prima

USING ARTIFICIAL INTELLIGENCE TO IMPROVE SAFETY PERFORMANCE

PRESENTATION FOR THE MEMBERS OF PRIMA PUBLIC RISK MANAGEMENT ASSOCIATION

AUGUST 20, 2025

SPECIAL THANKS TO PRIMA

- THANK YOU TO PRIMA FOR LEADING INNOVATION IN PUBLIC RISK
- HONORED TO SPEAK

MEET YOUR SPEAKERS

- KARL MILLER
- ANGELO LOSARDO

WHAT WE'LL COVER

1. HOW AI ADVANCEMENTS CAN IMPROVE WORKPLACE SAFETY

2. TOOLS AND TECHNOLOGIES FOR SAFER PERFORMANCE

3. BALANCING AI WITH EMPLOYEE INTEREST

4. UTILIZING AI WITH HISTORICAL DATA TO PREDICT POTENTIAL HAZARDS

WHAT YOU'LL LEAVE WITH

- BETTER UNDERSTANDING OF PRACTICAL AI TOOLS THAT WORK

- HOW TO DEPLOY AI RESPONSIBLY

- PREDICTIVE SAFETY STRATEGIES

BONUS: AI POLICY TEMPLATE

- PRACTICAL GUIDE FOR SAFE, ETHICAL AI USE

- INCLUDES RISK, ETHICS, AND COMMUNICATION TIPS

- PROVIDED FREE TO ATTENDEES
  - MORE INFORMATION AT THE END

AI OVERVIEW

- AI = MACHINES THAT LEARN, DETECT, RESPOND

- IN SAFETY: HELPS US SEE WHAT HUMANS MISS

- GOAL: PREDICT, PREVENT, PROTECT

PART 1:

HOW AI ADVANCES CAN IMPROVE WORKPLACE SAFETY

- AI HAS PROVEN TO BE A POWERFUL TOOL IN ADVANCING AND PROMOTING WORKPLACE SAFETY – FROM SECURITY CAMERAS TO ROBOTIC BOMB DETECTION AND DEFUSEMENT, ARTIFICIAL INTELLIGENCE IS PROVING TO BE AN IMPORTANT ALLY TO HUMAN INVOLVEMENT IN MITIGATING RISK

ABILITY TO DETECT HAZARDS IN REAL TIME

- CAMERAS AND SENSORS MONITOR SPILLS, GAS LEAKS, EQUIPMENT MALFUNCTIONS

- AID IN PROMOTING RESPONSE TO SITUATIONS THAT DO/CAN JEOPARDIZE EMPLOYEE OR STRUCTURAL SAFETY

SECURITY SURVEILLANCE AND ALERTS

- ABILITY TO MONITOR ACCESS TO RESTRICTED AREAS

- DETECTION DEVICES FOR PUBLIC EVENTS WHICH ARE POTENTIAL TERROR TARGETS

- FOREIGN OBJECT RECOGNITION

- HAZARD DETECTION

AUTOMATING HAZARDOUS TASKS

- ROBOTICS: BOMB DETECTION, ENVIRONMENTAL CLEAN UP

- LIFTING, HANDLING HEAVY/DANGEROUS MATERIALS

- BIOHAZARD DETECTION SYSTEM - IMPLEMENTED BY US POSTAL SERVICE AFTER ANTHRAX SCARE (2001)

SAFETY TRAINING

- VIRTUAL REALITY CAN CREATE SIMULATED EXPERIENCES TO TRAIN AND TEST ABILITY OF WORKERS WHO ARE ACTIVE IN CERTAIN ENVIRONMENTS

- DATA ANALYSIS OF WORKPLACE INCIDENTS CAN CONTRIBUTE TO THE DEVELOPMENT OF TRAINING AND MONITORING PROGRAMS THAT IS MORE JOB-SPECIFIC, HAZARD FOCUSED

PREDICTIVE ANALYSIS

- DATA GATHERING AND CULLING CAN HELP DETERMINE PATTERNS, HAZARDS TO PREDICT POTENTIAL RISKS AND HAZARDS TO BOTH EMPLOYEES AND THE PUBLIC BEFORE AN OCCURENCE

- MEASURING TRAFFIC DATA, VEHICLE REPAIR/USAGE INFORMATION AS A TOOL WITH FLEET AND HEAVY EQUIPMENT MANAGEMENT

- TRACKING TOOLS MONITORING DRIVING PATTERNS

TRACKING EMPLOYEE PERFORMANCE

- MODERN WEARABLES – EVERYTHING FROM HELMETS, SENSORS, BIOMETRIC TRACKERS

- WEARABLE TOOLS HELP REDUCE INJURY RATES, IMPROVE ERGONOMICS, PROVIDE BETTER RESPONSE TIMES, CONTRIBUTE TO PRODUCTIVITY

AUTOMATED REPORTING AND ANALYSIS

- AI HELPS IMPROVE THE COLLECTING, ANALYZING AND REPORTING OF WORKPLACE INCIDENTS

- CAN HELP IDENTIFY CAUSES AND TRENDS

- HELP ENSURE COMPLIANCE WITH REGULATIONS

PART 2:

TOOLS AND TECHNOLOGIES FOR SAFETY

AI TOOLS ALREADY HERE

- "AI IN SAFETY ISN'T SCIENCE FICTION—IT'S HERE"

- EVERYDAY PLATFORMS ARE EVOLVING INTO PREDICTIVE DEFENSE SYSTEMS

- FROM SPAM FILTERS TO BEHAVIORAL ANALYSIS—AI IS ALREADY BUILT IN

MICROSOFT 365 DEFENDER

- FLAGS UNUSUAL ACTIVITY (E.G., 3 A.M. LOGIN FROM A FOREIGN IP)

- UNDERSTANDS CONTEXT—DISTINGUISHES TRAVEL FROM TRUE THREATS

- REDUCES FALSE ALARMS, INCREASES TRUST IN ALERTS

PROOFPOINT

- DETECTS PHISHING ATTACKS TRADITIONAL FILTERS MISS

- LEARNS YOUR ORGANIZATION'S NORMAL COMMUNICATION PATTERNS

- FLAGS SUBTLE ANOMALIES IN TONE, TIMING, OR SENDER BEHAVIOR

BENEFITS OF SMART TOOLS

- FILTERS OUT FALSE POSITIVES, REDUCING ALERT FATIGUE

- SCALES TO MONITOR THOUSANDS OF EVENTS IN REAL TIME

- ADAPTS TO YOUR ORGANIZATION'S BEHAVIOR OVER TIME

CASE STUDY – INSIDER THREAT PREVENTION

- OFF-HOURS SHAREPOINT ACCESS TRIGGERED ANOMALY DETECTION

- AI ANALYZED LOGIN TIME, LOCATION, AND ACCESS TYPE AGAINST TYPICAL USER BEHAVIOR

- IDENTIFIED DEVIATIONS THAT MANUAL MONITORING MIGHT OVERLOOK

CASE STUDY – STOPPING AN INSIDER THREAT

- EARLY ALERTS ALLOWED SECURITY TEAM TO INTERVENE BEFORE ANY DATA WAS COMPROMISED

- MACHINE LEARNING MODEL IMPROVED ACCURACY OVER TIME, REDUCING FALSE ALARMS

- DEMONSTRATES HOW AI ENHANCES TRADITIONAL SECURITY BY CATCHING SUBTLE INSIDER THREATS

HUMAN + AI = BETTER OUTCOMES

- AI PROVIDES BROAD VISIBILITY ACROSS SYSTEMS

- ANALYSTS CAN FOCUS ON STRATEGY INSTEAD OF CHASING ALERTS

- THE COMBINATION OF AI AND HUMAN JUDGMENT LEADS TO BETTER OUTCOMES

KEY TAKEAWAYS

- PROACTIVE > REACTIVE

- TOOLS ADAPT OVER TIME

- AI DOESN'T REPLACE...IT AUGMENTS SAFETY TEAMS

PART 3:

BALANCING AI WITH EMPLOYEE INTERESTS

- THE PATHWAY TO BALANCING BEGINS WITH A CLEAR UNDERSTANDING OF YOUR AI USAGE POLICY

- DEVELOPMENT OF AN AI POLICY IS ESSENTIAL FOR ANY BUSINESS OPERATION

- EMPLOYEE AND COMPANY INTERESTS ARE BEST REPRESENTED WHEN AI POLICY IS WRITTEN IN PLAIN LANGUAGE AND CLEARLY COMMUNICATED TO STAFF

HOW TO DEVELOP AN AI POLICY FOR YOUR COMPANY

- CONSULT WITH COUNSEL, OTHER PROFESSIONALS

- INCLUDE STAFF IN DEFINING ROLES, OUTCOMES

- REVIEW INDUSTRY TEMPLATES, BE SURE TO IDENTIFY COMPANY NEEDS, AND HOW AI IS BEST DEPLOYED IN YOUR BUSINESS MODEL

WHAT SHOULD BE A PART OF YOUR POLICY?

1. CLEARLY DEFINED SCOPE

2. ACCEPTABLE USE GUIDELINES

3. DATA HANDLING/PRIVACY

4. ETHICAL GUIDELINES

WHAT SHOULD BE A PART OF YOUR POLICY?

5. TRAINING AND EDUCATION

6. MONITORING, AUDIT AND EVALUATION

7. DISCIPLINARY ACTION

8. POLICY REVIEW AND UPDATING

PRIORITIZING TRAINING

- ESSENTIAL TO PROVIDE EMPLOYEES WHAT THEY NEED IN ORDER TO WORK ALONGSIDE AI, PREPARE THEM FOR A FUTURE WORKPLACE WHERE AI TOOLS WILL BE AN IMPORTANT PART OF JOB FUNCTIONS

DETERMINING AN EFFECTIVE TRAINING PROGRAM

- IT IS OFTEN BETTER TO DEVELOP/DESIGN YOUR OWN TOOLS FOR TRAINING RATHER THAN RELYING ON A VENDOR/SERVICE

- EASIER TO ADAPT TO SPECIFIC JOB FUNCTIONS/DUTIES

- ABILITY TO PERSONALIZE TRAINING, SHOW HOW IT WILL IMPACT SPECIFIC ROLES

ENSURE HUMAN OVERSIGHT AND ACCOUNTABILITY

- NEED FOR ETHICAL DECISION-MAKING

- DEFINING ACCOUNTABILITY AND RESPONSIBILITY

- MAKING PROGRAMS MORE FLEXIBLE/ADAPTABLE TO WORKPLACE

- MEANS OF MITIGATING BIAS AND ERRORS

- ENSURING REGULATORY COMPLIANCE

REGULAR REVIEW OF UTILIZED AI PROGRAMS AND SYSTEMS

- GOALS/OBJECTIVES OF ANY TOOL UTILIZED, HOW ARE YOU MEASURING SUCCESS

- KPI'S

- WHAT IS THE IMPACT ON THE WORKPLACE?

- AS AI IS CONSISTENTLY AND RAPIDLY EVOLVING, HOW IS YOUR ORGANIZATION MONITORING REGULATORY CHANGE?

BEST MEANS OF BALANCING UTILIZATION OF AI WITH EMPLOYEE INTERESTS

- ALWAYS REMEMBER: AI TOOLS SHOULD BE USED TO ENHANCE AN EMPLOYEE'S ABILITY TO DO THEIR JOB SAFELY, NOT TO COMPETE WITH IT

- SOLICITING FEEDBACK/ ONGOING DIALOGUE ABOUT AI TOOLS, EMPLOYEE CONCERNS

PART 4:

UTILIZE AI WITH HISTORICAL DATA TO PREDICT POTENTIAL HAZARDS

EVERY INCIDENT LEAVES CLUES

- "MOST SAFETY INCIDENTS FOLLOW PATTERNS"
- AI CAN TURN PAST DATA INTO INSIGHTS THAT PREVENT OR NARROW FUTURE RISKS

2025 WEBINAR SERIES

TYPES OF HISTORICAL DATA USED

- INCIDENT REPORTS, FAILED LOGINS, PHISHING ATTEMPTS

- USAGE PATTERNS BY DEPARTMENT, ROLE, LOCATION, AND TIME

WHAT AI CAN PREDICT

- IDENTIFIES LIKELY INSIDER THREATS BASED ON PRIOR BEHAVIOR

- DETECTS PEAK RISK PERIODS LIKE HOLIDAYS OR LARGE EVENTS

- HIGHLIGHTS DEPARTMENTS OR ROLES WITH INCREASED EXPOSURE

CASE STUDY – PREDICTIVE PHISHING PREVENTION

- BEHAVIOR MODELING LEADS TO FEWER INCIDENTS

- AI REVIEWED TWO YEARS OF ANONYMIZED USER ACTIVITY AND PHISHING SIMULATION DATA

- DETECTED PATTERNS THAT PUT CERTAIN GROUPS (NEW HIRES, HIGH-STRESS TEAMS) AT HIGHER RISK

CASE STUDY – PREDICTIVE PHISHING PREVENTION

- BASED ON AI INSIGHTS, TARGETED PHISHING TRAINING WAS DELIVERED TO HIGH-RISK EMPLOYEES

- PHISHING CLICK-THROUGH RATES DROPPED BY 40% WITHIN JUST ONE QUARTER

- SHOWS HOW PREDICTIVE AI ALLOWS ORGANIZATIONS TO FOCUS RESOURCES EFFICIENTLY AND REDUCE RISK PROACTIVELY

LOOKING FORWARD, NOT BACK

- AI ENABLES PRE-EMPTIVE ACTION LIKE TRAINING OR ACCESS CHANGES

- YOU MOVE FROM REACTIVE FIXES TO PREVENTION BASED ON DATA TRENDS

ETHICS OF PREDICTIVE AI

- BE TRANSPARENT ABOUT HOW DATA IS COLLECTED AND USED

- USE PREDICTIONS TO GUIDE SUPPORT—NOT PUNISHMENT

- ETHICAL USE OF AI INCLUDES FAIRNESS, PRIVACY, AND COMMUNICATION

KEY TAKEAWAYS

- HISTORICAL DATA BECOMES ACTIONABLE INSIGHT THROUGH AI

- FORECASTING ALLOWS EARLY INTERVENTION BEFORE ISSUES ESCALATE

- HUMAN JUDGMENT MUST GUIDE THE USE OF AI IN SAFETY PROGRAMS

RECAP OF KEY TOPICS

1. HOW AI ADVANCEMENTS CAN IMPROVE WORKPLACE SAFETY

2. TOOLS AND TECHNOLOGIES FOR SAFER PERFORMANCE

3. BALANCING AI WITH EMPLOYEE INTEREST

4. UTILIZING AI WITH HISTORICAL DATA TO PREDICT POTENTIAL HAZARDS

THE AI + HUMAN PARTNERSHIP

- SMART SAFETY = AI POWER + HUMAN ETHICS
- EACH STRENGTHENS THE OTHER

WHAT TO DO NEXT?

- REVIEW CURRENT SAFETY SYSTEMS

- IDENTIFY WHERE AI COULD HELP

- START SMALL, MONITOR IMPACT

- AI POLICY TEMPLATE

REFERENCE PAGE

- Microsoft Purview Insider Risk Management
  https://www.microsoft.com/security/blog

- KnowBe4 Case Studies on Phishing Prevention
  https://www.knowbe4.com/resources/case-studies

- Cofense Phishing Defense Case Studies
  https://cofense.com/resources/case-studies/

2025 WEBINAR SERIES

QUESTIONS

THE END

- Thank you for your participation
- For a free AI Policy Template, contact:
  - angelolosardo@ace-it.com
  - 888-816-2436, Ext. 150