquisition Price Customer Class Action SEC Fine Securities Class Action Shareholder Derivative ICO Fine (DPA 1998)	Verizon Press Release U.S. District Court SEC Press Release U.S. District Court U.S. District Court ICO Notice

Notable NotPetya Business Interruption Commercial Impacts

Organization	Commercial Impact	Financial Components	Source
A.P. Moller – Maersk	$250-300 million	Earnings Reduction	Q4 2017 Financials
Beiersdorf AG	Minimal sales impact €15 million	€35mm sales shifted Q2 to Q3 Additional expenses	Q2 2017 Financials Q4 2017 Earnings Call
FedEx (TNT Express)	$400 million	Earnings Reduction	Q4 2018 Financials
Merck & Co.	$410 million $380 million	2017, 2018 Sales Reduction Additional Expenses	Q4 2017 Financials Q3 2018 Financials
Mondelez International	~$104 million $84 million	2017 Sales Reduction Additional Expenses	Q4 2017 Earnings Call Q4 2017 Earnings Release
Nuance Communications	$68 million $31.2 million	2017 Sales Reduction Additional Expenses	Q3 2018 Financials
Reckitt Benckiser	~£114 million	2% Q2 Sales Reduction 2% Q3 Sales Reduction	Press Release Q2 2017 Financials Q3 2017 Financials
Saint-Gobain	~€220-250 million €80 million	2017 Sales Reduction 2017 Earnings Reduction	Q3 2017 Earnings Release Q1 2018 Earnings Release

State of the Cyber Marketplace

Market Standard Cyber Coverages Overview

Operational Risk

- Network Business Interruption
- System Failure
- Dependent Business Interruption / System Failure
- Cyber Extortion
- Digital Asset Restoration

Privacy and Network Security Risk

- Privacy and Network Security Liability
- Privacy Regulatory Fines and Penalties
- Media Liability
- PCI Fines and Penalties
- Breach Event Expenses

Cyber Market Snapshot

↑ Claims & Losses

Stronger data is being gathered as more breaches are reported

- Complexity of breaches has driven an increase in incident response expenses incurred by Insureds
- Claims and loss data has expanded coverage offerings and improved actuarial data for loss modelling purposes
- Increasingly punitive legal and regulatory environment
- Breaches on accounts $1B+ annual revenue have been the main driver for an increase on Insurer Losses

↑ Coverage

Coverage continues to evolve and become more valuable for Insureds

- Insurers continue to update their policy forms to meet current market coverage needs
- Coverage breadth continues to expand
- Insurers continue to differentiate their offerings with new or enhanced coverage components
- Emphasis on pre-arranged vendors
- Broadening systems failure and contingent business interruption coverage solutions

↑ Capacity

Capacity is continuing to grow across geographies

- Over 75 unique Insurers providing Cyber Liability capacity
- Capacity is available the United States, London, Bermuda and Asia
- Growing number of Insurers developing appetites for large, complex risks
- There is over $1B in theoretical capacity available in the Cyber market place

↔ Retentions

Retentions are being reviewed

- Retentions of all levels are available in the market, but can vary greatly based on industry class, size and unique exposures
- Adjusting retentions can lead to increased coverage and/or pricing flexibility

↔ Pricing

Pricing trends are competitive, but increasing for some industries

- Average premium rates reflect a decline – however dependent upon underwriting and scope of coverage
- Excess rate environment continues to be competitive
- Some Insureds have secured significant coverage improvements as a result of paying higher premiums

Note: *This is a general summary and could vary based on client industry and size*

“Silent Cyber”: Potential Cyber Perils Under P&C Policies

Property

- Hacking automated manufacturing facilities to halt production
- Inflicting bodily injury or property damage through compromised network systems
- Plant explosions or damage due to a cyber related event

Intellectual Property

- Unreleased movie / media
- Proprietary design specs for tangible and intangible assets
- Trade secrets
- Copyright materials

D&O

- Disclosures of cyber incidents have a material impact on the organizations’ financial statements
- Reporting requirements
- Regulatory scrutiny

Marine

- Computerized hijacking
- Container tracking systems
- GPS navigation systems
- Automated shipyard processes

Cyber

Business interruption resultant from non-physical damage to computer systems due to a system failure

Security and privacy liability including settlements and defense costs

Breach response expenses

Cyber extortion

Bodily Injury and Property Damage (possible)

General / Product Liability

- Automated system hacking modifies product specs, creating faulty devices
- Increased products exposures to Internet of Things (“IoT”) vulnerabilities

Environmental

- Attacks on nuclear or energy facilities release hazardous chemicals or air emissions
- Untreated sewage releases to poison water supply
- Disablement of critical infrastructure leading to fires or explosions

Kidnap & Ransom

- Ransomware claims filed under K&R policies
- Social media extortion

Recall

- Hacking automated manufacturing plants
- Cyber vulnerabilities in cars and cameras
- Hacker contamination of design specs
- Nanotechnology and 3D printing

Terrorism

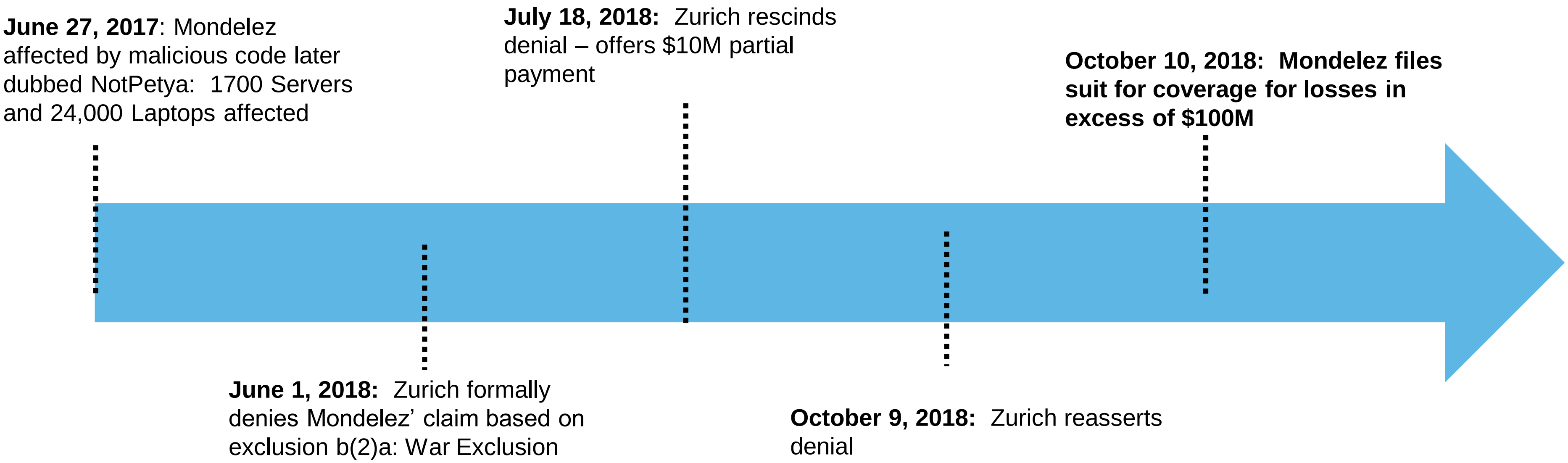
- Hacking medical devices to inflict bodily harm to political or public figures
- Deliberate release of misinformation to cause riot or civil unrest

Crime

- Increased sophistication of social engineering attacks
- Hacking major financial institutions or accounting software to steal monies
- Bitcoin wallet manipulation

Note that coverage in policy forms can vary materially from carrier to carrier, and from base policy forms to manuscript policy forms

Mondelez v Zurich



June 27, 2017: Mondelez affected by malicious code later dubbed NotPetya: 1700 Servers and 24,000 Laptops affected

June 1, 2018: Zurich formally denies Mondelez' claim based on exclusion b(2)a: War Exclusion

July 18, 2018: Zurich rescinds denial – offers $10M partial payment

October 9, 2018: Zurich reasserts denial

October 10, 2018: Mondelez files suit for coverage for losses in excess of $100M

Relevant Details:

Exclusion b(2)(a) *hostile or warlike action in time of peace or war, including action in hindering, combating or defending against an actual, impending or expected attack by any:*

(i) government or sovereign power (de jure or de facto);
(ii) military, naval, or air force; or
(iii) agent or authority of any party specified in i or ii above.

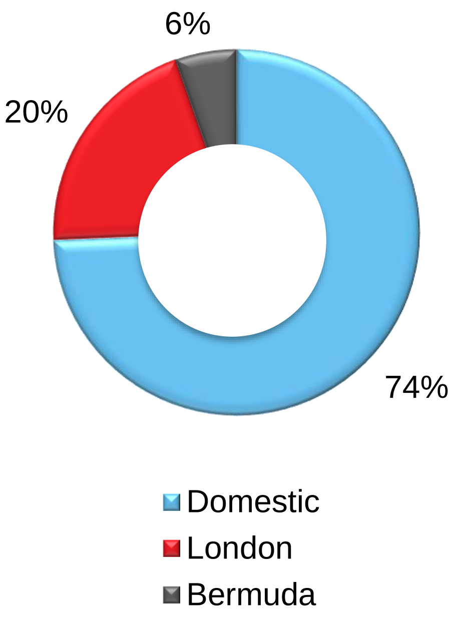
~$104M earnings reduction, $84M extra expense – 2017 Q4 Earnings Release

According to Property Claim Services (PCS) the total industry loss from the Petya / NotPetya cyber attack has now passed $3 billion, roughly 90% of which was driven by silent cyber impacts, the remainder from affirmative losses. https://www.reinsurancene.ws/petya-cyber-industry-loss-passes-3bn-driven-by-merck-silent-cyber-pcs/

Sample Cyber Carve-back language: "Cyberterrorism means the premeditated use of disruptive activities against any computer system or network by an individual or group of individuals, or the explicit threat by an individual or group of individuals to use such activities, with the intention to cause harm, further social, ideological, religious, political, or similar objectives, or to intimidate any person(s) in furtherance of such objectives. 'Cyberterrorism' does not include any such activities which are part of or in support of any military action or war."

Global Cyber and E&O Insurance Marketplace - 2019

Aon Client Premium Spend



DOMESTIC

- **AIG**
- Allianz
- Arch
- Argo
- Aspen
- At-Bay
- **AXA XL**
- AXIS
- AWAC
- BCS
- **Beazley**
- Berkley
- Berkshire Hathaway
- Cap Specialty
- **Chubb**
- CNA
- Coalition
- CV Starr
- Great American
- NAS
- Nationwide
- Navigators
- Hartford
- HCC
- Hiscox
- Huntersure
- Liberty/ Ironshore
- MunichRe
- QBE
- RLI
- RSUI
- Safety National
- SCOR
- **Sompo**
- Swiss Re
- Travelers
- Validus
- Zurich

LONDON

- AIG
- Allianz
- Amlin
- Amtrust
- Argo
- Ascent
- Aspen
- Aviva
- AXA XL
- Axis
- Barbican
- **Beazley**
- Brit
- CFC
- Chubb
- EmergIn Risk
- Hannover Re
- HCC
- HDI Gerling
- Hiscox
- Liberty
- Markel
- Munich Re
- Navigators
- Neon /Tarian
- Nirvana
- QBE
- Occam (formerly Sciemus)
- SCOR
- Swiss Re
- Talbot
- Tokio Marine Kiln
- WRB
- Zurich

BERMUDA (Excess only)

- AIG
- Arch
- AXA XL
- Chubb
- Markel
- Aspen
- AWAC
- AXIS
- Sompo
- Liberty Specialty

Regulatory Fines and Penalties DIC Cover (Bermuda)

Global Rise in Extraterritorial Data Privacy Regulation with Hefty Fines:

- **GDPR** (EU): the greater of €20M or up to 4% of global turnover *May 2018*
- **PIPEDA** (Canada): Fine up to C$100,000 *Nov 2018*
- **LGPD** (Brazil): up to 2% of gross sales (max R$50M) *Aug 2018*
- **CCPA** (California): $750-$7,500 per violation *Jan 2020*

Questions on the Insurability of Fines:

Cover is available for Regulatory Fines and Penalties in primary forms, however whether the insurer can make payment remains uncertain.

Aon/DLA Piper report highlights lack of insurability by EU member country (other than Finland or Norway):

- Most deemed likely to be uninsurable
- Some likely to be brought in a criminal court
- Others assumed to be against public policy

Excess insurance layer with DIC endorsement for an Additional Premium

Insurability trigger – must have affirmative cover in primary

Global cover for Civil and Criminal* fines and penalties

Bermuda Insurers irrevocably waive right to assert fines are uninsurable

Up to $20M available cover

AP ~20% of primary rate

**conduct exclusion added into endorsement to ensure no cover for deliberate wrongdoing. However triggers DIC if brought in a criminal court per bottom left section of this slide on the Insurability of Fines.*

Leveraging Bermuda's Jurisdictional Advantage:

- For many years Bermuda carriers have been offering punitive damages 'wrap' coverage
- In a similar vein, and without public policy constraints found in Europe or the cross-border agreements found in the US, they have started offering broader cover for fines and penalties arising from data breaches where US/EU carriers are not able to effect payment
- Cover available for all Regulatory Fines and Penalties and Punitive Damages for Data Protection violations (not just GDPR).
- Currently $20M capacity available in Bermuda
- Standard excess layer purchase with DIC purchased at an additional premium (~20% of primary rate).

To Note:

- Need to ensure affirmative cover in primary form for DIC endorsement to drop down on
- No solution for 'un collectable' – i.e. if company is prohibited from making collection
- Supplemental application required to be completed prior to quote (this is main basis for underwriting)

Note that coverage in policy forms can vary materially from carrier to carrier, and from base policy forms to manuscript policy forms

Our Capabilities

We Stand on the Shoulders of Giants.

Global strategic acquisitions have strengthened Aon’s fight against cyber risk. We are purpose built to be your best asset against cyber threats.

Cyber Solutions

Aon
Empower Results®

Recognized leader in risk management and cyber insurance solutions

STROZ FRIEDBERG
an Aon company

Global leader in incident response, digital forensics, eDiscovery, investigations, and security advisory

GOTHAM
DIGITAL • SCIENCE
A STROZ FRIEDBERG COMPANY

Specialists with deep and recognized experience in security testing, application security, penetration testing, and red teaming

We Provide a Holistic Solution

Helping to protect today and safeguard tomorrow

Our Unique Value

Digital Forensics & Incident Response

Solving your cyber events

Respond to the incident, create an investigation strategy, contain the incident while preserving evidence, and confidently communicate with your stakeholders

Find the smoking gun.

Security Advisory

Identifying your security weaknesses

Evaluate and remediate your vulnerabilities, determine your readiness to respond, and improve your organization's cyber resilience.

See your company like never before.

Testing

Illuminating your systems' vulnerabilities

Leverage real-world testing and simulations to help you better understand your weaknesses and strengthen your defenses.

Clear your way for peace of mind.

eDiscovery

Navigating the complex issues

Benefit from professional guidance through ever-changing technical and legal challenges.

Bring order to the disorder.

Investigations & Intelligence

Using knowledge to empower

Help protect your organization by applying traditional investigative techniques to the digital environment.

Protect your organization's brand.

Quantification

Optimizing your total cost of risk

Model cyber loss scenarios and stress test your current insurance limits to enhance your risk financing strategies.

Strategize for your company's future.

Broking

Securing your future

Protect your organization from the financial impact of a cyber incident.

Know it's not one size fits all.

Our People

Protectors and Problem Solvers

- Forensic computer analysts
- Penetration testers
- IT security engineers
- Information security analysts
- Security architects
- Former CISOs
- Fraud examiners
- Security risk consultants
- Investigators
- Criminologists
- Forensic accountants
- Governance & risk mgmt. professionals
- Privacy professionals
- Claims advocates
- Evidence Technicians
- Brokers
- CPAs

Oath Takers

- Former law enforcement*
- Former prosecutors
- AM Law 100 former partners

More than the Sum of Our Parts

- Former Big 4 Professionals
- Actuaries
- Statisticians
- Data analysts

* Includes former Head of the Cyber Division at FBI Headquarters and former founder of the FBI's computer crime squad in New York

Aon Cyber Quotient Evaluation (CyQu)

Digital transformation and cyber threats accelerate at a rapid pace, yet enterprise risk management strategies historically lag due to lack of real-time data and enterprise collaboration.

Introducing CyQu

One portal. One holistic view.

Developed to empower enterprises using leading cyber data analytics, Aon's CyQu enables you to rapidly evaluate the enterprise cybersecurity posture and develop a data-driven risk management strategy.

- Built with patent-pending analytics methodology
- Leverages proprietary claims and incident response data
- Facilitates risk transfer opportunities
- Made stronger by Aon's Cyber Solutions

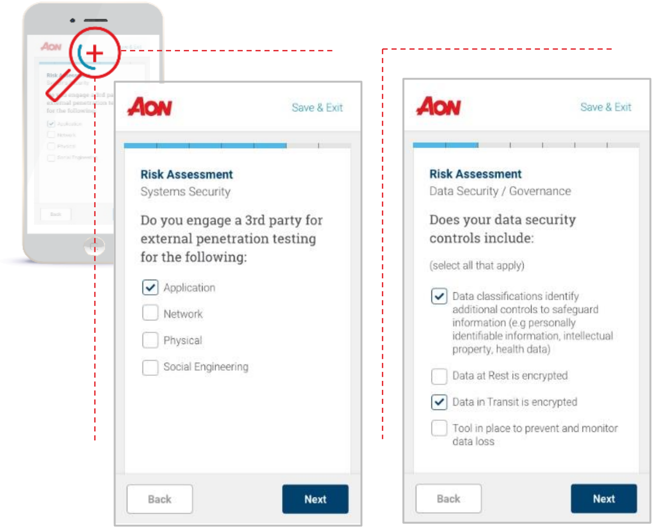
Aon Cyber Quotient Evaluation (CyQu)

One portal. One holistic view

1 **Quickly evaluate the cyber security posture and cultivate a data-driven risk management strategy**

2 **Immediate benchmarking against industry peers**

3 **Use to streamline a submission to cyber insurance carriers**



Risk Assessment
Systems Security

Do you engage a 3rd party for external penetration testing for the following:

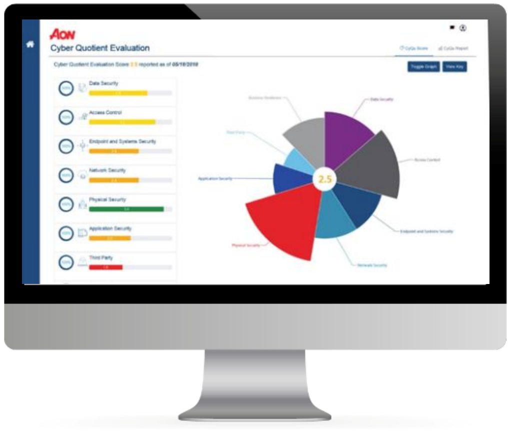
☑ Application
☐ Network
☐ Physical
☐ Social Engineering

Risk Assessment
Data Security / Governance

Does your data security controls include:

(select all that apply)

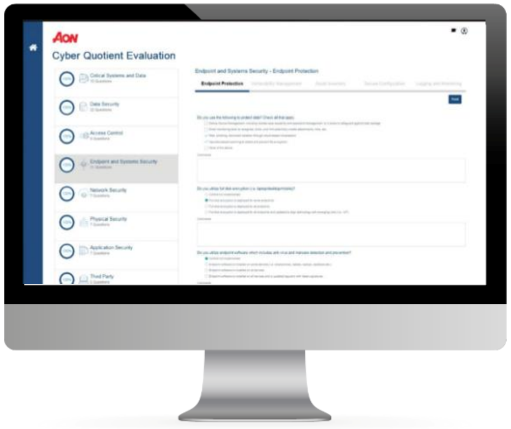
☑ Data classifications identify additional controls to safeguard information (e.g personally identifiable information, intellectual property, health data)
☐ Data at Rest is encrypted
☑ Data in Transit is encrypted
☐ Tool in place to prevent and monitor data loss



Cyber Quotient Evaluation

Cyber Quotient Evaluation Score 2.5 reported as of 05/10/2018

- Data Security
- Access Control
- Endpoint and Systems Security
- Network Security
- Physical Security
- Application Security
- Third Party



Cyber Quotient Evaluation

- Critical Systems and Data
- Data Security
- Access Control
- Endpoint and Systems Security
- Network Security
- Physical Security
- Application Security
- Third Party

Endpoint and Systems Security - Endpoint Protection

Do you use the following to protect data? Check all that apply.

Do you utilize full disk encryption (i.e. laptops/desktops/mobile)?

Do you utilize endpoint software which includes anti-virus and malware detection and prevention?

CyQu Platform is tailored to address any market segment

Instant cyber maturity scoring and vulnerability assessment

Flexible, self-attestation questionnaire framework

Aon Cyber Solutions – E&O/Cyber Broking Group

Experienced teams and resources

- **Over 60 global professionals** dedicated to strategy, execution, and service of errors & omissions and cyber insurance placements
- **Product and industry expertise** – Errors & omissions and cyber industry specialists aligned with Aon industry practices
- **Policy Committee** focuses on developing and enhancing policy language with clients and insurers as well as cyber product development

Market impacting solutions

- **Aon Cyber Enterprise Solution®**
- **Aon's Cyber BI+ Coverage**
- **Aon's GDPR Protect Solution**
- **Aon Cyber Captive Solution**
- **Aon Client Treaty**

Proprietary data and analytics

- **Aon Cyber Insight** loss quantification tool
- **Aon Cyber Quotient Evaluation (CyQu)**
- **Aon Cyber Impact Analysis**
- **Aon invests $400M** in technology / data and analytics. The driving goal is to provide clients with the tools to make fact based decisions

Client engagement and expertise

Aon is the broker for:

- 3 of the 4 world's largest cloud providers
- 3 of the 4 world's largest software companies
- 7 of the 10 world's largest technology companies
- 3 of the 4 world's largest content providers

$550M+
in total premium placed in 2018

60+
Global Professionals

700+
cyber claims managed by Aon

2018
Broker Team of the Year - Business Insurance

Aon’s Professional Risk Solutions – Legal & Claims Practice

Powerfully relevant and the best in the business

Handled

205

Cyber claims in 2018

Handled

1,309

E&O claims in 2018

$315M+

Insurance Recoveries in 2018 from E&O and Cyber carriers

Dedicated expertise

in **E&O and Cyber claims**

13 Dedicated Attorneys

19 Claims Advocates

6 Assistants

38 Total Staff

Your advocate during the claims process

Line of Coverage	Claims Handled By Aon
E&O	4,500+
Cyber (Total)	700+
Media	450+

CYBER RESILIENCE REDEFINED

We're Here for You

Aon's Cyber Solutions is a world-class cyber security team building confidence in a world of uncertainty. Offering holistic cyber risk management solutions, unsurpassed investigative skills, and proprietary technologies, we help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

Our clients call us — and we're at our best — when the stakes are high and the potential for damage is great. We are united by a common goal: Protect today. Safeguard tomorrow.

Find out more at aon.com/cyber-solutions.

We're standing by.

About Cyber Solutions

Aon's Cyber Solutions offers holistic cyber risk management, unsurpassed investigative skills, and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

About Aon

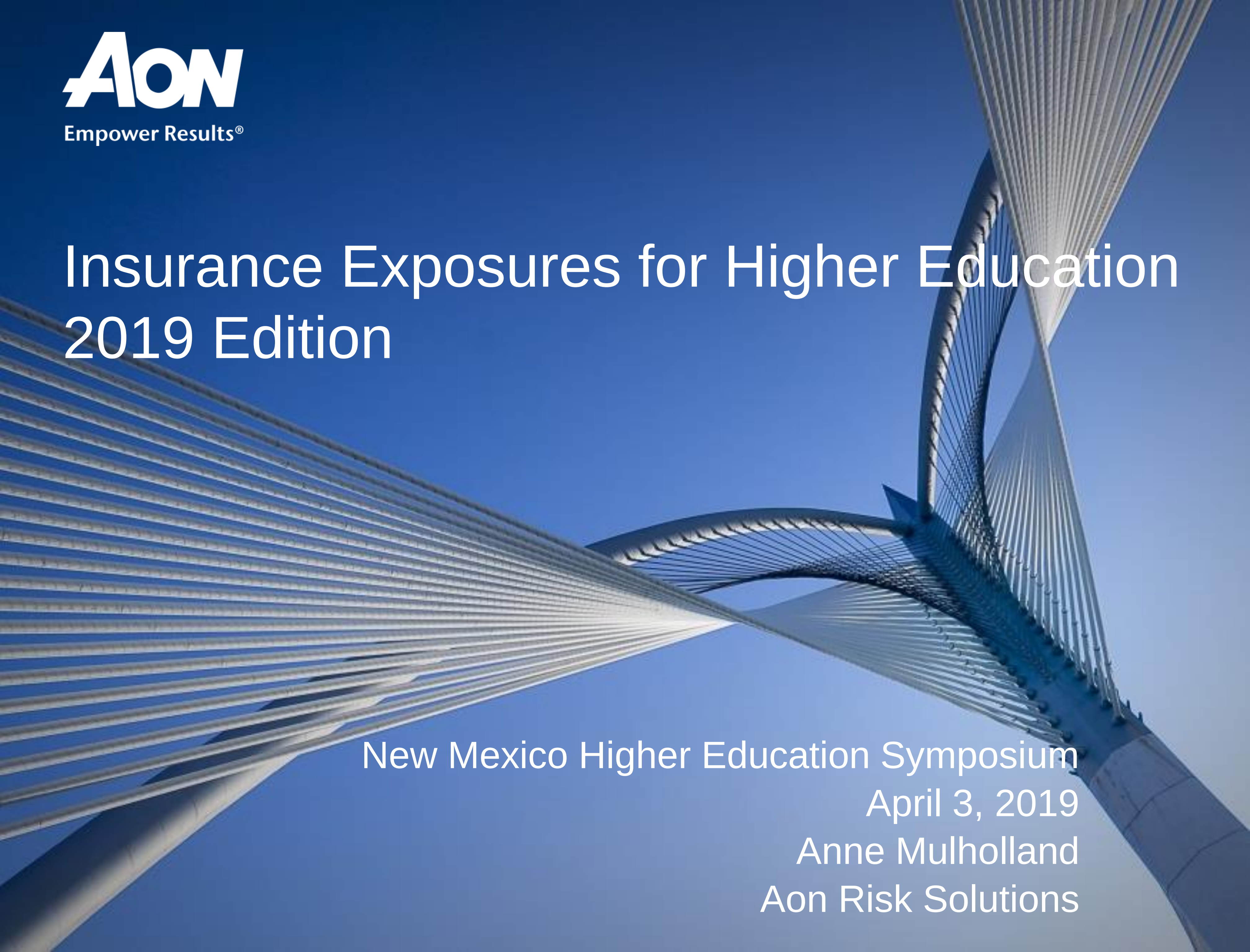
Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

Visit aon.com/cyber-solutions for more information.

Cyber security services offered by Stroz Friedberg Inc. and its affiliates. Insurance products and services offered by Aon Risk Insurance Services West, Inc., Aon Risk Services Central, Inc., Aon Risk Services Northeast, Inc., Aon Risk Services Southwest, Inc., and Aon Risk Services, Inc. of Florida and their licensed affiliates.

The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Empower Results®



Empower Results®

Insurance Exposures for Higher Education 2019 Edition

New Mexico Higher Education Symposium
April 3, 2019
Anne Mulholland
Aon Risk Solutions

1. Sexual Abuse and Molestation

- Insurers have typically construed this exposure as being centered around the protection of minors
  - Widespread acknowledgement and acceptance of the need to protect children from physical and sexual abuse
  - Mandatory reporting requirements give another reason to enforce a zero tolerance policy
- More recently, large incidents have been reported at Michigan State and the University of Southern California that highlight predatory behavior by two physicians against adults
  - Seek to replicate the successes in improving protection of minors
- Protect people where a power differential exists: training, prevention, monitoring and reporting of circumstances

2. Protection of Students

- As young adults, students are not always able to grasp the consequences of risky behaviors; whether it is the use of drugs or alcohol; or “just a prank” that goes awry
- In loco parentis is no longer the standard, despite some assertions that it has returned
  - Institutions have to adhere to best practices to protect students and head off any attendant legal liability

3. Title IX

- Gender Equity in Education
- A Reversal of the Obama DOE’s “Dear Colleague” Approach
- New Regulations Proposed by DeVos in November 2018
  - Comment period closed in January with over 100,000 comments
  - No telling when these will be official
- Procedures to investigate need to be followed and reviewed periodically to assure adherence to best practices
- Reverse “Title IX”

4. Website Accessibility and the ADA

- An Issue of Accessibility and Not Accommodations
- Rise in Lawsuits in Higher Education, including Aggressive Behavior by Plaintiff Firms
- More of a Nuisance than a Severity Risk
- A Reminder (Again!) to Implement Best Practices, Adhere to them and Review them Periodically

5. Traumatic Brain Injury

- Concern About Pending Class Actions in the Northern District of Illinois
  - Still in Discovery
- Plaintiff Lawyers have Filed Another 16 Purported Class Actions
  - Including Division II and III Schools
  - All Involve Alleged Injuries Prior to 2010
- Expect a Ruling from the Court in 2020 on those Class Actions already Pending
  - *TBI will continue to have significant limitations on Liability Insurance protections for education for years to come*

6. Law Enforcement Liability

- Greater Scrutiny by Insurers Related to General Law Enforcement Issues
  - University of Cincinnati Dubose Shooting
- Questions on Training and Experience of Officers
  - Is the Department Accredited?
- Mutual Aid Agreements
- Body Cameras
- Use of Force Policies
- Federal Law Claims

7. First Amendment Issues

- Obligation of Colleges and Universities Regarding Controversial Speakers
  - Public vs. Private Institutions
  - Student Groups vs. Outside Organizations
- Clear Communication with Sponsors
  - Expectations and Obligations
- Involve Public Safety Very Early On in Planning

8. Natural Disasters

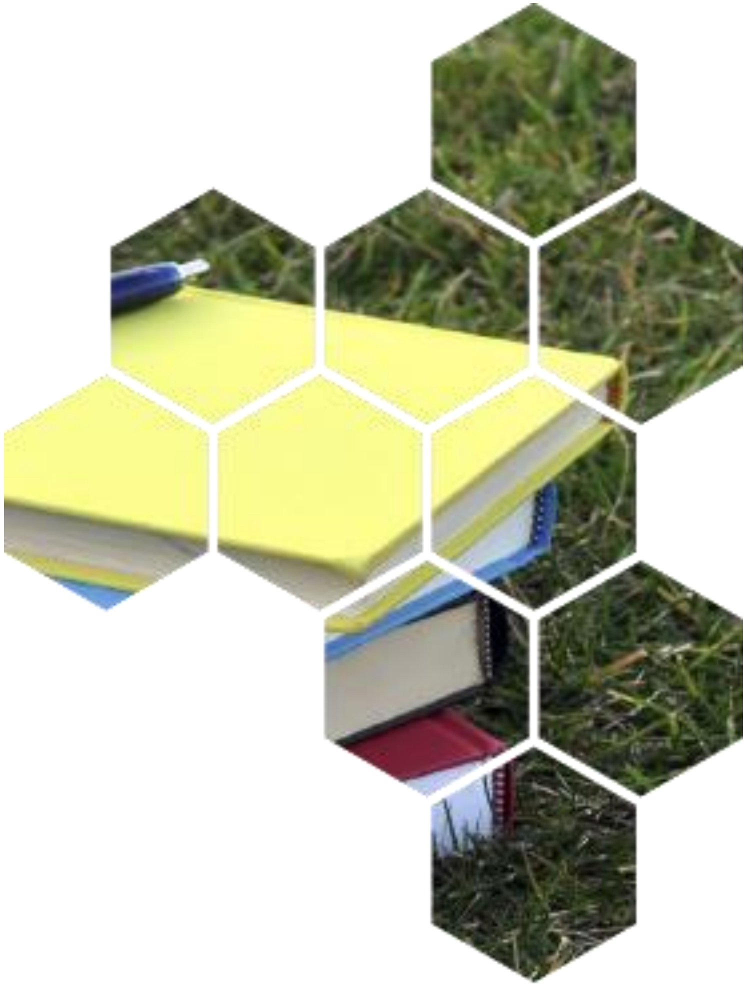
- Flooding
- Hail
- Tornado
- Wildfire

9. Research Issues

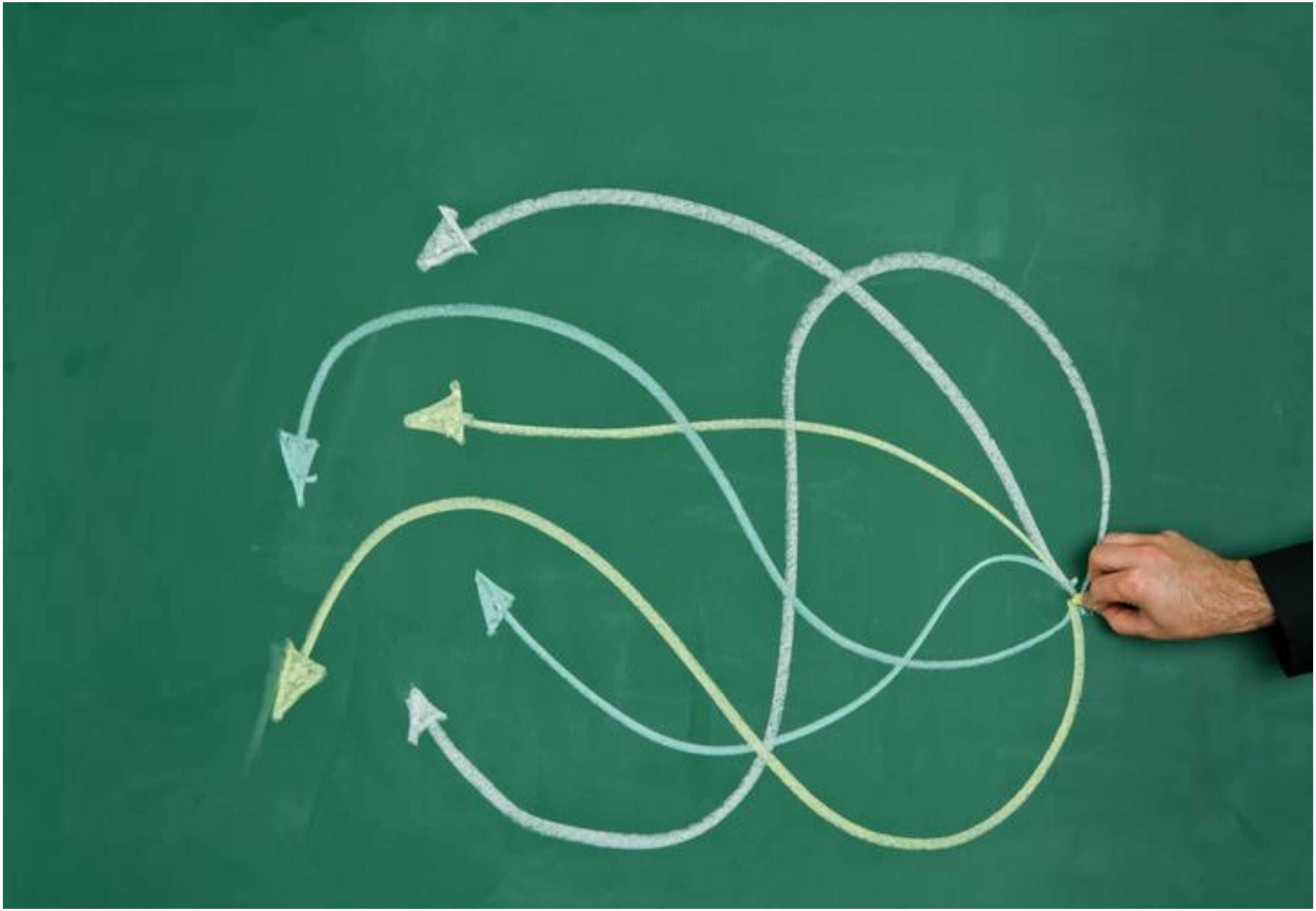
- Intersection of General Liability and Health Care
- Intellectual Property
- Clinical Trials
- Regulatory Compliance

10. Business Interruption and Continuity

- Disruptions to Operations from Any Cause
  - Fire, Flood
  - IT System Outage
  - Civil Authority
  - Pandemic
- Plans to Recover and Get Back to Normal
  - And to operate in the meanwhile



Questions?



Creating a Culture of Civility in the Workplace

State Personnel Office Training and Employee Development

AGENDA

Introduction and foundations

What is civility/incivility in the workplace?

What are the contributors to incivility?

What are the costs of incivility?

What are the benefits of a culture of civility?

Creating a culture of civility: 5 steps

Civility cautions

Wrap-up

Questions

Introduction and Foundations

Incivility, including basic rudeness and discourteousness, can reveal the beginnings of a workplace culture exhibiting hostility, intimidation, and abusive behavior.

"Harassment" as defined by equal employment opportunity laws represents significant legal/financial liability to the employer, in addition to losses in productivity and investment in the workforce.

The past 20 years of training efforts in order to prevent workplace harassment do not appear to have been sufficiently effective, and in some ways have been seen to backfire.

Introduction and Foundations

Harassment prevention training may have inadvertently encouraged a perception that only “unlawful harassment” matters.

Employees do need to be trained on what behaviors to avoid, but should also be given **affirmative information and skill-building**.

Training approaches to addressing harassment are moving away from the legal liability framework and **toward building respectful workplaces**.

What is civility?

Pearson et al. (2000) describe workplace civility as “behavior that helps to preserve the norms for mutual respect at work.”

“Civility demands that one speaks in ways that are respectful, responsible, restrained, and principled and avoid that which is offensive, rude, demeaning, and threatening.”

Civility … entails conveying respect and concern for the well-being of others (Peck, 2002; Sypher, 2004).

What is civility?

Civility is behavior that:

Shows respect toward another

Causes another to feel valued

Contributes to mutual respect, effective communication and team collaboration

What is incivility?

Workplace incivility has been defined as " … low-intensity deviant behavior with ambiguous intent to harm the target, in violation of workplace norms for mutual respect. Uncivil behaviors are characteristically rude and discourteous, displaying a lack of regard for others" (Andersson & Pearson, 1999).

"…a subtle form of interpersonal negative behavior characterized by rudeness and disrespect."

Contributors to incivility

High-stress environment

Culture of acceptance of rude behavior by high performers/valuable employees

Poor role modeling by management

Poorly-defined and -enforced expectations for conduct

Absent and/or poorly-trained leadership (lifeguard example)

Unevenly enforced rules (creates animosity)

Larger society that defines civil behavior as weakness and incivility as strength

Impact of incivility in the workplace

Porath and Pearson (The Cost of Bad Behavior)

80% lost work time worrying about the incident

47% intentionally decreased the time spent at work

78% said their commitment to the organization declined

38% intentionally decreased the quality of their work

66% said their performance declined

25% admitted to taking their frustration out on customers

63% lost work time avoiding the offender

12% said they left their job because of the uncivil treatment

48% intentionally decreased their work effort

Impact of incivility in the workplace

Costs include:

- time spent on **conflict management**
- **turnover** from employees who choose to leave a toxic workplace
- **diminished productivity** and **worse performance** for both targeted individuals and bystanders

- **loss of customers** due to poor customer service and/or customers being aware of toxic workplace
- **time and financial resources** put into responding to complaints and litigation

Benefits of a Culture of Civility

Promotes sense of authenticity by demonstrating alignment of values and actions

Fosters employees' feeling of value to organization

Creates community responsibility for respectful, positive workplace

Empowers effective intervention in problematic interactions and behaviors

Steps to Creating a Culture of Civility

1. Definition and Self-assessment
2. Modeling and Training
3. Policies
4. Continuous reinforcement
5. Accountability

1 Creating a Culture of Civility: Definition and Self-Assessment

Start by identifying and defining what you want.

Articulate values and set expectations: Communicate to employees that your organization truly values and expects certain attitudes, behaviors, and commitments.

Define civility: Help employees understand what is expected of them, with examples.

1 Creating a Culture of Civility: Definition and Self-Assessment

Managers can begin by assessing their own civility and behavior.

How do you behave under pressure? How do you respond to stress?

Do you need to address your own “bad behavior” in honest discussions about the culture with employees? Your own learning process is valuable information.

1 Creating a Culture of Civility: Definition and Self-Assessment

Civility Norms Questionnaire-Brief

A 4-item measure designed to assess workgroup climate for civility.

Climate for civility is defined as **employee perceptions of norms supporting respectful treatment among workgroup members.**

① Creating a Culture of Civility: Definition and Self-Assessment

Survey items:

1) Rude behavior is not accepted by your coworkers.
2) Angry outbursts are not tolerated by anyone in your unit/workgroup.
3) Respectful treatment is the norm in your unit/workgroup.
4) Your coworkers make sure everyone in your unit/workgroup is treated with respect.

2 Creating a Culture of Civility: Modeling and Training

Workplace leaders must set the tone by modeling the behavior they wish to encourage.

Show employees through your own actions what behaviors you expect, and be honest about the times you don’t do as well as you might like.

Managers and supervisors who consistently fail to engage in good role modeling will set the endeavor up for failure.

2 Creating a Culture of Civility: Modeling and Training

Suggestions for modeling behaviors:

Showing restraint in difficult interactions; reacting constructively

Refraining from negative talk about people; redirecting those conversations

Giving/getting feedback on behavior (destigmatizing/normalizing the interactions)

2 Creating a Culture of Civility: Modeling and Training

To teach employees these skills, give explicit training that:

- Describes what civility looks like
- Gives examples of situations in which employees sometimes act uncivilly
- Provides tips on how to maintain composure
- Affords opportunities to practice behaving civilly in emotionally charged situations

3 Creating a Culture of Civility: Policies

Anti-harassment and retaliation policies should be taken seriously, and clear about:

- What types of behaviors are prohibited?
- What are the consequences?
- How does this policy fit into the overall culture of civility?

Alternative Dispute Resolution: Should be a standard part of P&P for addressing workplace conflict.

Employee Code of Conduct: Consider supplementing with a code of civility.

3 Creating a Culture of Civility: Policies (example 1)

We greet and acknowledge each other.

We say please and thank you.

We treat each other equally and with respect, no matter the conditions.

We acknowledge the impact of our behavior on others.

We welcome feedback from each other.

We are approachable.

We are direct, sensitive, and honest.

We acknowledge the contributions of others.

We respect each other’s time commitments.

We address incivility.

3 Creating a Culture of Civility: Policies (example 2)

Treat each other with dignity and respect.

Exercise reasonable, good judgment in handling interpersonal disputes.

Refrain from use of abusive language.

Model respectful problem-solving.

Extend common courtesy to others, such as saying please and thank you.

Be respectful of others even in disagreement.

Address incivility when it is observed.

Practice civility in all conversations and behavior.

Seek to understand others’ points of view.

4 Creating a Culture of Civility: Continuous Reinforcement

The workplace can be an emotionally charged environment due to factors such as high stakes and different personalities and temperaments brought together for extended periods of time.

Because of this, the culture of civility is not a like a monument that is set in place and complete. It is more like a garden that requires cultivation and care.

The expected behaviors must be modeled day in and day out, and deviations must be addressed.

4 Creating a Culture of Civility: Continuous Reinforcement

Positive behaviors should be reinforced with praise when appropriate.

Managers should monitor the workplace for emerging issues even no complaints are made.

Signs that all is not well: Angry outbursts, harmful gossiping, “snippy” emails, exclusions from groups, etc.

4 Creating a Culture of Civility: Continuous Reinforcement

Provide civility-related trainings periodically on topics such as:

1) working across differences
2) dealing with difficult people
3) stress management
4) bystander intervention

Review fundamental concepts and expectations during coachings, and be prepared to hold people accountable.

5 Creating a Culture of Civility: Accountability

Accountability should be both both lateral and vertical.

Coworkers actively participate in creating and maintaining the culture by giving feedback.

Leadership must not only actively monitor the workplace, but also address issues as they arise.

5 Creating a Culture of Civility: Accountability

Accountability will include informal conversations about potential issues, but also more formal steps if necessary to address violations of policies.

Like all policies, employees must see that the expectations are upheld fairly and consistently. If anyone gets away with violating group norms and policies without consequences, the internalized respect for those expectations will vanish.

Civility Cautions

Similarly, a code of conduct/civility **should not be used to shut down complaints or disagreements.**

Legal liability may arise if people are deterred from making complaints or engaging in concerted activities.

Be mindful of employees and/or managers using **"civility" as a weapon** against those they don't like.

"Implicit bias" factors into what we think is acceptable behavior and what is not.

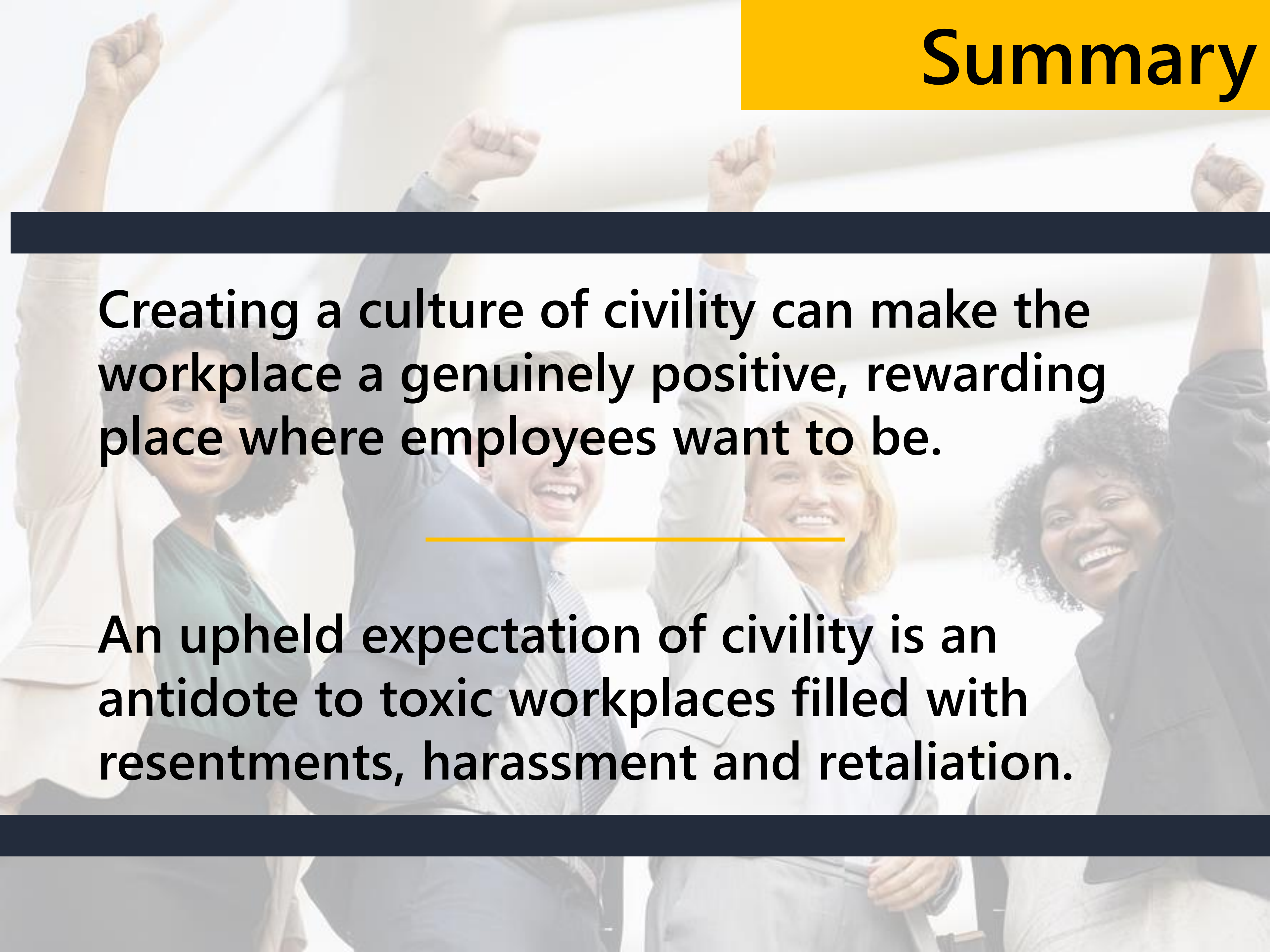
Summary

Civility must be defined and included as part of the organization’s values.

Civility must be modeled, trained, and reinforced regularly.

Managers should not rely on a code of civility as a reason not to manage actively and hold people accountable, but also should not over-enforce or enforce unevenly.

Summary



Creating a culture of civility can make the workplace a genuinely positive, rewarding place where employees want to be.

An upheld expectation of civility is an antidote to toxic workplaces filled with resentments, harassment and retaliation.

Contact information

Jaime L. Phillips, Ph.D.

Training and Employee Development Specialist

NM State Personnel Office

Jaime.Phillips2@state.nm.us

Crucial Conversations for Workplace Safety

Mary Beth Stevens

Laboratory Ombudsman

Certified Organizational Ombudsman Professional

Silent Danger, Key Findings

- 93% of employees say their workgroup is currently at risk from one or more of five “undiscussables”.
- Nearly 1/2 are aware of an injury or death caused by these threats.
- When employees see one of these threats, only one in 4* speaks up despite the potential likelihood for injury.

*identical % to 2016 EEOC data on sexual harassment reporting

The Undiscussables

1. Get It Done

Unsafe practices that are justified by tight deadlines

2. Undiscussable Incompetence

Unsafe practices that stem from skill deficits

3. Just this Once

Unsafe practices that are justified as exceptions to the rule

4. This Is Overboard

Unsafe practices that bypass precautions considered excessive

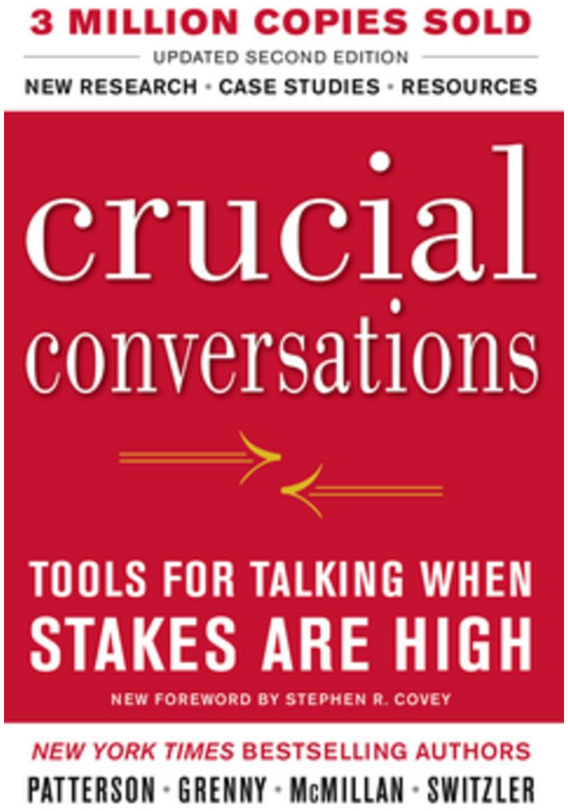
5. Are You a Team Player?

Unsafe practices that are justified for the good of the team, company, or customer

Candor Required

“The crucial ingredient … is ensuring a critical mass of people are willing and able to speak up when safety lines are crossed—irrespective of who crosses them.”

What’s a person to do?



3 MILLION COPIES SOLD

UPDATED SECOND EDITION

NEW RESEARCH · CASE STUDIES · RESOURCES

crucial conversations

TOOLS FOR TALKING WHEN STAKES ARE HIGH

NEW FOREWORD BY STEPHEN R. COVEY

NEW YORK TIMES BESTSELLING AUTHORS

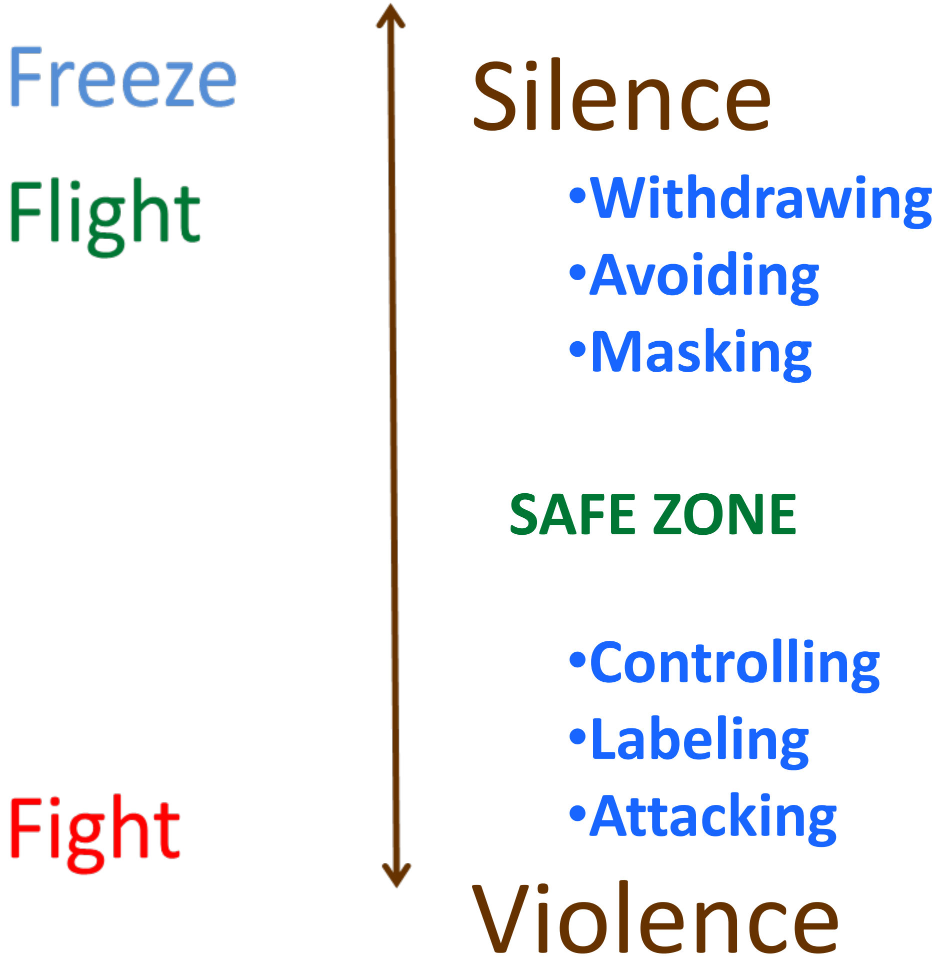
PATTERSON · GRENNY · McMILLAN · SWITZLER

Start with Heart

- Admit your role
- Re-engage your brain (& put on your own oxygen mask first)
- Focus on what you *really* want
- Refuse the "sucker's choice"

Patterson, K., et al. (2002). Crucial Conversations: *Tools for Talking When the Stakes Are High*. McGraw-Hill.

Interpersonal Flight to Fight



Freeze

Flight

Fight

Silence

- Withdrawing
- Avoiding
- Masking

SAFE ZONE

- Controlling
- Labeling
- Attacking

Violence

Patterson, K., et al. (2002).

Make It Safe

Step out of the content

Apologize when appropriate

Contrast to fix misunderstandings

Commit to seek mutual purpose

Patterson, K., et al. (2002).

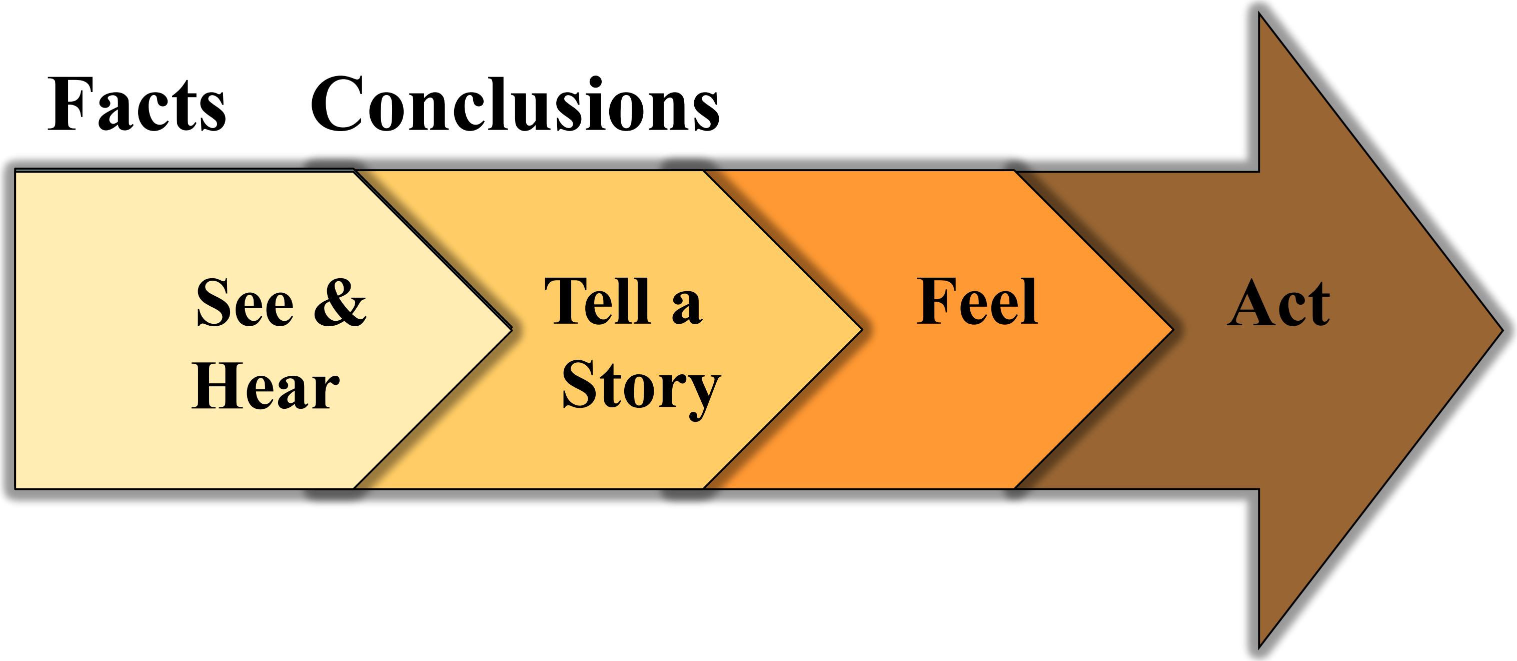
Now let's look at the stories you're telling about yourself, other people & your conflicts.

“Truthiness”

“Every(one)…comes with a story he or she wants you to believe. It is their ‘truth’ and they will try to convince you that it is a factual, even dispassionate, rendering of historic events.”

Puls, D. (2011, February). “Truth Distortions in Interpersonal and Organizational Conflict.” http://www.mediate.com/articles/pulsD11.cfm.

Path to Action



Facts

Conclusions

See & Hear

Tell a Story

Feel

Act

Patterson, K., et al. (2002).

The Empowering Question

Convert Victim → Problem-Solver

"What one thing can I do right now, to move toward what I really want?"

Patterson, K., et al. (2002).

The Humanizing Question

Convert Villain → Human Being

“Why would a reasonable, rational, & decent person do this?”

Patterson, K., et al. (2002).

Villainous stories in safety reporting

“It’s not that people who remain silent don’t care… it’s not bystander apathy; more like bystander agony.

“Employees don’t speak up (because) they don’t think it’s their role; they don’t know how; and they are afraid of retaliation.”

‘STATE’ Skills

Share your facts

Tell your story

Ask for others’ paths

Talk tentatively

Encourage testing

Patterson, K., et al. (2002). Crucial Conversations: *Tools for Talking When the Stakes Are High*. McGraw-Hill.

If you feel stuck

Ask

Mirror

Paraphrase

Prime

Close Cleanly

Who will do

What by

When?

Follow-up

Additional Tools

- Describe the Gap
  - expected vs. observed
- Name the Pattern

PRACTICE CRUCIAL SKILLS FOR SAFETY-RELATED CONVERSATIONS

Recommended Reading

Brafman, O. & Brafman, R. (2008). Sway: *The Irresistible Pull of Irrational Behavior*. New York, NY: Doubleday.

Lenski, T. (2012, September). "How to End a Negotiations Tug of War."

http://www.mediate.com/articles/LenskiTbl20120911.cfm#

Patterson, K., Grenny, J., McMillan, R., & Switzler, A. (2002). Crucial Conversations: *Tools for Talking When the Stakes Are High*. McGraw-Hill.

Persinger, T. (2004, May). "All Behavior Makes Sense." http://www.mediate.com/articles/persingerT4.cfm

Puls, D. (2011). "Truth Distortions in Interpersonal and Organizational Conflict." http://www.mediate.com/articles/pulsD11.cfm.

Ury, W. (2007). The Power of a Positive No: *How to Say No and Still Get to Yes*. New York, NY: Bantam Books.

Vivyan, C. (2009). "About Automatic Thoughts." www.getselfhelp.co.uk/thoughts.htm.

Silent Danger

The Five Crucial Conversations that Drive Workplace Safety

VitalSmarts®

Silent Danger The Five Crucial Conversations That Drive Workplace Safety

> *"One of our guys was changing out a commercial meter. When you're doing that you should always vent the gas outside. Everyone knows that, but we sometimes skip it because we're trying to keep up with the schedule. We don't want to be the weak link in the team. So we not only skip the venting, but have stopped reminding each other when we see our buddies taking risks. Well, the small room he was in filled with gas and was eventually ignited by the nearby water heater. The room blew up with the worker trapped inside by a locked door. Luckily someone in the hallway opened the door before the worker got killed. He came out badly burned. That slowed us down for a few months, but now I see us feeling pressured again to not let the team down when things get crazy. I sometimes feel like I should say something. But . . . "*

In the U.S., many of the most obvious workplace threats have been reduced or eliminated, making American workers safer. Time lost due to workplace injuries dropped a whopping 54.9 percent between 1991 and 2008. These improvements were seen across all industries, geographic regions, and companies of various sizes.[1] However, despite this positive trend, there is evidence these improvements are beginning to stall.[2] In 2007, more than 5,600 people were killed on the job and more than 4 million were injured.[3] What's more. these injuries cost firms upwards of $48.6 billion.[4]

The vast majority of the gains in workplace safety can be attributed to improvements in equipment, policies, systems, and training.[5] Leaders have applied quality, statistical, and project-management tools to safety issues and have achieved remarkable results. However, these formal tools often fail to address challenges that are less formal, are cultural in nature, and exist unacknowledged like icebergs below the waterline. These overlooked obstacles include entrenched habits, social norms, and informal practices.

This study probes below the surface by looking for unsafe conditions that are broadly recognized yet allowed to continue because of cultural norms and social taboos. The ugly secret behind most workplace injuries is that someone is aware of the threat well in advance, but is either unwilling or unable to speak up. Our study shows the greatest danger today is not from ignorance or inattention to risks—but from silence. The next leap forward in workplace safety will come not just from additional changes to processes, technology, or policies, but from changes to behavior. Unless and until the code of silence is broken, we'll continue to suffer completely avoidable losses in both health and performance.

The Study

Through extensive exploratory and confirmatory research. this study uncovered five workplace threats that are especially likely to persist as "undiscussables" in safety-conscious organizations throughout the U.S. To identify these threats, we studied more than 1,600 frontline

[1] "Workers Compensation Claim Frequency Continues Its Decline in 2008," Tony DiDonato, Matt Crotts, and Melissa Brown, NCCI Research Brief, July 2009.

[2] DiDonato et al, p. 1.

[3] Bureau of Labor Statistics, US Department of Labor, July 2009.

[4] 2008 Workplace Safety Index, Liberty Mutual Research Institute for Safety, 2008.

[5] The Need for New Paradigms in Safety Engineering, Nancy Leveson, in *Safety-Critical Systems: Problems. Process and Practice* edited by C Dale and T Anderson. Springer Verlag 2009.

workers, managers, and safety directors across thirty companies during the first half of 2009. In the first phase of the research, we conducted on-site interviews and focus groups with 130 people across all levels from eight different companies to find and analyze patterns of poor communication that threatened workplace safety. We then verified these patterns through a survey administered to 1,500 employees across all levels from twenty-two different organizations to test whether and how breakdowns in communication were confronted, and to test the impacts these breakdowns had on workplace safety.

What we found is that a whopping 93 percent of employees say their workgroup is currently at risk from one or more of five undiscussables or "accidents waiting to happen." And nearly half are aware of an injury or death caused by these workplace dangers.

The astonishing and troubling finding is that when employees see one of these five threats, only one in four speak up. This failure to speak up and correct unsafe conditions allows these risks to continue despite the inevitability of injury.

Based on the results of the research, we argue that more training, safety audits, and other tools that address the plainly obvious threats to workplace safety, while important, will never be enough to create a truly safe environment. The employees in this study already see and recognize these visible threats at the tip of the iceberg but choose to remain silent because of barriers that are hidden below the surface. Our research indicates that the "below-the-waterline" threats are the norms, habits, and assumptions embedded in the organization's culture. These cultural threats inevitably trump the formal policies. When employees see accidents waiting to happen, they feel culturally constrained from saying or doing anything to prevent them from occurring.

As we saw earlier, a scheduler can feel pressured to wedge one more commercial meter change into the day. Or an electrician can worry about being seen as a slacker because he or she doesn't turn the jobs around fast enough. So how can you maintain high reliability in a social system when any individual's action can put safety at risk?

The Missing Ingredient

Our research shows the missing ingredient for a safety culture is candor. When accountability is carefully and intentionally built into the culture, every employee is responsible for holding his or her peers accountable. In these cultures, the unsafe actions of errant individuals almost never persist. Ensuring a critical mass of people are willing and able to speak up when safety lines are crossed—irrespective of who crosses them—is crucial to a safety culture. There's the rub. While safety demands that people look out for each other, remind each other, and hold each other accountable, the reason safety risks persist is because in most organizations, people are unwilling and unable to step up to these most crucial of conversations.

In fact, accountability is the implicit assumption that underlies every safety program. Yet our findings show this assumption is more fiction than fact. Consequently, accountability is the critical weakness of the above-the-waterline approach to safety. If people don't hold each other accountable for acting on observed threats, then more training to help them recognize threats will be of limited value. Silence, not blindness, is the problem.

This discovery also points to an exceptionally high-leverage strategy for improving workplace safety. This study identifies five threats that are most likely to turn into undiscussables. If leaders focus on these five threats and transform them from undiscussables into approachable accountability discussions, they can expect dramatic improvements in workplace safety.

And while safety improvement is reason enough to build a cultural capacity for dealing with these crucial conversations, the potential benefits go far beyond ensuring human health. Our study shows that investing in people's capacity to step up to such conversations can likewise lead to improved accountability for quality, productivity, cost control, HR policies, and any other area of performance. *When people learn to sustain high levels of accountability in any area, they can perform better in every area.*

The Five Crucial Conversations That Drive Workplace Safety

To uncover the five crucial conversations of safety, we started by looking for the telltale signs of an "accident waiting to happen." We found that these signs combine two elements of any risk assessment: they are common and they are costly. But we also found a third element: these are risks that have become undiscussable.

Below are the conversations that fit these three quantitative conditions. We illustrate each conversation with real-life examples drawn from our interview data.

1. **Get It Done.** Unsafe practices that are justified by tight deadlines.
2. **Undiscussable Incompetence.** Unsafe practices that stem from skill deficits that can't be discussed.
3. **Just this Once.** Unsafe practices that are justified as exceptions to the rule.
4. **This Is Overboard.** Unsafe practices that bypass precautions considered excessive.
5. **Are You a Team Player?** Unsafe practices that are justified for the good of the team, company, or customer.

Get It Done. According to the results, 78 percent of respondents see their coworkers take unsafe shortcuts. What's more, 19 percent can cite an injury or death caused by one of these unsafe shortcuts. Yet only 25 percent of employees say they speak up and share their concerns with the person who is putting safety at risk. What is most astounding is that ***these common and risky shortcuts are undiscussable for 75 percent of the workforce.***

> *"When a welder tripped on a bleach hose, broke the nozzle, and was burned, the Emergency Response Team quickly shut off the valve to the bleach hose. Since they were in a rush, the leader of the team stood on a milk crate because he didn't feel he had time to get the appropriate equipment to reach the valve. The crate tipped over and the supervisor came down hard, ripping his protective suit and getting an even bigger burn than the welder had received."*
>
> —frontline employee in the chemical manufacturing industry

Undiscussable Incompetence. Sixty-five percent of respondents see their coworkers create unsafe conditions due to incompetence and 18 percent can cite an injury or death caused by incompetence. While 26 percent say they speak up and share their concerns with the person who is putting safety at risk, ***the remaining 74 percent of workers say safety risks sustained by incompetence are undiscussable.***

> *"Some people just don't get it. For example, when blocking a line, they'll just kink it rather than putting on a squeeze. The problem is that kinking the line could cause a static ignition, where a squeeze couldn't. We had it cause a fire out on the coast. One guy told me he thought static electricity works different here because we're inland. Yeah, okay. One of these days someone is gonna get themselves burned."*
>
> —frontline employee in the utility industry

Just this Once. The results confirm that 55 percent of respondents see their coworkers make unsafe exceptions and 18 percent can cite an injury or death caused by these exceptions. Despite the prevalence of this potentially fatal oversight, ***only one in four speak up and share their real concerns with the person who is putting safety at risk.***

> *"We had to change out one of the catalysts (a heavy industrial component). When we swapped it out, we put the wrong catalyst in and had to redo the job. This required moving a 150-pound cover. This is a job for a crane, but since we were trying to correct our mistake, we decided to remove the cover with a forklift. This was obviously against safety protocol. We ended up dropping the cover, damn near crushing our maintenance guy."*
>
> —frontline employee in the chemical manufacturing industry

This Is Overboard. The majority of respondents, 66 percent, see their coworkers violate safety precautions they've discounted; 22 percent can cite an injury or death caused by these violations. Yet ***close to three out of four either say nothing or fall short of speaking up candidly to share their real concerns.***

> *"One guy fell off his ladder and now we have a new ladder policy. You are always supposed to have someone hold the ladder as you ascend it, and then you're supposed to always tie the ladder off once you reach the top. If you're working on the ladder, you need to tie off on the ladder. Well, even though policy has changed, not many of us follow it. I'd say 75 percent of us still do it the old way. There's just not much danger in it. We're trained professionals. We know what we're doing."*
>
> —frontline employee in the oil and gas industry

Are You a Team Player? The data reveals 63 percent of respondents see their coworkers violate safety precautions "for the good of the team, company, or customer." What's more, 17 percent can cite an injury or death caused by these violations. And still, only ***28 percent say they speak up and share their concerns with the person who is putting the team at risk.***

> *"Sometimes we're expected to go into manholes with energized cable. This is not a safe practice and it's not in line with our policy, but our only alternative is to turn the power off, which would make our customers angry and wouldn't fly with management. So I go in and do the work anyway. It's my job to get the power on and that's what I'll do. I'm not gonna wimp out."*
>
> —frontline employee in the utility industry

Taken together, these five undiscussables account for a vast number of accidents waiting to happen. And it's not that the people who remain silent don't care. What we heard in our interviews wasn't bystander apathy; it was more like bystander agony. Employees describe themselves as "holding their breath," "feeling tortured as they watch," and "not able to watch" as their coworkers put themselves and others in danger. But regardless of their fear, employees don't speak up when faced with one of these five undiscussable situations. They don't think it's their role; they don't know how; and they are afraid of retaliation. The cultural norms, habits, and assumptions that exist "below-the-waterline" prevent employees from voicing concerns.

Learn from the Best, Teach the Rest

Notice that none of the examples above are completely undiscussable. There is always a minority, ranging from 25 to 28 percent, who say they are able to speak up effectively and address the unsafe situation. These few individuals have an amazing impact: 63 percent of the time they create a safer situation. This correlation makes sense. People who feel able to confront and resolve potential problems they see take action and make the environment safer for everyone. Consider one example of a peer addressing the incompetence of another frontline worker in a way that is both candid and respectful.

> *"I'd like to talk to you about an important concern. You may not realize it, but I think the way you do certain procedures puts yourself and the rest of the crew at risk. I really value our relationship and respect your experience and so I'd like to explore this issue with you. Can I explain what I'm seeing and get your point of view?"*

What is most important about an interaction like this is that it gets to the heart of the accident waiting to happen—the incompetent practice that puts others' safety at risk. An individual with the skills to speak up like this in crucial moments is essentially motivating the other person to behave differently based on the natural consequences of his or her behavior—in this case putting others at risk. Those who use this tentative approach, and other crucial conversations skills, find that their coworkers are more willing to listen and solve the problem.

Cultures of Silence vs. Cultures of Safety

Twenty-five years of research into the best practices of communicating in high-risk, highly emotional moments have taught us the problem is not that speaking up doesn't work, it's that speaking up doesn't happen. In these undiscussable moments, when it matters the most, most people do their worst at speaking up skillfully in a way that will be heard. Yet our research reveals that a select few who work side by side with the silent majority are able to voice their concerns, and by doing so, prevent accidents.

Organizations that train their employees to speak up when faced with the five undiscussables outlined in this report experience dramatic improvements in their safety record. For example, Pride International, a client of VitalSmarts, built a culture of safety where employees held their peers accountable to policies and procedures by speaking up in crucial moments. In the year following their training initiative, the offshore drilling contractor saw a 55 percent drop in their total incident rate and did not report a single accident where employees were required to take time off the job.

As our data and case studies suggest, widespread competence in these skills—along with other sources of influence required to ensure people use the skills—is the missing element of most safety cultures. When these "silent dangers" become discussable—when the norm changes from ignoring to confronting—the unsafe behavior stops. According to the research, when people speak up, 82 percent say their actions result in a safer work environment for everyone. The bottom line promise: *leaders who align the "below-the-waterline" cultural elements with the "above-the-waterline" formal elements reap huge advances in safety.*

So what will it take to move from risky silence to a culture of candor and accountability?

VitalSmarts has spent two decades studying this question. Our research has focused on what it takes to influence rapid, profound, and sustainable change in behavior in the face of deeply entrenched cultural norms. The results of that research were recently recognized by *MIT Sloan Management Review* as the "Change Management Approach of the Year." This research outlines the six sources of influence leaders must engage in order to influence and sustain the kind of behavior change we call for here—it requires a workforce that is both motivated and able to speak up when any of these five dangers exist.

> "All that is needed for evil to triumph is for good people to say nothing."
>
> —Elie Wiesel, Nobel Laureate

One of these sources of influence is personal ability. Organizations with strong cultures invest substantial resources in increasing the ability of individual employees to speak up skillfully and hold crucial conversations. But skills aren't all that is needed. The other five sources of influence described in the *MIT Sloan Management Review* article, when added to effective investments in increased ability, lead to substantial change in a relatively short period of time. And if leaders sustain the sources of influence required to change these behaviors, the new behaviors become the norm.

Nobel laureate Elie Wiesel once said, "All that is needed for evil to triumph is for good people to say nothing." The future of safety—not to mention the futures of four million workers who will otherwise be injured in the coming year—cannot be secured without a deep change in people's ability to step up to and hold the necessary crucial conversations. It is a change in behavior we are confident will leave organizations twice blessed—with a safer and more productive workplace.

VitalSmarts Can Help

Leaders need to make improving employees' skills one of their top priorities. The reluctance to speak up and confront coworkers is so deeply rooted in the safety cultures of organizations that it will take a concerted effort by leaders to create lasting improvements. Here are a few recommended next steps:

1. **Establish a baseline and a target for improvement.** The fundamental principle of organizational attention is that if you don't measure it, you don't care about it. Survey your organization to establish a baseline measure of the five crucial conversations for safety and set a clear target for improvement. To help you get started, we've created an organizational assessment that will uncover areas for improvement. **Access the assessment at www.vitalsmarts.com/safety.** Update the baseline at least quarterly so people can be rewarded and held accountable for progress.
2. **Teach your employees world-class skills.** A handful of people in your organization are already speaking up and preventing accidents from occurring around them. Training can be a powerful way to help others speak up and effectively address the five crucial conversations for safety.

   We've distilled this high-leverage skill set into our award-winning training programs, Crucial Conversations and Crucial Confrontations Training, and the *New York Times* bestselling books of the same titles. These resources have a proven track record of leading organizations to results, and when safety is in question, results don't just mean improvements in quality, efficiency, or morale—results equate to saved lives. See **www.vitalsmarts.com/safety** to get started.
3. **Target six sources of influence.** Once you've taught your employees crucial skills, guarantee the success of your training initiative by identifying the few vital behaviors that, if changed, will lead to the safety results you desire. Then, ensure these behaviors are adopted by targeting six sources of influence that both motivate and enable your employees to change. When used appropriately, this influence process will increase your chances of a successful culture change tenfold.

For a complete description of the six sources of influence, as well as instructions for how to apply the "Change Management Approach of the Year" in your organization, see **www.vitalsmarts.com/influencerreport**.

To register for a safety Web seminar or find out how VitalSmarts can help you build a culture of safety, visit **www.vitalsmarts.com/safety** or call 1.800.449.5989.

MANAGING REPUTATIONAL RISK FOR HIGHER EDUCATION

NEW MEXICO HIGHER EDUCATION SYPMPOSIUM

APRIL 3-5, 2019

KELLY ALLEN, VICE PRESIDENT, CIC

WEST BY SOUTHWEST HIGHER EDUCATION PRACTICE LEADER

REPUTATIONAL RISK

- "The way to a good reputation is to endeavor to be what you desire to appear" - Socrates

- "Character is like a tree and reputation is like a shadow. The shadow is what we think of it; the tree is the real thing." - Abraham Lincoln

- "It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently." - Warren Buffet

1. What is Reputation Risk?

Reputation

is about the **perception by others** and the danger of loss or opportunity of gain that such perception provides to such entity, thing or person.

REPUTATION + RISK =

THE PERCEPTION OF OTHERS THAT CAN IMPACT OBJECTIVES

AGENDA

- 1. Define Reputational Risk
- 2. Sources of Reputational Risks
- 3. Recent Events in Higher Education
- 4. What are the costs associated with these events
- 5.Managing your institution’s Reputation

2. SOURCES OF REPUTATIONAL RISK

- Athletics
- Student Life
- Sexual Assault /Title IX
- Cyber Security / Data Breaches
- Institutional Management

ATHLETICS

Coach and Staff Behaviors

Institutional Cultural "Understandings"

Athlete Behaviors

Athlete Safety

Recruiting Methods

Team Transportation

STUDENT LIFE RISKS

- Behaviors
  - Student Organizations – Controversial Speakers, Dangerous Activities
  - Mental Health – Adequate Management
  - Drug and alcohol use, prevention and response
- Sexual Assault and Title IX
  - Changing regulations make it challenging for Institutions to maintain consistent best practices
  - Perception from the public – Is the institution doing enough
  - Prevention and response for misconduct –Does the punishment adequately match the crime?

STUDENT SAFETY

- Diversity and inclusion of students, faculty, and staff
- The Equity and Diversity focus area emphasizes social justice and the continued diversification in today's higher education environment.

  Gender Identification, Gender equity, Sexual Orientation, Race, Nationality
- The prevalence of Social Media
- The rate at which negative information can be disseminated into the public

DATA BREACHES NEGATIVELY IMPACT THE INSTITUTIONS REPUTATION

- Data breaches continue to happen at colleges and universities across the country at alarming rates.
- They are targeted nearly as often as financial institutions
- Data storage, transmission, and collection points and the use of handheld and portable devices adds to the vulnerability
- Data Breaches are expensive and time consuming to the institution to manage
- They cause people to feel violated and unsafe
- These attacks not only cause current and prospective students concern but also have an impact on potential donors sense of security

3. EVENTS IN HIGHER ED

University of North Carolina at Chapel Hill Football Scandal

Penn State Sex Scandal

University of Louisville Basketball Scandal

Baylor University Sexual Assault Scandal

Duke LaCrosse Rape

Admissions practices investigations at prominent Universities

4. COSTS ASSOCIATED WITH REPUTATIONAL RISK

- Reduced Enrollment
- Reduction in Donations
- Loss of

5.MANAGING YOUR INSTITUTION’S REPUTATION

Have a common understanding of the institutions reputation

Identify and manage risk portfolio

Assess culture and work to improve where weakness is identified

Question patterns and practices when they don’t make sense or “feel” right

Develop a chain of command and establish ownership

Self-Insurance Pool Rate Development

MUJTABA DATOO ACAS, MAAA, FCA
ACTUARIAL PRACTICE LEADER

APRIL 5, 2019

Aon Global Risk Consulting
17875 Von Karman Ave, Suite 300, Irvine, CA 92614
(949) 608-6332 | mujtaba.datoo@aon.com
www.aon.com

Empower Results®

5 Principles of Cost Allocation

- Ease of understanding
- Budget stability
- Fairness and objectivity
- Responsiveness to loss experience
- Measurement of exposure and experience

5 Principles of Cost Allocation

1. Ease of understanding

- Department heads must be able to easily understand the cost allocation plan and the data it relies upon
- If not, they will not understand the actions they must take to reduce costs

Empower Results®

5 Principles of Cost Allocation

2. Budget stability

- Must be responsive to changes in a department's losses and operations, and yet provide some year-to-year stability.
- New Mexico caps losses
    - 5% of department budget
    - Minimum $2,500 and Maximum $1,000,000

5 Principles of Cost Allocation

3. Fairness and objectivity

- Most successful cost allocation plans rely on data that is easily verifiable, difficult to manipulate and readily available
- Consider data used, objectivity, fairness, frequency of plan changes and how results are presented to departments

5 Principles of Cost Allocation

4. Responsiveness to loss experience

- Reflects responsiveness to claims frequency and claims severity.
- Must achieve a balance between responsiveness and stability.

5 Principles of Cost Allocation

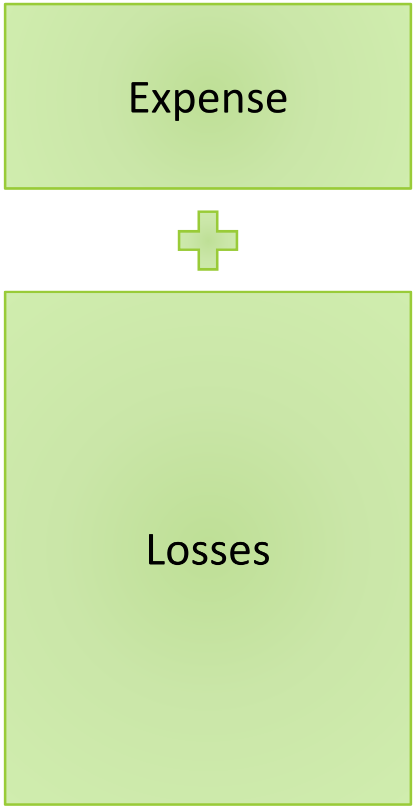
5. Measurement of exposure and experience

- Balance (1) exposure to loss (e.g., payroll for workers compensation) and (2) loss experience
- Weight exposure and experience
  - Weights can vary based on exposure size, or
  - Fixed weights to exposure and experience
- NM weights:
  - WC: 90% losses & 10% exposure
  - Liability: 70% losses & 30% exposure
  - Property: 30% losses & 70% exposure

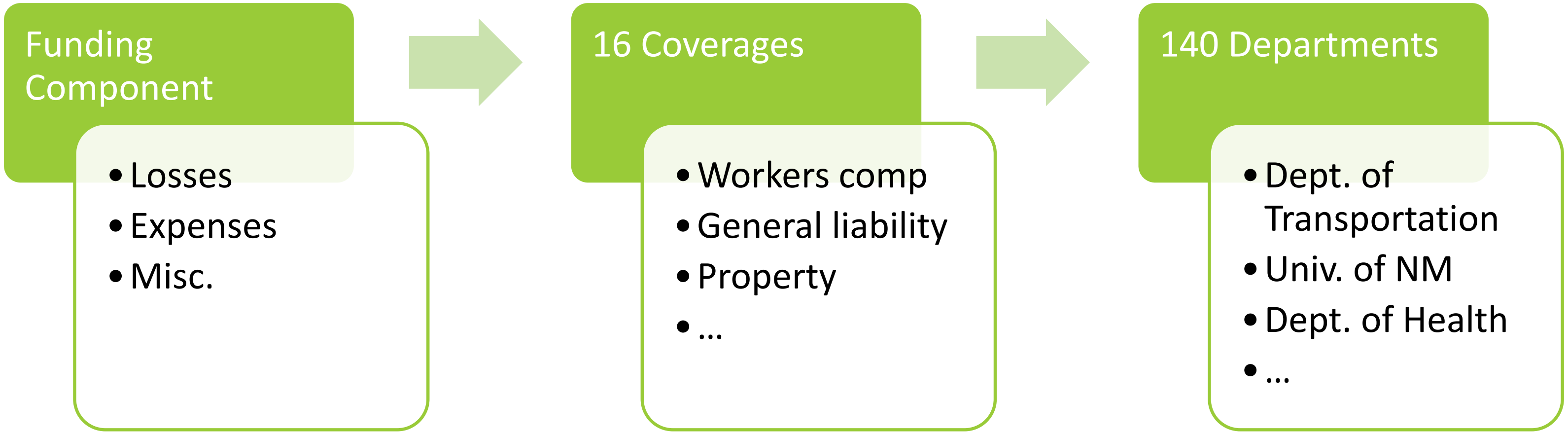
Regulatory Guidelines

- Established in June 1997 by General Services Department, Risk Management Division
  - Title 1 – General Government Administration
  - Chapter 6 – Risk Management
  - Part 2 – Premium rating for Certain Risks
- Sets out rules:
  - Data to use
  - Structure to follow
  - Gives Director various discretionary authority

Funding Components



Rate Components



Funding Component

- Losses
- Expenses
- Misc.

16 Coverages

- Workers comp
- General liability
- Property
- …

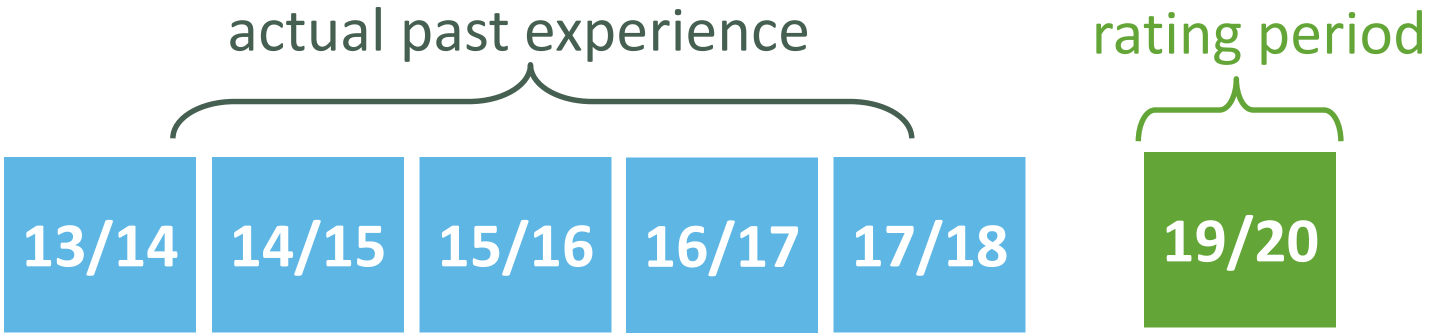
140 Departments

- Dept. of Transportation
- Univ. of NM
- Dept. of Health
- …

Empower Results®

Losses

- 5-year incurred losses
- Cap
  - 5% of department budget
  - Minimum $2,500 and Maximum $1,000,000



actual past experience

rating period

13/14 14/15 15/16 16/17 17/18

19/20

Adjusting Losses to Projected Period

- Adjust 5-year incurred losses to ultimate settlement
  - Apply loss development factor as if all closed at final settlement value
  - Apply trend factor (CPI)

- Example: WC

5-year average incurred losses:		$11.8M
Loss development factor:		1.3
Trend factor:		2.8%
Total:	$11.8M x 1.3 x 1.028 =	$16M

Expenses

- Excess insurance
- Admin
- Misc. – unfunded liability

Empower Results®

Unfunded Liability @6/30/18

Assets available	$116M
Estimated outstanding losses	$138M
Unfunded liability	-$22M

Empower Results®

Minimum Premium

- Each coverage has a minimum premium
- Ranges from $100 (property) to $1,000 (med mal)

Illustration of Allocation

WC

Dept	Latest Payroll	% Payroll	5-yr Avg. Expected Losses	% Losses	Premium = 90% to losses + 10% to payroll
A	18M	0.6%	0.8M	1.4%	$0.2M
B	209M	6.7%	7.9M	13.5%	$2.3M
C	248M	7.9%	5.5M	9.5%	$1.7M
…	…	…	…	…	…
Total	3,127M	100%	58M	100%	$17.9M

Pay As You Go

- 2 types of funding losses
    - Accrual funding
    - Pay-as-you-go
- Losses projected are a proxy of what is expected to be paid out in 2019/20

Budgetary Process

- Risk Management proposes budget
- GSD submits to Finance Legislative Committee
- Legislature approves final budget
- Department contributions adjusted up/down to meet overall approved budget

Summary

- Overall budget is an estimate
  - Future losses are variable, and forecasted
  - Expenses are less variable
- Reasonable to meet budgetary objective
- Allocate overall budget to departments
  - Stable and equitable
  - Outliers can be discretionarily adjusted by the Director

Questions?

Mujtaba Datoo, ACAS, MAAA, FCA
Actuarial Practice Leader
Aon Global Risk Consulting
(949) 608-6332
mujtaba.datoo@aon.com

Empower Results®

Thank you!

Empower Results®

EMPLOYERS UNITY LLC

UNEMPLOYMENT WORKSHOP

EMPLOYERS UNITY LLC

OBJECTIVES OF THE EMPLOYERS UNITY, LLC PROGRAM

- Reduce unemployment expenditures
- Reduce administrative costs
- Keep management advised with detailed and accurate information

DID YOU EVER HEAR?

I’ve paid into the system my whole life, so why not draw benefits

If I quit, I cannot draw benefits, but if you fire me, I will get benefits

The last employer I worked for pays all my benefits

We quit contesting claims because the employer never wins

EMPLOYERS UNITY LLC

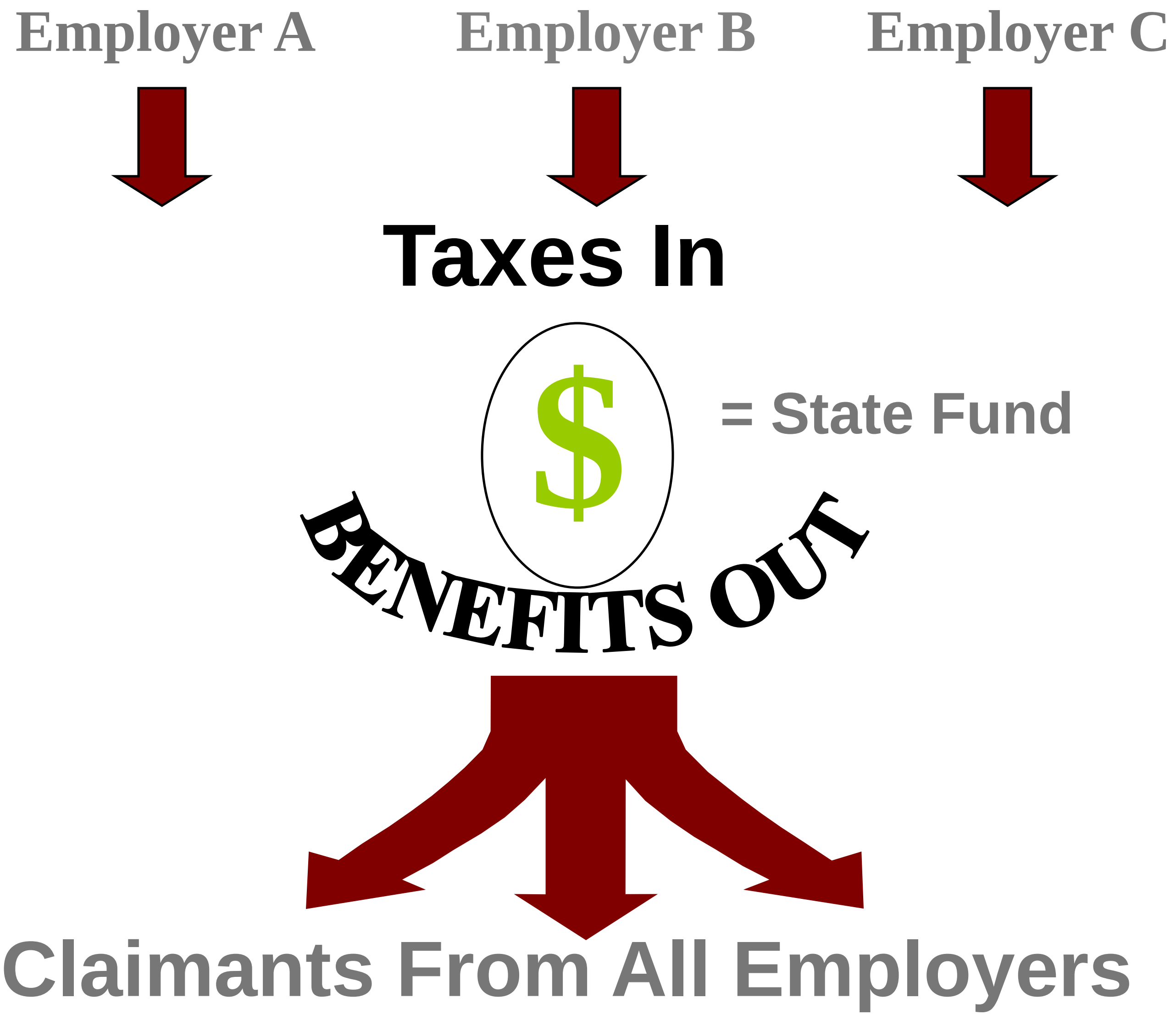
PROGRAM HISTORY

- 1935 Social Security Act
- Federal Unemployment Tax Act (FUTA)
- States Empowered – Laws Vary, but Must Conform to Federal

UNEMPLOYMENT PROGRAM PURPOSE

- To Provide Subsistence to Those Who are Involuntarily Unemployed Through No Fault of their Own

STATE HISTORY



Employer A

Employer B

Employer C

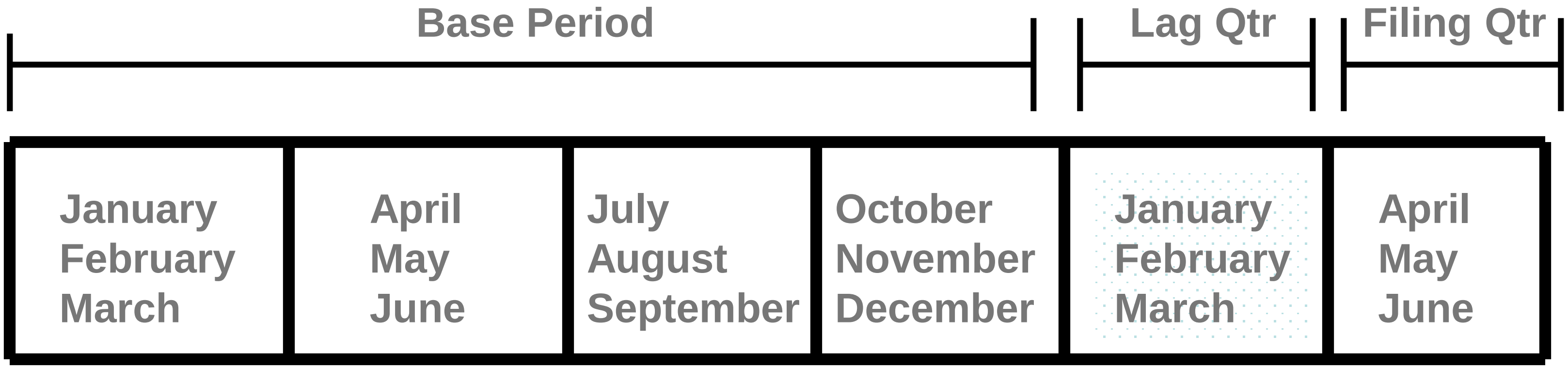
Taxes In

$ = State Fund

BENEFITS OUT

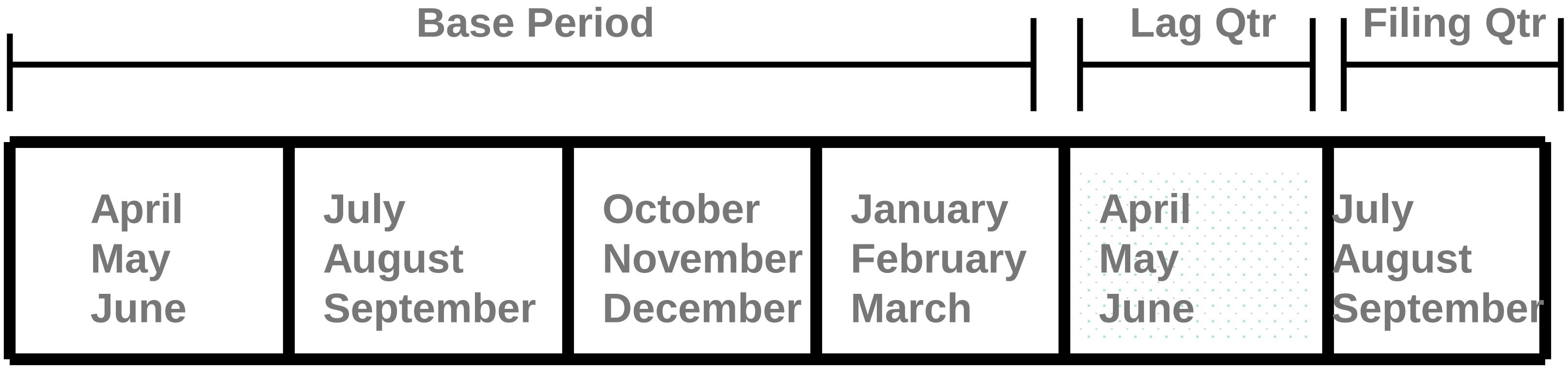
Claimants From All Employers

BASE YEAR EXPLANATION



Base Period				Lag Qtr	Filing Qtr
January February March	April May June	July August September	October November December	January February March	April May June

BASE YEAR EXPLANATION



Base Period				Lag Qtr	Filing Qtr
April May June	July August September	October November December	January February March	April May June	July August September

Weekly Benefit Amounts

Maximum WBA $442.00

Maximum claim $11,258

Minimum WBA $84.00

THREE TYPES OF SEPARATIONS

Lack of Work

Voluntary Quit

Discharge

VOLUNTARY QUITS

- Medical Related
- Substantial Changes in Hire Agreement
- Reduction in Hours/Pay (Partial)
- Another Job/Better Job
- Job Abandonment
- Relocating
- Personal Reasons
- Dissatisfaction
- Quit in Lieu of Discharge

DISCHARGES

- Unable to perform
  - inefficiency
  - inadequacy
  - incompetent
  - failure to perform
  - unable to live up to standards & expectations
  - NO misconduct

- Unwilling to perform
  - violation of rules, policies, regulations
  - intentional disregard
  - insubordination
  - burden of proof
  - documentation
  - verbal & written warning

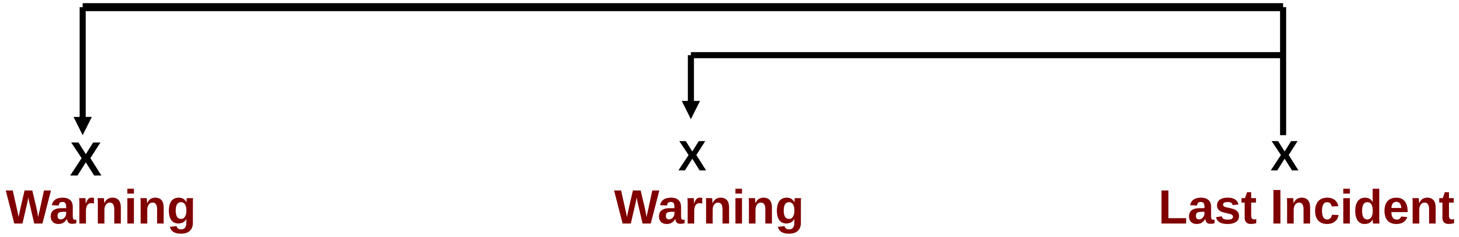
THREE PARTS OF A WARNING

- The violation
- Expected action or how to improve
- The consequences

DISCHARGES

- Final incident/triggering event
  - Quick decision must be made…do not keep employee on until a replacement is found
  - Event should be an issue in which they have been previously warned…(see policy), and not a mix
  - Timing on absenteeism/tardiness issues
  - Use clear, distinct & precise terminology to describe separation to employee

LAST INCIDENT



X
Warning

X
Warning

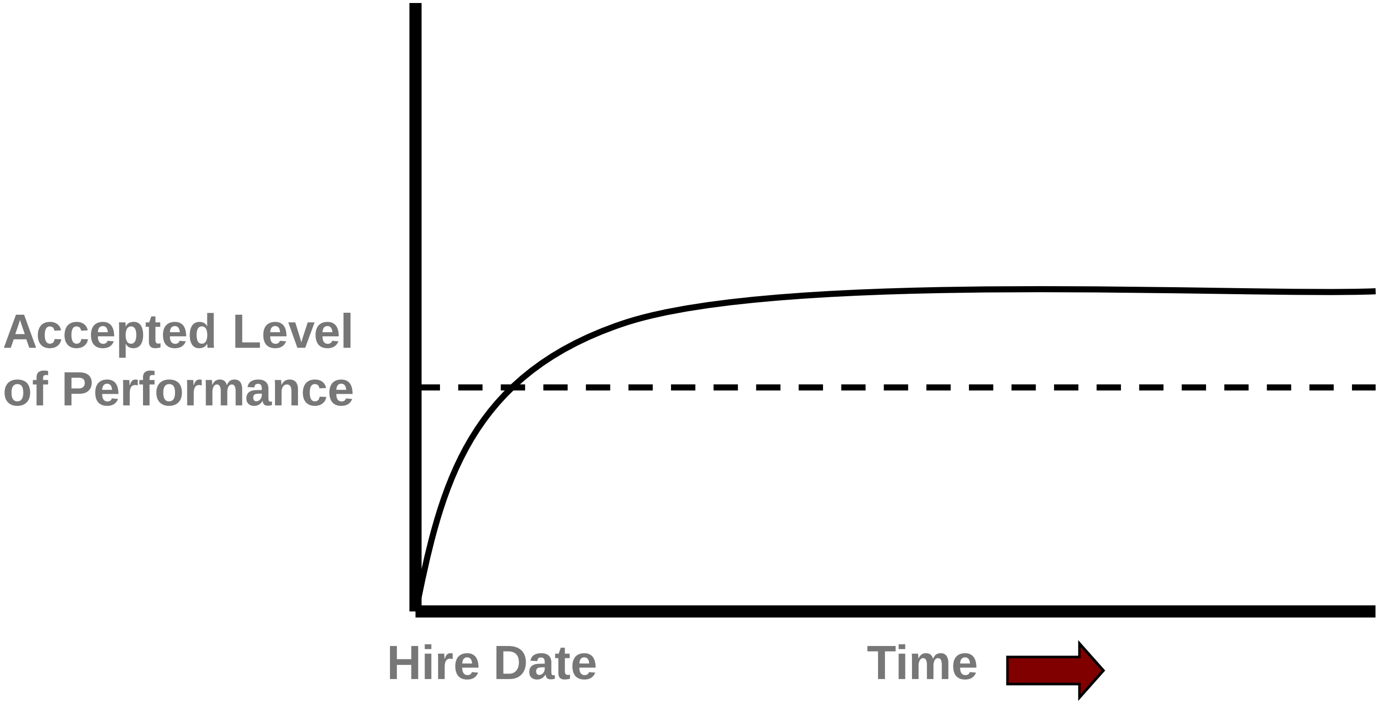
X
Last Incident

The last incident and prior warnings must be in the control of the claimant

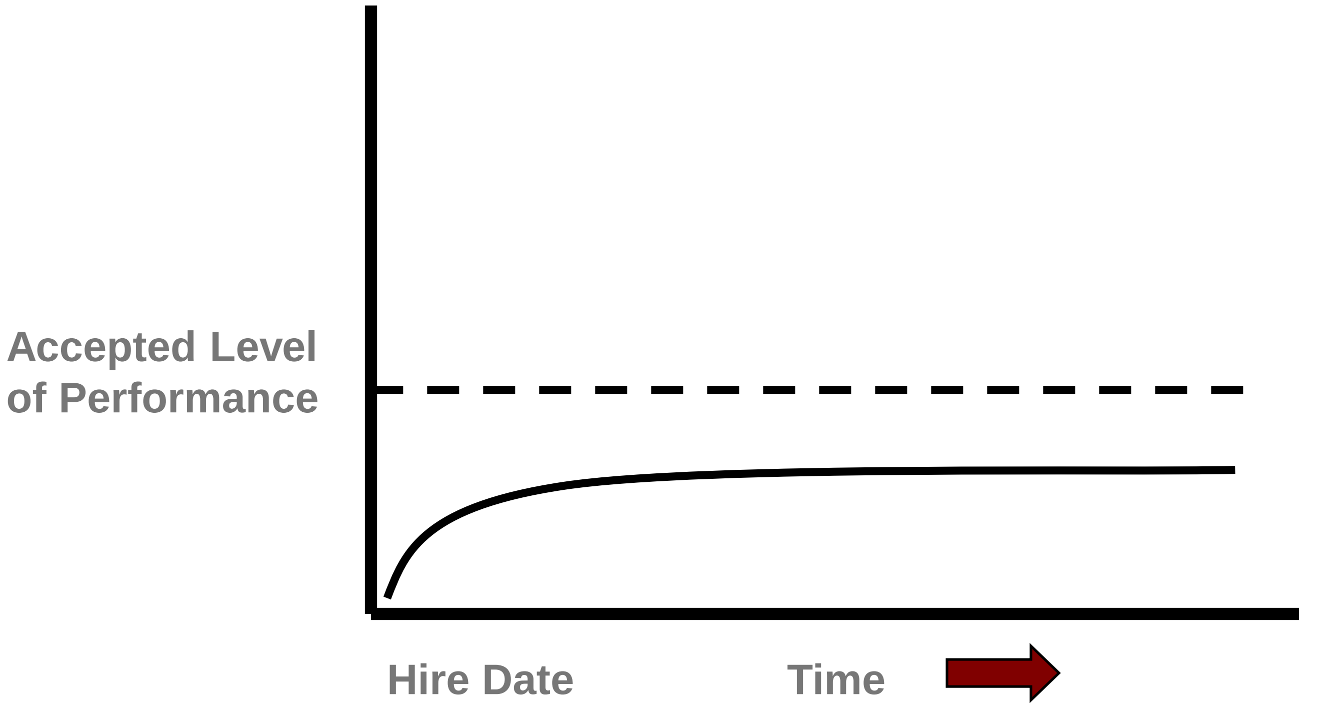
The last incident must relate to previous warnings, unless gross misconduct

During the hearing, testimony will start at the final incident and proceed in reverse chronological order.

THE GOOD EMPLOYEE

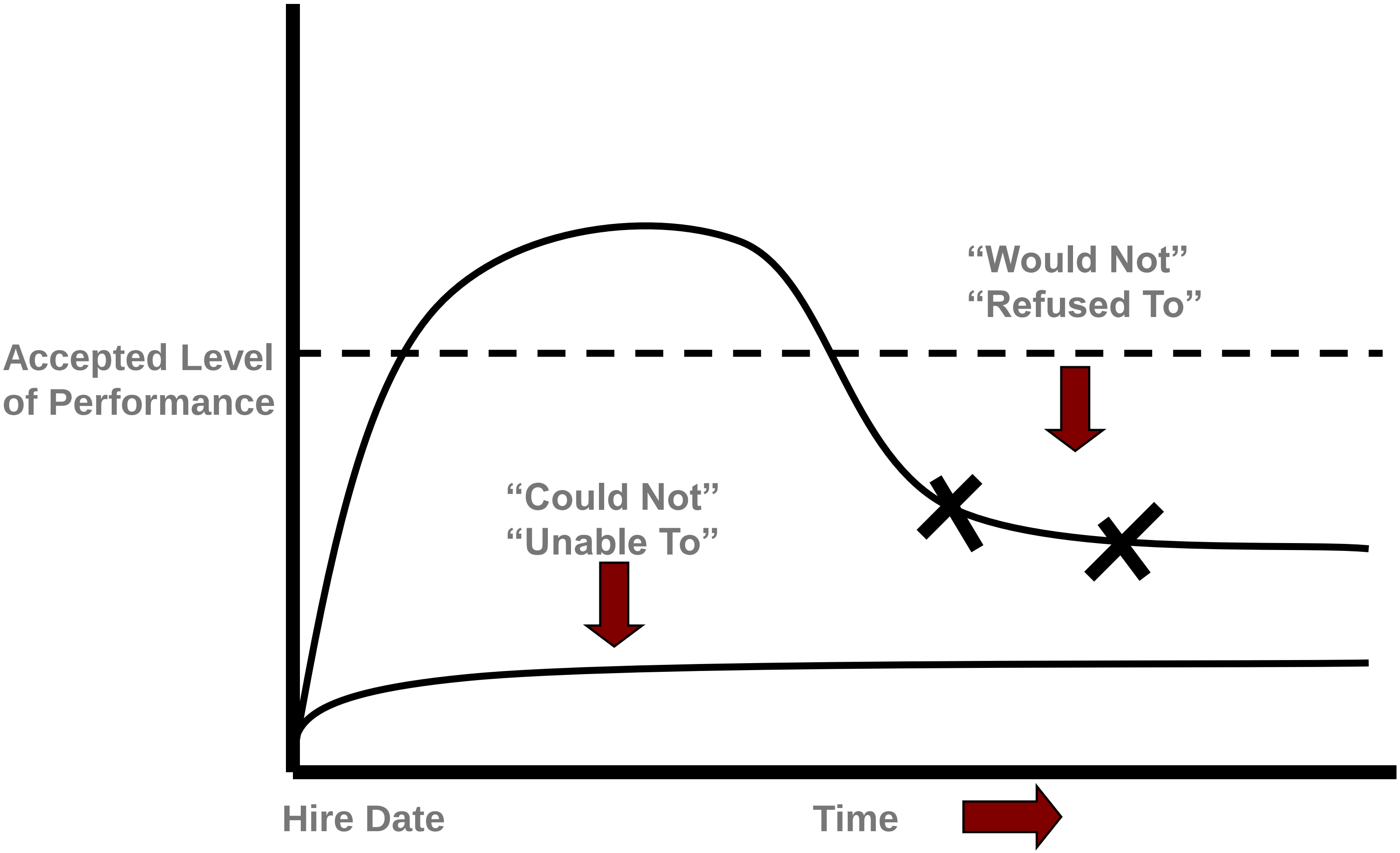


THE UNQUALIFIED EMPLOYEE



An unable or unqualified employee
The employer cannot prevail in an unemployment claim

TERMINOLOGY



Accepted Level of Performance

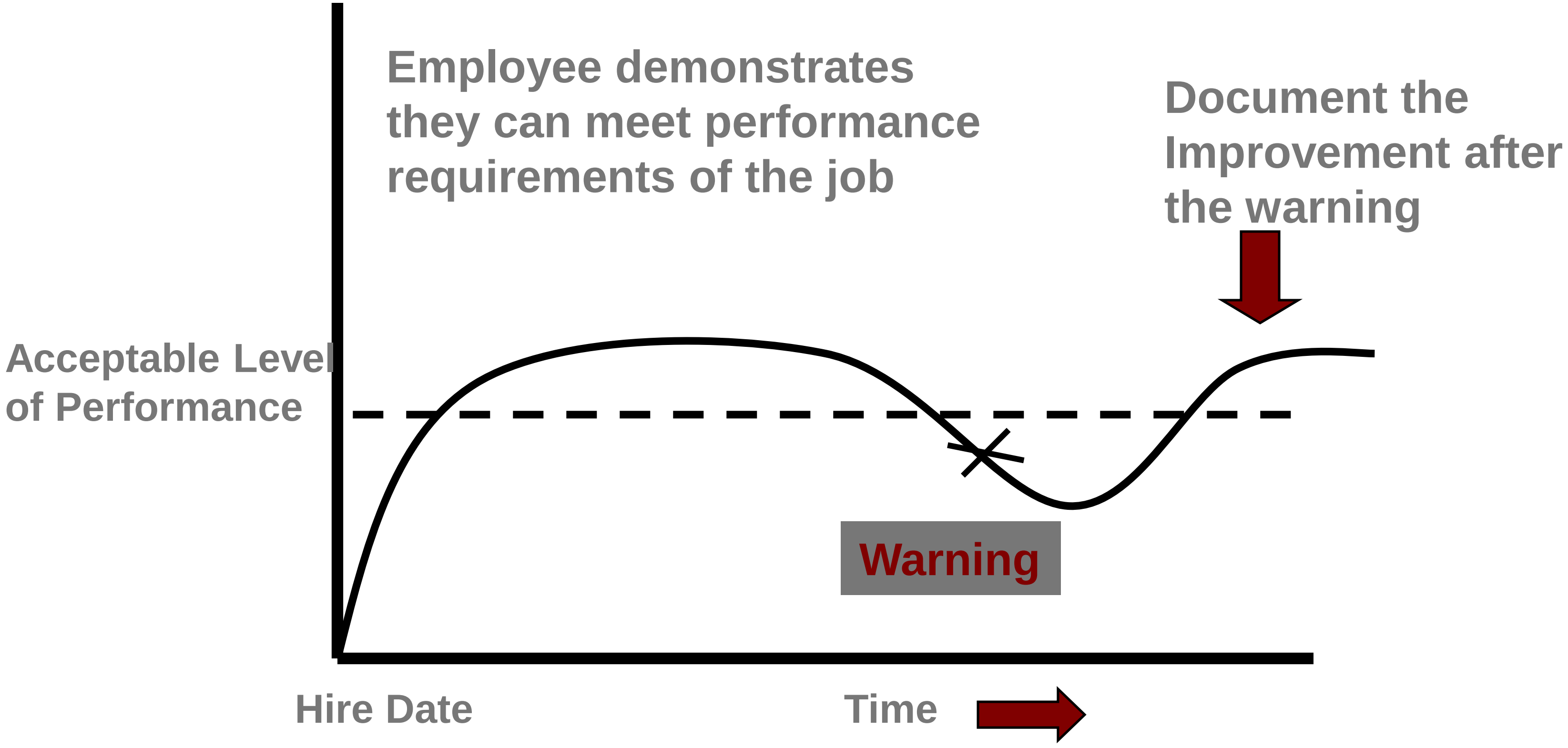
“Would Not”
“Refused To”

“Could Not”
“Unable To”

Hire Date

Time

WARNINGS



Employee demonstrates they can meet performance requirements of the job

Document the Improvement after the warning

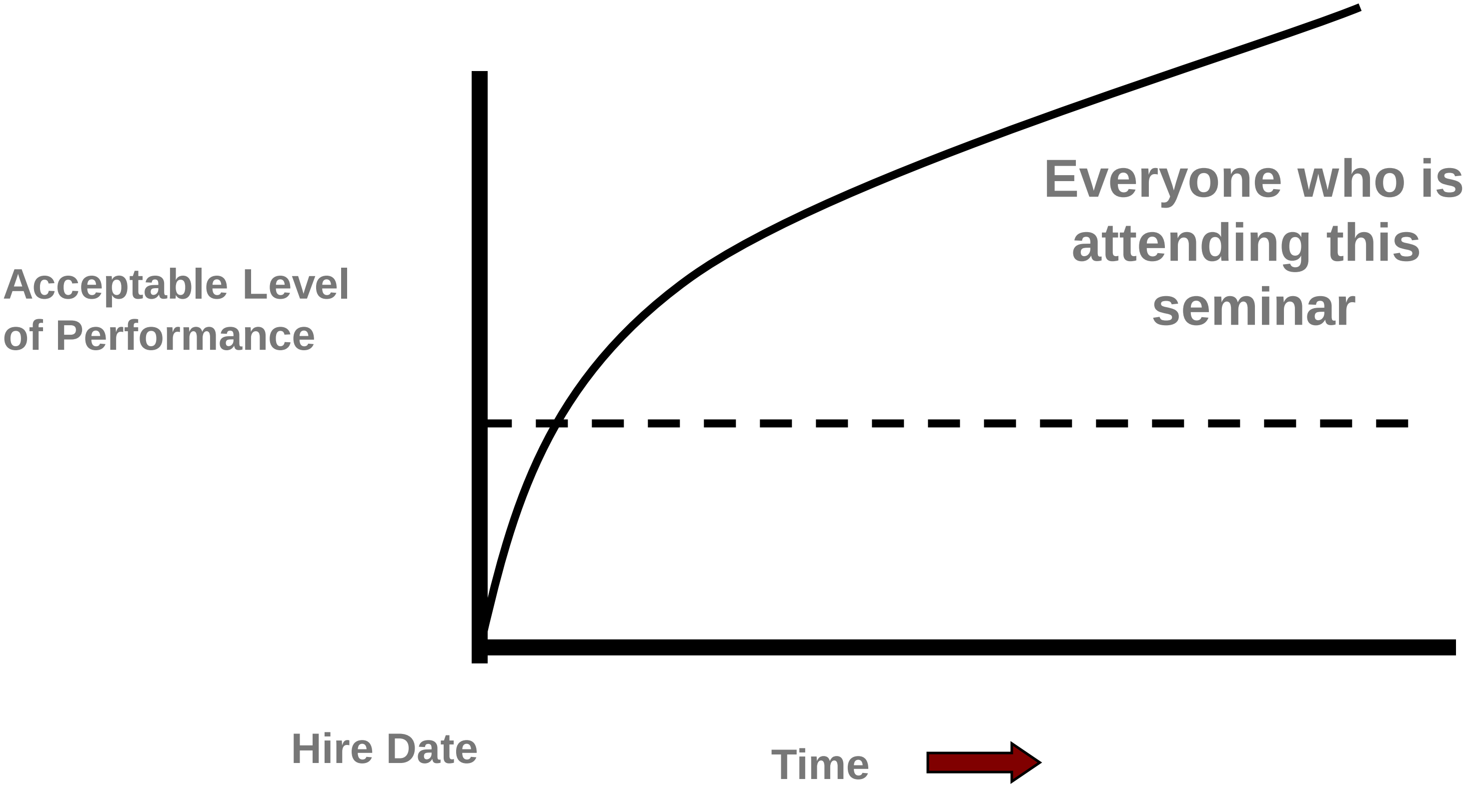
Acceptable Level of Performance

Warning

Hire Date

Time

THE GREAT EMPLOYEE!



Everyone who is attending this seminar

Acceptable Level of Performance

Hire Date

Time →

EXPLAIN THE LAST INCIDENT IN DETAIL

Examples of what Managers have turned in to EU in the Past

- Let go for not being a team player
- Let go for a bad attitude
- Let go for using foul language
- Let go for being late too often
- Let go for mistakes in everyday duties
- Let go for poor job performance

EMPLOYERS UNITY LLC

CONTRADICTIONS

Evaluations

vs.

Warnings

Probationary/Performance Plan Periods

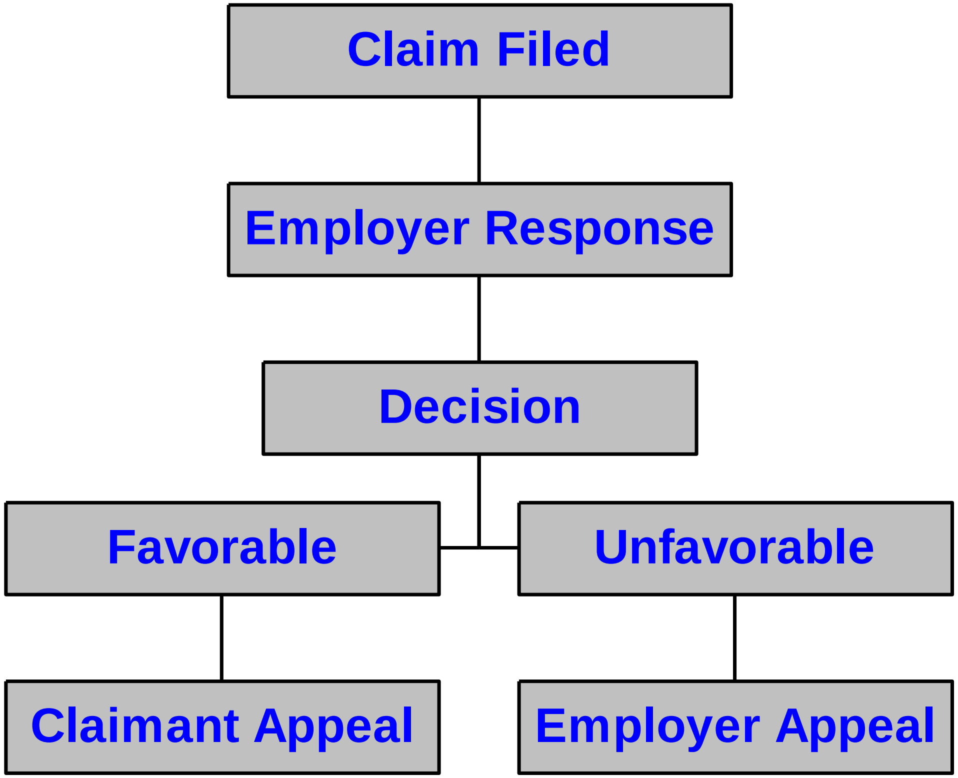
vs.

Promise of Employment & Last Incident

TO RECEIVE BENEFITS AS A CLAIMANT

- Must be available for full-time work
- Must be physically able to work
- Must be actively seeking work

CLAIMS PROCESS



Claim Filed

Employer Response

Decision

Favorable

Unfavorable

Claimant Appeal

Employer Appeal

Information Needed Upfront on Initial Protest

Many states are excluding the employer from being a party to the claim if their initial protest is generic or lacking enough detail

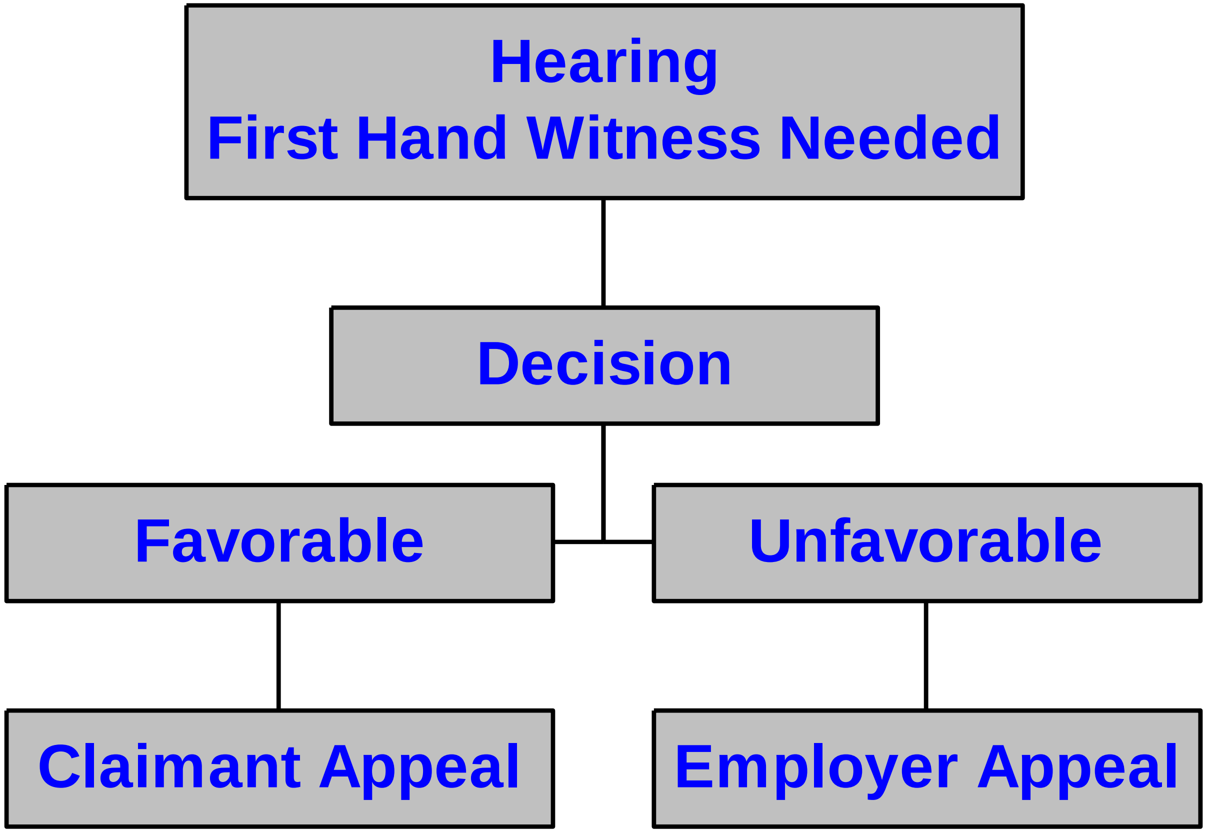
Employers Unity needs ***ALL*** details of incident for our initial protest

- If Discharge-
  - Copies of ***<u>relevant</u>*** warnings
  - Copies of detailed separation documents
  - Any exhibits that pertain to separation (handbook policies, witness statements, audio/visual, etc)
- If Voluntary Quit
  - Copies of resignation letter/email
  - Separation notice if signed or refused to sign –in lieu of resignation letter, witness statements from person/s that heard the person quit if nothing in writing

THE UNEMPLOYMENT HEARING

- Five basic questions about ex-employee
  - first day worked
  - last day worked
  - position/job description
  - rate of pay at time of separation
  - REASON for separation
    - quit?
    - discharge? - why? Be VERY specific
    - layoff?

HEARING PROCESS



Hearing
First Hand Witness Needed

Decision

Favorable

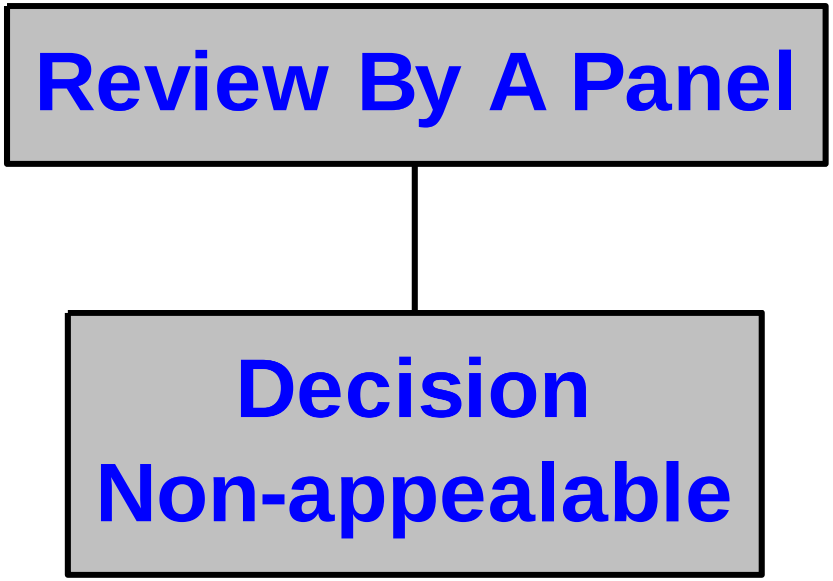
Unfavorable

Claimant Appeal

Employer Appeal

INFORMATION OBTAINED AT THE HEARING WILL BE UTILIZED BY THE BOARD OF REVIEW WITHOUT AN OPPORTUNITY FOR ANY ADDITIONAL FACTS.

BOARD OF REVIEW

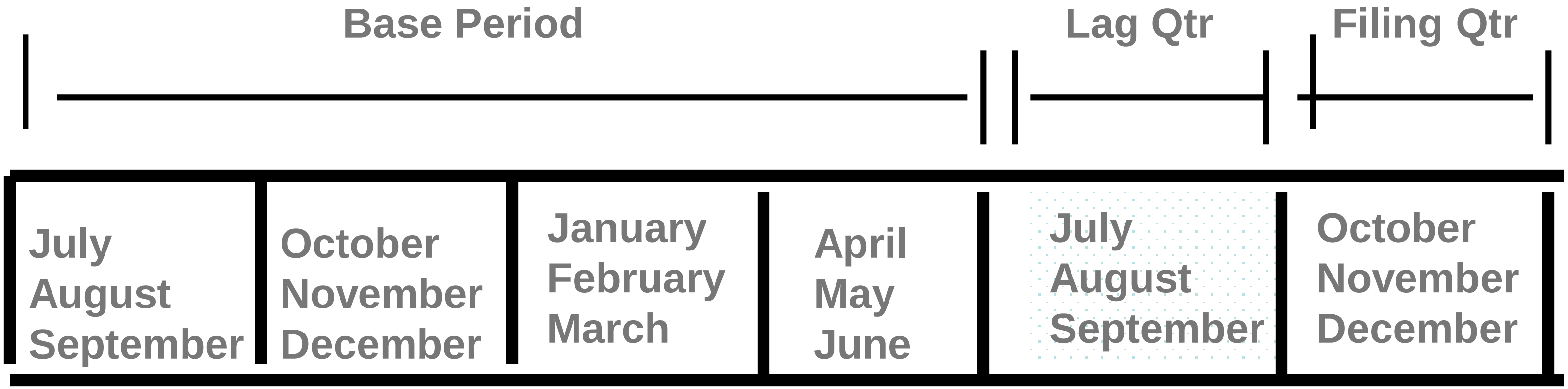


Review By A Panel

Decision
Non-appealable

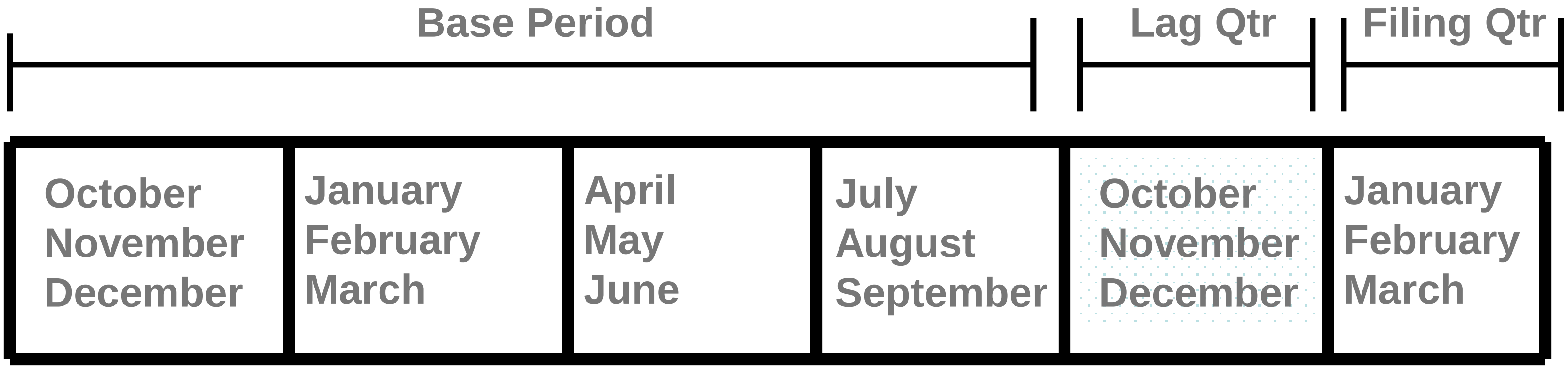
The recommendations made by Employers Unity, LLC. and your account manager are for unemployment insurance purposes only. There may be occasions that arise where the recommendations may not meet the best course of action required when dealing with other types of issues and/or legal matters. These issues should be taken to your own legal counsel. Once again, these recommendations are for the best handling of an unemployment claim only and are not legal advice in whole or part.

BASE YEAR EXPLANATION



Base Period				Lag Qtr	Filing Qtr
July August September	October November December	January February March	April May June	July August September	October November December

BASE YEAR EXPLANATION



Base Period				Lag Qtr	Filing Qtr
October November December	January February March	April May June	July August September	October November December	January February March

Presenter	Email	Phone
#1: Corey McDowell Laura K. Vega	cmcdowell@allenlawnm.com lvega@allenlawnm.com	
#2: Leland Frische	lfrische@cnm.edu	505-224-4438
#3: Ryan Mercer	Ryan.mercer1@aon.com	312-381-9587
Lunch: Jaime L. Phillips	Jaime.phillips2@state.nm.us	
#4: Anne Mulholland	Anne.mulholland@aon.com	312-381-3963
#6: Mary Beth Stevens	marybeth@lanl.gov	
#8: Kelly Allen	Kelly.allen3@aon.com	503-306-2839
#9a: Mujtaba Datoo	Mujtaba.datoo@aon.com	949-608-6332
#9b: Bob Nellans	rnellans@employersunity.com	