INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

# WORKPLACE HARASSMENT AND VIOLENCE:

## A PRIMER ON CRITICAL STRATEGIES

## FOR SMALL AND MEDIUM-SIZED BUSINESSES


**Institute for Homeland Security**

**Sam Houston State University**

Narasimha Shashidhar

Cihan Varol

Jayanthi Ramamoorthy

# Workplace Harassment and Violence:

## A Primer on Critical Strategies for Small and Medium-Sized Businesses

PI, and Co-PI: Narasimha Shashidhar, and Cihan Varol

Doctoral Student Investigator: Jayanthi Ramamoorthy

Department of Computer Science
Sam Houston State University
Huntsville, TX
jxr153@shsu.edu, nks001@shsu.edu, cxv007@shsu.edu

# Contents

## Purpose

Workplace violence and harassment affects millions of employees every year. According to the US Department of Justice, an average of 1.3 million nonfatal violent crimes occurs in the workplace every year [1].

This document provides a cybersecurity forensic framework and strategy for small and medium-sized businesses (SMBs) to Identify, Prevent and Respond to workplace violence and harassment incidents. The recommended framework includes tools and techniques to identify patterns of such incidents, analyze the underlying factors, and provide businesses with strategies to address them effectively.

## Introduction

To ensure safe and healthy working conditions for workers the congress enacted the Occupational Safety and Health act of 1970 which led to the creation of Occupational Safety and Health Administration (OSHA) as part of the United States Department of Labor. According to OSHA, any act or threat of physical violence, harassment, intimidation, or other threatening or disruptive behavior that occurs at the work site is considered workplace violence [2]. Workplace violence can range from verbal abuse and threats to physical assault and homicide. The International Labor Organization (ILO) defines workplace violence and harassment as follows:

*"The term 'violence and harassment' in the world of work refers to a range of unacceptable behaviors and practices, or threats thereof, whether a single occurrence or repeated, that aim at, result in, or are likely to result in physical, psychological, sexual, or economic harm, and includes gender-based violence and harassment."*

In effect, workplace harassment and violence can be verbal, physical, or psychological regardless of the intent or source.

## Definition of Workplace harassment and Violence

The U.S. Bureau of Labor Statistics defines workplace violence and harassment [3] as -

"*An action (verbal, written, or physical aggression) which is intended to control or cause, or is capable of causing, death or serious bodily injury to oneself or others, or damage to property. Workplace violence includes abusive behavior toward authority, intimidating or harassing behavior, and threats.*"

"*Intimidating or Harassing Behavior - Threats or other conduct which in any way create a hostile environment, impair operations; or frighten, alarm, or inhibit others. Psychological intimidation or harassment includes making statements which are false, malicious, disparaging, derogatory, rude, disrespectful, abusive, obnoxious, insubordinate, or which have the intent to hurt others' reputations. Physical intimidation or harassment may include holding, impeding, or blocking movement, following, stalking, touching, or any other inappropriate physical contact or advances.*"

Moreover, workplace violence can occur anytime and anywhere including social settings and other circumstances related to work, regardless of the employee status, such as tenured employees, contractors, jobseekers, volunteers, interns, and customers. See Appendix A, 2019 statistics on workplace harassment and violence in U.S.

*Definition of terms*

Source: National Crime Victimization Survey and Census of Fatal Occupational Injuries

| |
|---|
| *Workplace*—Place where an employed person is working or on duty. |
| *Workplace violence*—Nonfatal violence (sexual assault, robbery, and aggravated and simple assault) against employed persons aged 16 or older that occurred while they were at work or on duty. |
| *Nonworkplace violence*—Nonfatal violence (sexual assault, robbery, and aggravated and simple assault) against employed persons aged 16 or older that occurred while they were not at work or on duty. |
| *Violence against persons not employed*—Nonfatal violence (sexual assault, robbery, and aggravated and simple assault) against persons aged 16 or older who did not have a job at the time of the crime. |
| *Workplace homicide*—Homicide of employed victims aged 16 or older who were killed while at work or on duty. Excludes death by accident. |

## Compliance and Legal support for harassment and violence at work

According to a survey conducted by the Society for Human Resource Management (shrm.org), 28% of U.S workers have either witnessed or been subjected to aggressive workplace interactions [4]. In this section, we will discuss federal and state laws that govern violence and harassment in the workplace.

### Federal and Texas State Laws on safety of workplace

The Occupational Safety and Health Act of 1970 (OSHA) is the primary law regulating workplace safety and health in the U.S. It mandates private-sector employers to provide a hazard-free workplace for their employees and adhere to OSHA's occupational safety and health standards (29 U.S.C. § 654).

Although OSHA does not apply to the Texas state government or any of its agencies (29 U.S.C. § 652(5)), it does not preempt State laws in Texas that offer more protection or benefits to employees. Many occupations are regulated under the Occupations Code safety laws to ensure workplace safety and health laws that protect employees.

Per Common-Law principles, an employer is liable for workplace violence including but not limited to the following:

- *Doctrine of Respondent Superior*
  The employer is implicitly responsible for their employees' actions. This is a fact-based liability on whether the employer's actions or lack thereof contributed to the violent act.

- *Premise liability*
  The worksite security and safety measures that the employer is expected to provide to ensure the safety of its employees.

- *Negligence*
  Employee background checks that the employer is responsible for, along with the appropriate response measures that should be in place to prevent and respond to workplace violence.

- *Harassment and Discrimination*

The employer is liable for workplace discriminatory practices and harassment protected by Federal and Texas State laws.

The government agency Equal Employment Opportunity Commission (EEOC) holds the employer accountable for the following Federal Discrimination laws:

- Discrimination based on race, color, national origin, sex, pregnancy, sexual orientation, gender identity, and religion is covered by Title VII of the Civil Rights Act of 1964.
- Discrimination against employees for disabilities is protected by the Americans with Disabilities Act (ADA) and requires employers to provide reasonable accommodations to employees with disabilities.
- Discrimination based on genetic information of the employee is protected by Genetic Information Non-discrimination Act (GINA).

*Small businesses are exempt from the following discrimination laws:*

- *Discrimination based on citizenship or immigration status is protected by the Immigration and Nationality Act (INA) - (Not enforced for small businesses).*
- *Discrimination based on age is protected by the Age Discrimination in Employment Act (ADEA) for workers who are at least 40 years or older. (Not enforced for small businesses).*

The Texas Workforce Commission (TWC) is a state government agency that enforces employment discrimination laws as per Chapter 21 of the Texas Labor Code that deals with discrimination based on race, color, disability, religion, sex, national origin, or age.

## Framework for workplace violence and harassment

Small businesses should establish a comprehensive framework to effectively address and mitigate incidents of violence and harassment in the workplace. This is essential for several reasons:

### Motivation

*Emergency Readiness:* Prepare ahead to handle workplace violence incidents that can occur suddenly.

*Repeatable Incident Response:* Having an incident response plan enables teams to respond consistently and effectively, optimizing their time.

*Effective Coordination:* Maintaining communication among all internal and external stakeholders during a crisis can be challenging. A well-defined process facilitates better coordination.

*Identifying Security Gaps:* Implementing an incident response plan in small businesses with limited resources or technical expertise helps uncover and address vulnerabilities before a crisis arises.

*Preservation of Knowledge:* An incident response plan ensures that valuable knowledge and best practices for crisis management are not lost over time. By incorporating lessons learnt from a pos-incident analysis, the organization can continue to evolve the process and address the business' unique needs.

*Clearly Defined Roles and Responsibilities:* An incident response plan establishes a well-defined, consistent process for handling incidents, thereby enhancing coordination and response effectiveness over time.

*Documentation and Accountability:* An incident response plan promotes documentation of actions taken and assigns responsibility, fostering accountability throughout the incident response process.

### *General guidance*

For general guidance on workplace violence prevention and response, Cybersecurity & Infrastructure Security Agency (CISA) offers a detailed guide [5] intended for various sectors including SMBs. The guidance addresses factors to consider when establishing a program to detect and respond to workplace violence and harassment. In cases that involve mental health, small businesses are advised to consult with a qualified mental health professional, as well as seek legal counsel, to ensure compliance with relevant laws, responsibilities, and safeguards for both the individual engaged in workplace violence and the organization.

The Texas Department of Insurance, a division of Texas Workers' Compensation publication on workplace violence [6] identifies the risk factors, prevention strategies, and guidance on effective controls.

## Employer commitment and Statement

Workplace violence and harassment is classified as Insider threat according to Cybersecurity & Infrastructure Security Agency (CISA) [7]. The definition and scope for workplace violence and harassment is outlined as follows:

"Workplace/organizational violence consists of any act or threat of physical violence, harassment, sexual harassment, intimidation, bullying, offensive jokes, or other threatening behavior by a coworker or associate that occurs in a person's place of employment or while a person is working."

### Developing an Organizational policy on workplace violence and harassment

We adapt guidance from CISA on insider threat in developing an organizational policy on workplace harassment and violence.

Policies and Procedures

| |
|---|
| Develop a policy for violence and harassment prevention which addresses the following at a minimum:<br>– Definition and organizational responsibility<br>– Security and safety measures that are in place to deter or prevent workplace violence and misconduct.<br>– Legal support<br>– Responsible personnel and escalation process<br>– Training employees |
| Develop threat management programs with the appropriate tools for detecting, responding, and reporting of these security incidents. |
| CISA advises against zero-tolerance policies since it may result in employees hesitant to report incidents due to concerns that it would cost the coworker to lose their job. Therefore, the policy |

| |
|---|
| should clearly state the due process and investigation that will be followed upon receiving a report of misconduct. |
| The organizational policy should address the legal boundaries and not infringe on privacy and civil liberties of people involved in the incident. Following are some of the legal foundations and constraints to consider:<br>– Employment, regulatory laws and Occupational Safety and Health Act (as discussed in the section above)<br>– Privacy/confidentiality laws and regulations<br>– Ethics<br>– Liability and management<br>– Pre-hire background checks<br>– Lawful termination<br>– Disability laws and regulations<br>– Freedom of Information Act and open records (FOIA)<br>– Stalking and criminal threats<br>– Due process protections and investigative procedures<br>– Criminal and civil protective orders<br>– Emergency protective or restraining orders<br>– Civil commitment<br>– Wrongful termination and retaliation<br>– Privilege and confidentiality of all the people involved in reporting and investigating the incident.<br>– Informed consent<br>– Duty to warn and duty to protect.<br>– Liability, negligence, foreseeability, emotional distress<br>– Health Insurance Portability and Accountability Act (Medical conditions including mental illness) |

## Framework components

### Plan and Prepare

During the planning and preparation phase, it is important to consider the necessary infrastructure to prevent, detect, or respond to incidents of harassment and violence in the workplace.

*Communication & Process*

| |
|---|
| Identify stakeholders such as Human Resources, Legal, security and external law enforcement entities. |
| Identify on-call information within the company directory for reporting and escalation of workplace violence and harassment incidents.<br>Establish reporting mechanisms by publicizing phone numbers, email addresses, online portal, and secure instant messaging systems, where at least one mechanism to report incidents anonymously.<br>Develop a process for collecting information and escalation, along with verification mechanisms for the contact's identity. |
| Use an Issue tracking system for tracking reported incidents with details on the incident and status. |

| |
|---|
| For online communication of the incident to external authorities and internal communication, use encryption strategies to preserve the privacy of individual related to the incident. For example, encrypt email, and password-protect shared documents. |
| Identify a secure storage facility for storing and preserving evidence and other sensitive materials that are related to the incident. |

*Hardware and Software support*

| |
|---|
| Identify digital collaboration and communication tools.<br>For example, email, chat (e.g., slack), meeting (e.g., Microsoft Teams, Zoom), internal company portals. |
| Identify logs to be collected, their location, retention, and query mechanisms.<br>For example, Web activity logs, emails, network logs etc.<br>For SMBs involving regulated industries such as healthcare, internet service providers and businesses with credit card related transactions, there may be additional considerations to protect the privacy and integrity of data collected. |
| Setup alerting using automated tools.<br>For e.g., Microsoft Power Automate to alert on specific keywords or sentiment analysis, and employee monitoring tools). *See appendix for more details and references on tools*. |
| Documentation of location of the logs, query mechanisms and appropriate access controls. |

*Setup for Incident Analysis*

| |
|---|
| Digital forensic workstation or backup devices to save relevant data from the incident for all digital artifacts pertaining to the incident. |
| Digital evidence data acquisition from cloud, mobile, social networks, and other digital and non-digital sources. Tools such as *Autopsy* [8] to create a forensic image of the device which can be analyzed by digital forensic experts to retrieve artifacts including deleted files, emails, and images. |
| Tools for capturing and analyzing network capture data such as *Wireshark* [9], and any reporting software if applicable. |
| Printer, removable media, Digital Forensic software, networking equipment and other evidence gathering and preserving tools. |
| Documentation for Operating Systems, applications, protocols, and intrusion detection and antivirus products, Network diagrams and lists of critical assets. |
| Create a step-by-step runbook and checklist that the Incident responder should follow when an incident is detected or reported. |

## Detection and Incident Analysis

Incidents related Workplace harassment and violence may not always have a digital footprint. Moreover, it is not practical to define a process for every specific incident. Therefore, depending on the industry related to the business, specific trigger or attack vectors should be considered. For example, informing a customer of a declined claim, employee attrition, employees working nightshifts, security personnel with weapons etc.

*Assess, manage, and mitigate risk*

| |
|---|
| Identify Trigger scenarios, and corresponding mitigation in terms of processes and procedures. For example, including an insurance specialist that the customer can work with for a declined claim, or assistance in job searches for another role within a company for an employee affected due to attrition. |
| Employ employee monitoring tools and solutions that align with compliance regulations. |
| Automate alerts from monitoring solutions and integrate with an Incident response workflow or tool. |
| Establish periodic assessment of logs to improve the accuracy of automated alerts. |

*Tools and techniques*

Employee monitoring tools and solutions can provide valuable insights and capabilities that can help businesses prevent workplace violence and harassment, create a safer work environment, and foster a culture of mutual respect and professionalism. Many of these tools allow businesses to set customizable policies that reflect their specific needs and priorities.

Guidelines

| |
|---|
| Check for jurisdiction, compliance regulations, and best practices of using Employee monitoring solutions. |
| Define the scope of employee monitoring systems, identify workstations and devices that need to be imaged for the digital forensic investigations. |
| Identify software solutions used by employees for communication and collaboration. Ex: email, collaboration tools such as chats and conferencing software.<br>Identify software that will aid in Incident evidence collection. For example, Disk imaging software such as *Autopsy Sleuthkit* [8], tools such as *Wireshark* [9]to capture network communication etc.<br>Refer *Appendix C.* |
| Create a monitoring policy including Administration of the policies and procedures. |
| Integration of monitoring and analytic solutions with custom in-house tools that are developed for workplace collaboration and communication. |

Examples of tools that aide in prevention of workplace harassment and violence are as follows:

IBM Watson [10] provides API support and uses natural language processing (NLP) and machine learning algorithms to analyze the tone of written text, including emails, chat conversations, and social media posts, to identify any language that may be aggressive, confrontational, or threatening.

Microsoft Power Platform [11] is a business productivity tool that provides workflow automation. The platform provides a prebuilt Sentiment Analysis AI (Artificial Intelligence) model which can be integrated with email, chat and other text documents that are used by employees, customers, and vendors.

Instructions: https://learn.microsoft.com/en-us/ai-builder/prebuilt-sentiment-analysis

## Incident Response

Once a workplace harassment or violence is detected or reported, the responder will decide on the criticality of the incident.

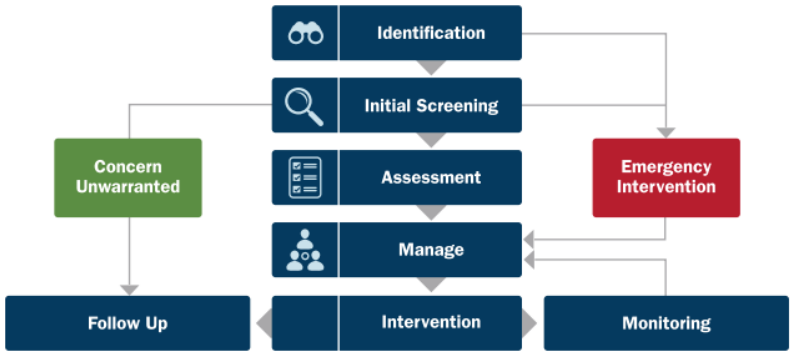



*Figure 1. Threat assessment process as defined by CISA [7]*

**Assessment**

The Incident responder will then assess the case. The template for threat assessment from the Plan & Prepare phase will be used to assess the incident. A Sample of threat assessment questions can be found in *Appendix D.*

**Threat management & Preservation of Evidence**

As outlined in the Incident Analysis Setup of the *Plan & Prepare* section of this guide, any digital evidence collected from logs and other tools should include digital hashes and chain of custody for storage equipment and related devices to ensure that the integrity of the evidence is maintained. These measures play a crucial role in preserving the integrity of the evidence, making it admissible in court and facilitating the involvement of law enforcement and external entities in digital forensics investigation.

| |
|---|
| Once the incident is assessed, the incident responder will follow the runbook from the plan & Prepare phase by involving the stakeholders identified for threat management team and escalation. |
| Maintain the integrity of the evidence collected by ensuring the preservation of digital hashes. By default, digital imaging software such as the open-source tool Autopsy [8] maintains the digital hashes, safeguarding the integrity of the collected evidence. |
| Maintain chain of custody for the evidence collected. |

## Post-Incident Activities

A threat incident report should be created for every incident that documents as much information as possible from the following:

| |
|---|
| Documenting the details of the incident, including the date, time, location, individuals involved, witnesses, along with any evidence or supporting documentation. (e.g., HR report, background check, health records, previous assessments) |
| Reporting the incident to appropriate authorities, such as law enforcement or regulatory agencies, as required by law. Internal communication should also take place to inform relevant stakeholders, such as management, HR, and legal teams. |
| Reported warning signs; indicators/ stressors/triggers from tools or individuals |
| Any other open-source search results (e.g., social media, blogs, internet search) |
| Reports from concerned parties |
| Interview reports |

| |
|---|
| Threat management team findings, including risk level. |
| Details on Digital Forensic workstation or backup devices, removable media, printers, data acquisition methodology and tools used for digital evidence collection and preservation |

### Follow-up actions

Threat management is an iterative process. After a workplace violence and harassment incident, organizations can engage in several follow-up activities as part of their post-incident response. Analyzing the incident enables various teams to reflect on the efficiency of the process and identify any gaps in tooling and processes.

| |
|---|
| Implementing corrective and preventive measures to address any gaps or weaknesses in existing policies, procedures, tooling, and training related to workplace violence and harassment prevention. |
| Review Employee Assistance Programs (EAP) to provide support and resources to the victim, including access to counseling services, medical assistance, and ensuring their safety and well-being. |
| Review training and awareness programs to educate employees about workplace violence and harassment, prevention strategies, reporting mechanisms, and available resources. |
| Consultation with legal to ensure compliance with applicable laws and regulations, and to assess any potential legal implications or liabilities arising from the incident. |
| Monitoring the workplace environment for any signs of recurring or escalating incidents. |
| Recommendations for management strategies and improvements. |

## Conclusion

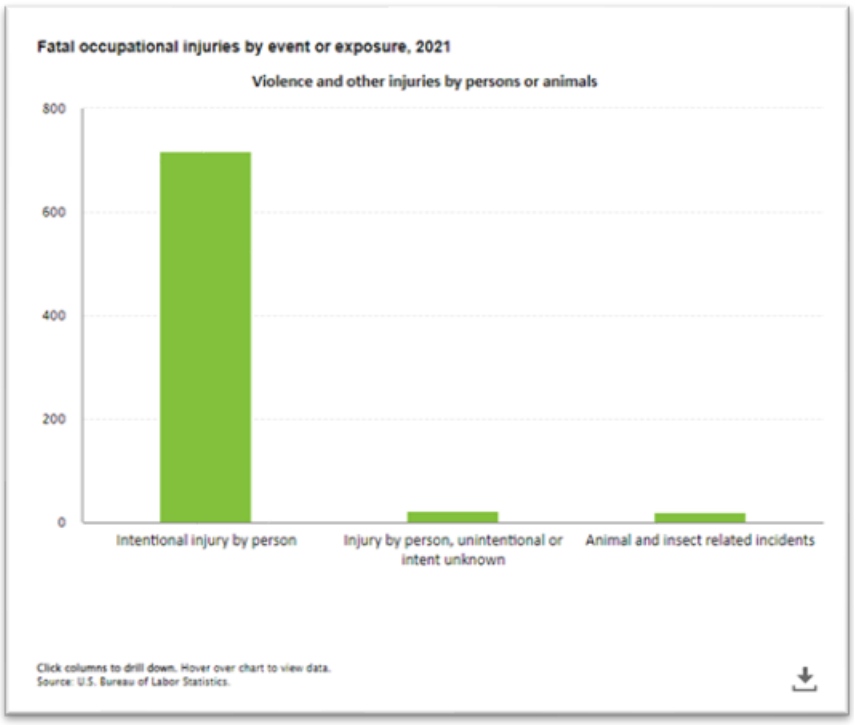
Workplace violence and harassment pose significant risks to employees and businesses, with millions of incidents occurring each year. In this guide, we provide guidelines and references for implementing an organizational policy to prevent harassment and violence in the workplace. Additionally, we offer strategies, tools, and techniques that small and medium-sized businesses (SMBs) can follow from a cybersecurity and forensics perspective.

The extent to which these recommendations should be followed and implemented depends on the type of business and the individual organization's level of maturity, as well as their commitment to continual improvement.

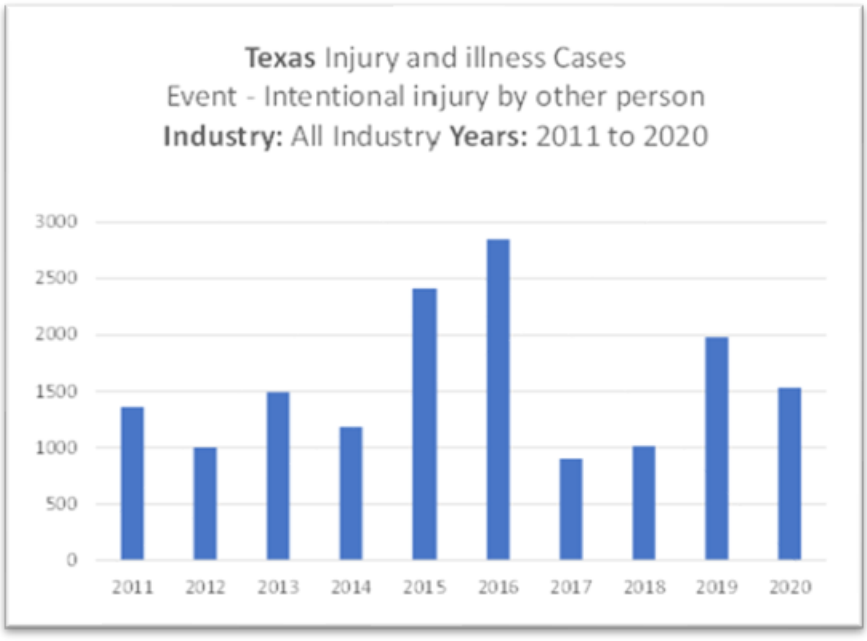
## Appendix A

### Workplace harassment and violence Statistics

The U.S. Bureau of Labor Statistics show 718 reported fatalities due to violence in workplace caused by intentional injury by person in the year 2021.




### State of Texas statistics on workplace violence



## Examples of workplace violence and harassment

# Appendix B

## Sample Workplace Violence Prevention Policy Statement

Recommended sample of Workplace Violence Prevention Policy Statement from Texas Department of Insurance, Division of Workers' Compensation -

*[Employer Name] is concerned and committed to the safety and health of our employees.*

*We refuse to tolerate violence in the workplace. We will make every effort to prevent violent incidents by implementing a Workplace Violence Prevention Program. We will provide adequate authority and budgetary resources to responsible parties to meet our goals and responsibilities.*

*All managers and supervisors are responsible for implementing and maintaining our Workplace Violence Prevention Policy. We encourage employee participation in designing and implementing our program. We require prompt and accurate reporting of all violent incidents, whether physical injury occurred. We will not discriminate against victims of workplace violence.*

*A copy of this Policy Statement and our Workplace Violence Prevention Program is readily available to all employees from each manager and supervisor.*

*Our program ensures that all employees, including supervisors and managers, adhere to work practices designed to make the workplace more secure. They will not engage in verbal threats or physical actions that create a security hazard for others in the workplace.*

*All employees, including managers and supervisors, are responsible for using safe work practices, following all directives, policies, and procedures; and maintaining a safe and secure work environment.*

*The management of [Employer Name] is responsible for ensuring that all safety and health policies and procedures involving workplace security are communicated and understood by all employees.*

*Managers and supervisors are expected to enforce the rules fairly and uniformly. Our program will be reviewed and updated annually.*

# Appendix C

## Tools and Resources

IBM Watson Tone Analyzer: Text analysis from various sources, including IRC messages, and identify emotions, social tendencies, and language tones in the text.

Microsoft Azure Text Analytics: Sentiment analysis of several types of text, including IRC messages, and can identify key phrases and entities.

RapidAPI Sentiment Analysis API: Has an API to provide sentiment analysis along with other NLP features.

Autopsy [8]: Sleuthkit Autopsy is a free open-source digital forensics platform that can be used to obtain a digital image of the victim and/or offender's workstation for further analysis. https://www.sleuthkit.org/autopsy/

Wireshark [9]: Wireshark is a free and open-source packet analyzer that can be used to analyze network communication and obtain evidence logs. https://www.wireshark.org/

## Appendix D

### Sample Threat assessment questions from CISA [7]

| |
|---|
| What is the exact nature and context of the threat and/or behavior? |
| Who or what is the intended target? |
| Was the threat and/or behavior intentional or unintentional? |
| What was the possible motivation for the threat and/or behavior? |
| Has an organizational policy or regulation been violated? |
| Does the person of concern have the intent, motivation, and ability to carry out the threat? |
| Has the law been broken? |
| What is the person of concern's history? |
| What are the behavioral and technological indicators? |
| Does the person of concern have any stressors/personal predispositions? |
| Why, at this time, has the person of concern made comments or actions that have been perceived by others as threatening? |
| What is happening in the personal life of the person of concern that might be relevant? |
| What has been said to others (e.g., friends, colleagues, coworkers, etc.) regarding the matter that is troubling them? |
| How does the person of concern view themselves in relation to everyone else? |
| Does the person of concern feel they have been wronged in some way? |
| Does the person of concern accept responsibility for their own actions? |
| How does the person of concern cope with disappointment, loss, or failure? |
| Does the person of concern blame others for their failures? |
| How does the person of concern interact with coworkers or associates? |
| Does the person of concern feel they are being treated fairly by the company or organization? |
| Does the person of concern have problems with supervisors, management, or leadership? |
| Does the person of concern care about job practices and responsibilities? |
| Has the person of concern received unfavorable performance reviews or been reprimanded? |
| Is the person of concern experiencing personal problems, such as divorce, death in the family, health problems, or other personal losses or issues? |
| Is the person of concern experiencing financial problems, high personal debt, or bankruptcy? |
| Is there evidence of substance abuse, mental illness, or depression? |
| Has the person of concern spoken of homicide or suicide? |
| Does the person of concern have a past criminal history? |
| Does the person of concern have a planned course of action, and, if so, does the plan make sense, is it reasonable, and is it specific? |
| Does the person of concern have the means, knowledge, and ability to carry out their plan? |

# References


[1] Bureau of Justice Statistics (BJS), the Bureau of Labor Statistics (BLS), and the National Institute for Occupational Safety and Health (NIOSH), "Indicators of Workplace Violence, 2019," [Online]. Available: https://bjs.ojp.gov/library/publications/indicators-workplace-violence-2019 . [Accessed 16 05 2023].

[2] Occupational Safety and Health Administration, "Workplace Violence," [Online]. Available: https://www.osha.gov/workplace-violence. [Accessed 05 2023].

[3] Department of Labor, "DOL Workplace Violence Program - Appendices," [Online]. Available: https://www.dol.gov/agencies/oasam/centers-offices/human-resources-center/policies/workplace-violence-program/appendices. [Accessed 05 2023].

[4] shrm.org, "Workplace Violence," [Online]. Available: https://www.shrm.org/hr-today/trends-and-forecasting/research-and-surveys/pages/workplace-violence.aspx. [Accessed 16 05 2023].

[5] CyberSecurity and Infrastructure Security Agency, "ISC Violence in the Federal Workplace Guide," 12 2020. [Online]. Available: https://www.cisa.gov/resources-tools/resources/isc-violence-federal-workplace-guide.

[6] Texas Workers' Compensation, "Workplace Violence Fact Sheet: Protecting Employees from External Threats," [Online]. Available: https://www.tdi.texas.gov/pubs/videoresource/fswvpstrat.pdf.

[7] Cybersecurity and Infrastructure Security Agency, "Insider Threat Mitigation Guide," 11 2020. [Online]. Available: https://www.cisa.gov/sites/default/files/2022-11/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf. [Accessed 20 5 2023].

[8] sleuthkit.org, "Open Source Digital Forensics, Autopsy, The Sleuthkit," [Online]. Available: https://www.sleuthkit.org/autopsy/.

[9] Wireshark, [Online]. Available: https://www.wireshark.org/.

[10] IBM Watson, [Online]. Available: https://www.ibm.com/watson.

[11] Microsoft, "Microsoft Power Automate," [Online]. Available: https://powerautomate.microsoft.com/en-us/connectors/details/shared_teams/microsoft-teams/?slug=microsoft-teams.

# INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University



Shashidhar, N. & Varol, C. (2023) Workplace Harassment and Violence: A Primer on Critical Strategies for Small and Medium-Sized Businesses. (Report No. IHS/CR-2023-1029). The Sam Houston State University Institute for Homeland Security. https://doi.org/10.17605/OSF.IO/D67HV