Do You See What I See?

Navigating Human & Cyber Threats at the Workplace

The views expressed by us are not representative of the City of Charlotte.
OUTLINE

• INTRODUCTIONS
• HUMAN THREATS
• CYBER THREATS
• QUESTIONS
INTRODUCTIONS

• Courtney Rogers, Esq.
  • Graduate of the Charlotte School of Law
  • Provides legal guidance and support to Human Resources professionals

• Thomas E. Powers III, Esq.
  • Graduate of the University of North Carolina – Chapel Hill School of Law
  • Handles litigation and represents the organization before courts of law
Human Threats
Workplace Violence

• Any act or threat of physical violence, harassment, intimidation, or other threatening disruptive behavior that occurs at the work site.

• It ranges from threats and verbal abuse to physical assaults and even homicide.
Protection of employees against workplace violence is the responsibility of employers.
Human Threats
Workplace Violence - Awareness

• CAUSES:
  • Termination
  • Other discipline
  • Poor performance review
  • Conflict with coworker
  • Perceived unfairness
  • Domestic violence
  • Substance abuse
  • Untreated mental illness
  • Stressful life event
Human Threats

Workplace Violence - Policy Creation & Implementation

Zero-tolerance workplace violence policy
Human Threats
Workplace Violence - Policy Creation & Implementation

• Educate
  • New hire orientation / annual training
    • Carefully review policy
    • Risk factors to look for
  • Critical that all employees know the policy and understand that all claims of workplace violence will be investigated and remedied promptly.
Human Threats
Workplace Violence - Reporting/Training

• It is critical that all employees are trained to recognize concerning behaviors.

• Help employees feel safe when reporting issues.
  • Employees need to understand their obligation to report.
  • Allow anonymous reporting, if possible.
    • Hotline/tip line
Human Threats
Identifying At-Risk Employees

• Violent incidents can be avoided in many cases.
  • They are often preceded by warning signs.

• Generally, violence develops over time.
Human Threats
Identifying At-Risk Employees

• Early Potential for Violence:
  • Dehumanizing other people
  • Challenging authority / insubordination
  • Regularly being argumentative
  • Alienating clients or coworkers
  • Unusual or strange behavior
Human Threats
Identifying At-Risk Employees

• Escalated Potential for Violence:
  • Ignoring policies / procedures
  • Stealing from company or coworkers
  • Making threats
  • Blaming others for all problems
  • Destruction of property

• Potential for Violence is Realized:
  • Displaying or brandishing a gun, knife, or other weapon
  • Physical violence
  • Threatening suicide
  • Stalking
Human Threats
In the News

McDonalds employees allege restaurant redesign has caused more workplace violence to occur:

Employee fatally shoots Molson Coors coworkers:

Nurses filed OSHA complaint that hospital is not protecting staff or patients from abusive individuals seeking treatment: https://abc7chicago.com/5967518/
HR professionals have many responsibilities, but none quite as important as their duty to protect employees and their company.

In today’s digital world, you must become cyberwarriors!
Cyber Threats
Confidential Information Theft – Major Costs

- Reputation damage
- Financial hit/fines
- Litigation costs
- Ransomware
- Employee disengagement/distraction
Cyber Threats
Confidential Information Theft – Awareness (Red flags)

- System failure or disruption
- Suspicious questioning
- Unauthorized access
- Unauthorized changes or additions
- Suspicious emails
- Misuse of computing resources
- Reports of hostile workplace
- Tests of security
Cyber Threats
Confidential Information Theft – Policy Creation & Implementation

• Limit which employees have access to sensitive data.
• Control password creation and train employees on password strength.
• Train employees to be careful of phishing.
• Create and enforce policies limiting internet access and prohibiting unauthorized software.
• Police and train employees in the use of mobile devices.
• Create a culture of security awareness and a sense of shared responsibility.
Cyber Threats
Confidential Information Theft – Employee Records

When I was young, my mom said I can be anyone I want to be

False! That’s identity theft
Cyber Threats
Confidential Information Theft – Employee Records

- Too much information collected at the wrong time.
- Once collected, track what you have.
- Decide what information will be available only to the HR department.
- Encrypt as much as possible.
Cyber Threats
In the News

Around 30 servers at Mecklenburg County were held hostage by hackers using ransomware:

An unauthorized third-party had access to personal information, including email accounts, names, social security numbers, and credit card information of some guests and employees of Carnival Corporation:
Cyber Threats
Significant Caselaw / How to Avoid this Landmine

In re Horizon Healthcare Services Inc. Data Breach Litigation
846 F.3d 625 (3rd Cir. 2017)

- FACTS: Horizon Healthcare Services, Inc., d/b/a Horizon Blue Cross Blue Shield of New Jersey provides health insurance products and services and collects and maintains personally identifiable information (e.g., names, dates of birth, social security numbers, and addresses) and protected health information (e.g., demographic information, medical histories, test and lab results, insurance information, and other care-related data). Two unencrypted laptops stolen from company.

- COURT SAID: Improper disclosure of one’s personal data in violation of the Fair Credit Reporting Act provides a basis to sue the violator.

- WHY IT MATTERS: Any unauthorized disclosure of personal information constitutes a violation of the Fair Credit Reporting Act, regardless of whether it is major or minor.
Cyber Threats
Significant Caselaw / How to Avoid this Landmine

Remijas v. Neiman Marcus Group, LLC
794 F.3d 688 (7th Cir. 2015)

• **FACTS:** Hackers attacked Neiman Marcus between July and October 2013 exposing 350k cards. Class-action lawsuit was filed alleging negligence, breach of implied contract, unjust enrichment, unfair and deceptive business practices, invasion of privacy, and violation of multiple state data breach laws.

• **COURT SAID:** A person, who must undertake resolving fraudulent charges and protecting oneself from future identity theft, has a basis to sue the violator.

• **WHY IT MATTERS:** Where a person has spent time and money to resolve a fraudulent charge after a data breach, it is more likely that the court will allow the case to proceed.
Cyber Threats
Significant Caselaw / How to Avoid this Landmine

*Krottner v. Starbucks Corp*
628 F.3d 1139 (9th Cir. 2010)

• **FACTS**: A unencrypted laptop was stolen in 2008 with the names, address, and social security numbers of 97k current and former employees. Class-action lawsuit was filed alleging negligence and breach of implied contract under state law.

• **COURT SAID**: A person, who must undertake resolving fraudulent charges and protecting oneself from future identity theft, has a basis to sue the violator.

• **WHY IT MATTERS**: Employees enrolled in the company’s free credit watch services but the court still allowed the lawsuit to proceed because of the substantial time and effort spent to resolve fraudulent charges and protect oneself from future identity theft.
Cyber Threats
Significant Caselaw / How to Avoid this Landmine

Beck v. McDonald
848 F.3d 262 (4th Cir. 2017)

• FACTS: Laptop containing 7400 patients’ personal information and boxes containing 2000 patients’ personal information went missing. Two class-action lawsuits were filed alleging violation of Privacy Act and federal Administrative Procedure Act.

• COURT SAID: None of the plaintiffs had a basis to sue because the injury was speculative in nature.

• WHY IT MATTERS: Court acknowledged Remijas and Krottner but stated that plaintiffs did not offer evidence of new financial accounts being opened or fraudulent charges occurring after personal information went missing.
QUESTIONS/COMMENTS?

#TheEnd