ALFA International
THE GLOBAL LEGAL NETWORK

2024 International Client Seminar

February 29 - March 3, 2024

The 5 Olympic Rings of Crisis Communication: Commitment, Communication, Concentration, Control, & Confidence.

How to Ensure Your Company Medals Gold.

Kelly M. Hoffman, Esq.
Moderator
NORMAN, HANSON & DETROY, LLC
Portland, Maine
khoffman@nhdlaw.com

Christen Blackburn, Esq.
LEWIS THOMASON
Nashville, Tennessee
cblackburn@lewisthomason.com

Introduction

A crisis in the workplace can happen at any time and always seems to arise when we are least expecting it. The risk of potential crisis is unavoidable. However, recent crisis-level events globally have shown that certain types of catastrophic risks in the in the workplace often are accompanied by the collateral consequences of severe financial or reputational damage to a company, or liability flowing from ill-informed employment practices and poorly executed responses to catastrophe. These collateral consequences may be mitigated by developing a robust and dynamic crisis response plan informed by the past and which is constantly revised with an eye to the future.

If a company neglects to address the possibility of certain risks, the consequences in modern times can be dire. Employers now more than ever must realize that developing a proactive plan for handling disaster needs to be a priority for the sake of the physical wellbeing of its employees and the continued success of the company in the aftermath. To minimize the collateral effects of a crisis, this article reflects on the lessons learned over the past several years of employers responding to various disasters. What many employers may not consider while formulating a crisis response plan is action in context. Whether it be natural or manmade, a global pandemic, active shooters, bomb threats, cyber-attacks, or public relations crisis, what matters for most in mitigating collateral damage in a crisis is having a response plan informed by the law, the past and which is executed in a socially aware manner.

Building a Crisis Management Plan

The SARS-CoV-2 (COVID-19) pandemic starkly revealed the critical weaknesses, if not outright failures, in the infrastructure, plans, and preparedness of most organizations. To be fair, the COVID-19 pandemic was the first of its kind in terms of the scope of its devastation across sectors globally. However novel in intensity the COVID pandemic was, the world *had* experienced global disease outbreak relatively recently and was on notice that something this could happen again. Just eleven (11) years before, the H1N1 influenza (swine flu) pandemic of 2009 spread from Mexico and the United States to other part of the world in just two months.[1] Though the swine flu ultimately yielded a relatively low death toll and global economic impact, the unprecedented rate at which the swine flu spread was a harbinger of the risk that a more dangerous disease could pose in the future with the continued globalization of the world's economies and population.

To this day, businesses around the world continue to struggle with the fallout of the COVID-19 pandemic. The health, economic, and social impacts of the pandemic are significant. As of December 17, 2023, the World Health Organization reported nearly seven million COVID-related deaths reported globally.[2] The overwhelmed healthcare systems, supply chain disruptions, mandatory business and school closures, travel restrictions, and the transition to hybrid or entirely work-from-home employment models has resulted in a total estimated economic cost to the United States more than $16.1 trillion.[3]

It is impossible to predict what the next global disaster will be or when it will occur. Yet the factors believed to contribute to the spread of a new infectious disease continue to exist and will likely grow with time.[4] Some experts predict that the next pandemic may well be on its way.[5] COVID-19 and its on-going aftermath is a key example of how businesses can make a bad situation even worse when

they are forced to scramble and apply ad hoc solutions to address unanticipated problems.

Luckily, "knowledge is power" and one of the silver linings of the COVID-19 pandemic (as well as the other crises described below) is that employers now have the power to conduct internal self-assessment informed by what went wrong in the past to identify their company's strengths and weaknesses in their communication and response strategies.

One thing that all successful crisis management and communications plans must have in common is that they must be multi-faceted, dynamic, and functional at every level of a business's operations. Multi-faceted means strategizing the physical aspects of crisis management as well as anticipating information technology (IT), cyber security, human resources, and public relations disasters. Although each discrete category of crisis management must be a component part of a larger concerted mechanism that aligns with the business's corporate strategy or ideals, each component is a universe of its own warranting its own designated team.

Within each component universe of the crisis management plan, the overarching development strategy remains largely the same and follows these ten steps:

1. Identify the team devoted to each sector of the entity's crisis management strategy.

2. Each sector's team must outline the scenarios that the organization may face, informed by previous struggles within an organization as well as global events in the news. Having a specific sense of these potential occurrences must guide planning. It's not necessary to plan for every conceivable risk, but each crisis response team should cover a broad range (for example the physical crisis management team should consider everything from a pandemic recurrence to the effects of hurricanes or floods, to active shooters or bomb threats).

3. The team should develop a clear activation protocol. This means that the circumstances that trigger the crisis management plan should be well-defined to avoid wasting time in the event of an emergency.

4. Within each management team a clear chain of command needs to be established. The team must create a crisis management-related organization chart so it's clear who has final authority and who reports to whom. Making a well-defined organization chart supports coordination and consistency, which large, decentralized organizations can struggle to achieve on a larger scale. Depending on the seriousness of the event, the plan may require additional layers of command. For example, an emergency at one site may activate the response leader at that site, but a company-wide crisis will require a headquarters crisis team with regional teams operating beneath it. The relevant management team will also be heavily influenced by the type of crisis that is identified to be underway.

5. A command "center" should be identified, meaning that a base of operations for the team to return to in a crisis or where individuals can direct questions and concerns or escalate important information. In many circumstances a physical centralized locale is key to quick responses in

emergency scenarios.

6. Each team should develop a response action plan. This should be executed by performing detailed planning around how the team and the organization as a whole will respond to a variety of crisis scenarios. Such planning will require assigning responsibility for each task. The response actions should be analyzed and implemented as modular elements which can be tailored to the specifics of the emergency at hand. Conceptualizing crises in modular elements makes the crisis management plan more adaptable and flexible.

7. A defined external communication plan is critical. Particularly in the context of human recourses or public relations crises, there must be a defined plan for communication with the public and key external stakeholders. Businesses should appoint a spokesperson and write detailed instructions including holding statements which allow for more specific details to be entered later. It's important for an organization to leave room for external social and political context to be accounted for in their communications strategies. As explained below, to ensure that public communications align with the business's holistic public relations goals and to avoid further media complications, having a response informed by social context is key.

8. The response team should have sufficient emergency response resources. This may include financial resources, personal protective equipment, or a public relations advisor who is easily accessible. Information resources are particularly key in times of crisis, this may include maps of facilities, timelines, or flowcharts of key processes. Particularly key to human resources crises is having employee data, personnel files, and benefits information easily accessible.

9. Routine training program implementation is paramount to swift execution. Holding drills and exercises with the crisis management team is crucial toward achieving that goal. Rehearsals and drills can reveal flaws in the flow of a plan and may make the crisis team become more comfortable with their role in the plan and to work together more seamlessly.

10. A structured review process is important as your company and the risk environment changes. Additionally, and especially after any actual crisis occurs, the team should analyze what went well and what did not. It will be necessary to identify any pitfalls and implement necessary changes.

Below, this Article outlines the specific sectors where individualized crisis management teams should be developed and their processes implemented. This will include physical crisis management, IT crises, cyber threats, human resources crises, and consumer or public relations crises. Within each sector, relevant case studies and specific recommendations are discussed and offered. Ultimately, an analysis of crisis management in the context of modern events will help to improve how employers handle crises in the future across sectors and will minimize collateral financial loss and avoidable exposure to liability.

Physical Crisis Management

Physical security involves the protection of people, assets, and property from actions that could cause damage or lead to other forms of loss.[6] At its core, this involves keeping the brick-and-mortar facilities and everything within it safe from real world threats. The COVID-19 pandemic and recent disastrous weather events precipitated by climate change have shown that environmental threats must be anticipated in managing physical crises.[7]

While the health and safety hazards may be obvious at worksites with heavy machinery and equipment, which require employees to engage in a lot of strenuous labor, a number of hazards can be present in an office setting as well.[8] According to the Bureau of Labor Statistics, for the year of 2021-2022 employees in office and administrative positions spent collectively over 100,000 days away from work due to a workplace injury.[9] Many of these injuries are caused by falls, or ergonomic injuries that easily may have been prevented with sufficient planning and accommodation.

Environmental workplace hazards are not insignificant, yet the most concerning physical workplace hazards are becoming increasingly human. Workplace violence including potential active shooters and bomb threats occur very frequently. Therefore, employers should implement a restrictive security system at their building's thresholds of ingress and egress where employees work and where important records are stored or otherwise accessible.

It's common place for employers to require that employees or other regular facility personnel to use scannable security fobs that allow only authorized individuals to enter their building casually. Alternative methods of verifying visitors' entry are then established, such as requiring visitors to check in with a front desk attendant or security guard.

These systems aren't infallible. Particularly in multi-tenant commercial buildings or large enterprises, "tailgating" is common and creates loopholes in a company's ability to keep track of who has entered or left their facility.

Access to a building's facilities by an unauthorized employee is a security breach in and of itself that may expose certain enterprises (dealing in health care or certain other types of information) to civil liability under laws such as HIPAA. Additionally, if tailgating is a common and pervasive phenomenon in a multi-tenant commercial building, for example, an employer could be charged with constructive notice of third-party ingress and egress, resulting in as well the perverse result that if the unauthorized party were injured on the premises the employer may be found liable in tort.

Tailgating can impact a building's management practices as well. If the HVAC or lighting system is tied to occupancy an influx of unexpected individuals will affect energy expenditures. Additionally, having an inaccurate headcount during an emergency could lead to occupants who are unknowingly left behind or emergency personnel needlessly searching for people who were never on the premises.

Unauthorized entrants to a building pose many dangers beyond the civil liability of the premises owner and building management concerns. The entrant could threaten the physical safety of employees, steal information or merchandise, deposit malware on the business's servers, or even place

a bomb on the premises.

Preventing tailgating can be simple, and easily retroactively fit to a company's existing security systems. The cheapest solution begins with employee training and building a culture where employees are aware of the risks and feel empowered to challenge unfamiliar faces.[10] A more foolproof solution is to implement multiple levels of security hardware at building thresholds. For example, companies could implement a turnstile-type mechanism which allows for only one entrant to pass at a time with a security fob. Additionally, pin numbers could be an added requirement to a turnstile apparatus. Unique pin numbers would cut down on the likelihood that an employee's fob could be misplaced or stolen.

Employers should be very careful if they choose to implement a biometric system of employee verification as a safety mechanism. Several states such as Illinois, Texas, and Washington recent have enacted laws heavily regulating the use of biometric data and (in Illinois) giving employees (whose data was harvested) a private right of action if their data is handled improperly.[11] Though, for many employers dealing in highly sensitive matters, it may be worth installing biometric verification systems, in compliance with all governing law.

Workplace Violence

Workplace violence has grown to become a national epidemic that warrants focused attention and premeditated response plans at every level of an organization. Workplace violence is increasingly prevalent and is a crisis identified as one of the fastest growing problems in the United States. Estimates suggest that yearly costs to employers for incidents of workplace violence have reached billions of dollars.

Quantifying the acts and means of violence inducing crisis in the workplace may at times be challenging because technology has diversified the conceivable mechanisms for nefarious actors to cause harm. Furthermore, limiting such a calculation to a numerical measure of the problem cannot convey the meaning of loss of a human life, the emotional impact on those affected, and the qualitative cost to society beyond the impacted organizations.

On a personal level for those employees on the ground, violence (and the looming shadow of its probability) increases stress, inflicts emotional wounds, and lowers morale. Organizationally, it diminishes credibility, decreases productivity, creates work-specific tension, and damages property. From a societal perspective, the constant threat of violence in the workplace creates political divide, incentivizes the dissemination of false information, and broadly has threatened to undermine the Constitutional protections of the First Amendment.

Every organization is susceptible to crisis by some form of workplace violence. Some may have robust crisis response programs in place, others may be unsure where to start in terms of building a crisis management program capable of anticipating and responding to the myriad threats that modern life presents. Some may have an established program and are seeking ways to improve upon what already exists. No matter how an organization might qualify the nature of their crisis response programs on introspection, it is of the utmost importance for organizations to be vigilant in their efforts to constantly review, revise, and update their practices informed by modern events.

The Threat of Active Shooters

The Federal Bureau of Investigation (FBI) defines an active shooter as someone "actively engaged in killing or attempting to kill people in a confined and populated area."[12] In 2023 alone, the United States experienced over 400 mass shooting incidents.[13] Yet many organizations do not have an active shooter response plan in place, and even fewer have trained their employees on what to do in an active shooter scenario. This is a huge mistake. Employers must provide the necessary resources and support to prevent such a scenario, if possible or how to stay safe if one occurs.

Training should be conducted by qualified instructors, who are experienced in law enforcement or military operations. Employees should be given the chance to ask questions and must be familiar with the layout of their workplace and have a plan of action in case of an emergency.[14] The training employees receive must inform them that they need to be physically and mentally prepared to face an active shooter. Where natural survival responses are fight, flight, fawn, or freeze the importance of mental training for moments of emergency can't be stressed enough.[15] Though the natural reaction to a dangerous event may be the inability to think or act decisively, fawning and freezing at such a critical moment can be deadly.[16]

The first step in training employees to avoid fawning and freezing if they were to face an active shooter is to inform them why they might engage in this responses (which is, most often due to fear). When the human brain goes into survival mode, focus turns entirely to the danger at hand and everything else is tuned out.[17] To best overcome this initial response, employees need to train their brains to focus during a crisis.

The best way to train employees to avoid freezing is to instruct them to picture themselves in an active shooter scenario. Next, they should visualize themselves confidently taking action and escaping or helping to stop the threat. A useful mnemonic is: O-M-G, which stands for Orient, Move, and Ground.[18] Practically, requiring that employees practice drills evacuating the building will not only provide estimates of how much time it takes to clear the building, but also will ensure that employees are practicing "MOVE," towards maintaining conscious connection with the body as opposed to contracting in fear.[19] Instilling a sense of urgency in the drills will help staff to focus consciously on escaping the threat in the moment instead of freezing. Further to combat freezing or fawning, employees should be encouraged to not only visualize movement, but if they begin to feel overwhelmed to engage their bodies with small movements: wiggling their toes, rubbing their hands together, feeling their feet on the ground, imagining themselves running through grass with bare feet or feeling the wind hitting their faces.[20]

The next step is to ensure that the company is ready from an operational perspective. For example, installing physical apparatus to keep unauthorized entrants out of the building or security cameras is very important.

The Department of Homeland Security's Cyber Security and Infrastructure Security Agency (CISA) recommends that, once the threat of the active shooter no longer exists and all wounded individuals have been evacuated, the management should engage in post-incident assessments in conjunction with law enforcement and ensure that all relevant government agencies are notified of the incident.[21]

Management must account for all individuals, including those deceased. They must also assess the psychological state of individuals at the scene and refer them to counseling or health care services. Federal and State laws mandate the care of crime victims in certain circumstances. Notably, the Department of Justice and the Federal Bureau of Investigation's Office for Victim Assistance provides substantial resources. Though, in the crisis management plan, such resources should be identified and already on-hand.

After an active shooter event ends, the location is an active crime scene. The CISA dictates that nothing should be touched unless it involves tending to those wounded.

To assist with the quick dissemination of accurate information to friends, family and other interested parties, the CISA recommends establishing a Joint Information Center (JIC) through which all external communications relating to the incident can be funneled.[22] JIC enhances information coordination, reduces misinformation, and maximizes resources by having information officers accessible in a unified location.

After a crisis scenario ends, employers have many affirmative duties to help care for those affected. Managing the responses of victims and their families and friends requires things like sharing of information, coordinating medical and psychological care resources, and long-term plans for moving forwards.

Ultimately, redundancy is the key to a successful security plan. Having multi-dimensional tactics in the emergency response plan is non-negotiable and constantly reviewing and revising the plan that is in place must be routine.

Bomb Threats

Unfortunately, active shooting scenarios are not the only physical danger in the workplace that has become almost common in recent years. Bomb threats are not uncommon and have the potential to be incredibly dangerous. Although responding to a bomb threat is an incredibly disruptive process, the risk is simply too high not to take threats seriously and respond accordingly.

Bomb threats can be delivered in several ways such as through phone calls, letters, notes, social media, or even through air drop photo sharing. For example, in July of 2023 Southwest Airlines was forced to divert a flight from Las Vegas to Hawaii and execute an emergency landing in Oakland California due to a bomb threat. A passenger on the plane had used Apple's airdrop feature to send a message to all passengers who had air drop engaged that a bomb was on the plane.[23] The plane was landed immediately, and all passenger's luggage was immediately searched, no bomb was discovered.

Even though it was a false alarm in Southwest's case, bomb threats should never be taken lightly. CISA also has issued a checklist that is designed to help employees and decision-makers at commercial facilities respond in a uniform manner if they receive a bomb threat.[24] The instructions are tailored to responding when a bomb threat is received through the phone. In these cases, it is recommended to stay on the line as long as possible and to listen carefully and avoid hanging up. From a different phone, immediately contact authorities and await instructions.

These instructions are difficult to engraft onto the apple air drop threat case, which have proven to be increasingly common and do not provide for communication with the threat actor.[25] Employers, the facilities management, and dedicated crisis management team must anticipate the scenario where a bomb threat is delivered through a source like AirDrop. Although it is a new phenomenon, it must be addressed as a possibility. Perhaps, requiring that employees shut off their airdrop function while they are inside the facility would help reduce threats' spreading in this way. However, a facility chooses to address this threat, what remains of primary importance is planning ahead and developing a team and a plan of action.

Information Technology and Cyber Threat Crisis Management

Any business's Information Technology team is a key staple to day-to-day functionality. Whether it's on–boarding a new employee, fixing or supporting computers and software, or otherwise managing and improving a company's working online information management programs, properly functioning technology is what makes a company's wheels turn. Because it is such a key facet of everyday operations, IT threatens to become an Achilles heel. If it's not properly managed and backup plans are not forcefully enacted, a system error (or a bad actor who has hacked into a system) can paralyze operations, cause massive loss due to theft or ransomware, require affirmative data breach reporting response (which is costly), and expose the company to liability from data breach lawsuits. What's further concerning is that if the company's data security practices were suspected to be insufficient, state and federal agencies may commence an investigation and could possibly impose penalties if found to be deficient.

When a cyber incident occurs, the designated crisis response team must be ready to immediately respond with a strategic framework. The most important items of priority when something goes wrong with cybersecurity are to stop the bleeding, as in limit continuing damage, and reinstate normal operations as soon as possible. The information technology team will play a key role in identifying exactly where a breach has occurred and in suggesting possible remedies right away. Sometimes, a breach can be fixed by simply changing a password, but yet other times as in ransomware or other malware situations, the fix is not so simple.

Next, the crisis response team will often need to call for outside help from cyber security software vendors, cyber forensics investigations firms, the government, or industry partners devoted to helping remedy cyber security incidents and at times law enforcement especially where money or information has been stolen. These entities will need to help identify what information has been accessed, what has been stolen, and what residual issues the system will continue to face (depending on the malware at-issue).[26] Consider building relationships with these firms in advance and understand what is required to obtain their support before a true emergency arises. The FBI provides a dedicated hub for helping and reporting cyber and critical infrastructure attacks. Local law enforcement also should receive a report of the incident for their records, especially if there is financial loss.

Often cybersecurity incidents activate local or federal breach reporting obligations. Most states have a standardized breach reporting law, which depending on the type of information accessed (health, financial, or credit reporting data) the company may have heightened breach reporting

obligations to the individuals whose data was accessed and to the state attorney's general office (and in some rare cases the media). In California and in certain sectors such as healthcare and credit reporting, data breaches also create a private right of action for individuals whose data was subject to the breach.[27] In these instances, it is prudent for a company to promptly notify their cyber insurance carrier (or other commercial liability carrier which may provide coverage for cyber losses) of the possibility of data breach lawsuits.

What is highly important for the crisis response team in their development of a plan in anticipation of a data breach is to: first, understand what data the company handles, where it is stored, and how it is accessible; and second, the applicable state and federal laws that might apply to the sector of commerce in which the company deals. All data breach reporting laws have a "time is of the essence clause," though the level of specificity varies by state. The most relaxed require the reporting of data "as soon as is practicable," while others set a specific time frame. For example, Maryland requires business to report breach within forty-five (45) days of discovery or notification of the breach.[28]

While developing a crisis response plan, after the team become aware of all relevant cyber security obligations legally imposed on the business, routine cybersecurity drills testing the effectiveness of the program must be executed. They constantly should be tested and improved. This includes providing employee training on the identification and avoiding of phishing schemes in emails or other forms of electronic correspondence. As an aside, most cybersecurity insurance policies require routine employee training to ensure that employees and key personnel in the company understand their role in protecting data and systems.

"Social engineering" such as preying on employees through phishing schemes is a common method that hackers use to subvert even the best security software. Alternatively, hackers can physically enter a building by tailgating and upload a malware program to a company's system manually. What is additionally possible is for a disgruntled employee or newly fired employee who retains legitimate entry authority to the building to steal information or to upload malware that might facilitate their remote access later. Social engineer threats are not necessarily novel in 2023, but they are certainly something that must be planned for in a crisis response plan.

Money Wiring

Related to cybersecurity best practices are safe money wiring procedures. Nefarious actors can easily penetrate a business's computer system through a phishing scheme. Once an employee clicks on the phishing link, an invisible piece of code can remain in the system's software system and monitor the business's transactions and external communications.[29] The bad actor can lay dormant for months or even years waiting for a large financial transaction and observing business customs. At the perfect moment, the hacker is able to mimic the correspondence between parties and fool one or the other to wire money into a fraudulent account (believe they were speaking to the party they had be dealing with for months). The hacker then will immediately abscond with the money.

These types of schemes happen when parties have been engaged in business together for a long time and trust that money will be sent as part of routine business. It is a mistake not to implement a dual identity verification procedure before sending large sums of money, even to those a business may

feel certain is a legitimate enterprise.[30] The United States Office of the Comptroller of Currency recommends invoking the following protections.

1. Never provide personal information in response to an unsolicited request, even if benign.

2. If one believes that the contact is legitimate, contact the financial institution independently to verify. It can never hurt to quickly follow up before moving forwards.

3. Never provide a password over the phone or in response to an unsolicited request online.

4. Review account statements regularly to ensure that all charges are correct.[31]

If funds are re-directed as a result of phishing or the actions of a nefarious third party, they are almost impossible to get back. What's more, if the business that has lost sent the funds files an insurance claim for losses under their commercial property loss policy, they will likely not be covered. This is because the standard cyber-related lost endorsement covers losses due to cyber activity, implying that the loss was caused by a third party removing the funds from the possession of the business. If the business voluntarily (though mistakenly) redirects the funds into the hands of the bad actor, the loss generally will not fall under the cyber activity coverage provision.

In sum, a simple multi-factor verification mechanism is critical when transferring large sums of money through the internet, even in routine business dealings with familiar parties.

Human Resources Crisis Management

A business's human resources team plays a fundamental role in any crisis management plan as a centralized information hub for employees and often is the first point of contact an employee may have with a business.

Some crises are specific to human resources, however. The HR team must be cognizant of applicable employee rights. Specifically, this is pertinent to the accumulation and handling of a personnel file, reasoning behind hiring and firing decision, and the company's response to employee complaints of harassment from other employees. Human resources also must remain aware of employees' off-duty conduct in certain circumstances. Even off–duty conduct can have a material effect on an employer's liability if it is shown to be an extension of a pattern of behavior exhibited at work.

For example, in the First Circuit case of *Crowley v. L.L. Bean*, the Court affirmed the jury verdict issued by the lower court finding that L.L. Bean was liable under Title VII of the civil rights act of 1964 and the Maine human rights act for maintaining a hostile work environment by disregarding the totality of the evidence that a coworker was sexually harassing the plaintiff.[32]

In *Crowley*, the plaintiff was an employee at the L.L. Bean warehouse in Freeport, Maine and worked filling catalogue orders.[33] One of her male co-workers started to incessantly stalk and sexually harass her. The plaintiff reported most the incidents of harassment to her shift supervisors and team leaders. One (1) month after the plaintiff reported the harassment to the shift leaders, her stalker was moved to a separate work area. Nonetheless, due to the pervasiveness of the stalker's conduct, L.L.

Bean had in effect facilitated a hostile work environment for the plaintiff.[34] The Court explained that,

Title VII of the Civil Rights Act of 1964 provides, in relevant part, that "[i]t shall be an unlawful employment practice for an employer . . . to discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual's race, color, religion, sex, or national origin." 42 U.S.C. § 2000e–2(a)(1). The Supreme Court has stated that, "'[t]he phrase "terms, conditions, or privileges of employment" evinces a congressional intent to strike at the entire spectrum of disparate treatment of men and women in employment,' which includes requiring people to work in a discriminatorily hostile or abusive environment."[35]

For the Plaintiff to prove a claim of hostile work environment sexual harassment, she would need to prove that the harassment she was subject to based on her sex was so "severe and pervasive so as to alter the conditions of" her employment and create a hostile work environment.[36]

L.L. Bean argued that it had taken sufficient remedial measures to ensure that, while the plaintiff was at work, her stalker would not be near her. The supervisors did this by changing the warehouse location where the stalker was assigned to work and gave his strict written warning instructions not to contact the plaintiff.

Reviewing the plaintiff's entire recitation of stalking and harassment incidents, the Court found that when viewed as a whole, L.L. Bean had allowed the stalker to create a hostile work environment so severe and pervasive as to alter the conditions of Crowley's employment, even though some of the instances of harassment did not occur at work.[37]

The stalker would not just follow the plaintiff at work. The plaintiff reported to her supervisors instances where the stalker entered her home uninvited, would "volunteer for shifts" that he was no scheduled to work to work in the warehouse with her and would otherwise spend his off-duty time furthering his harassment of her.[38]

Even though L.L. Bean could not have controlled the stalker's off-duty conduct as it pertained to the plaintiff, his off-duty conduct contributed to the Court's holistic interpretation of the severe and pervasive harassing environment was created by L.L. Bean's failure to reprimand or terminate him.

What the L.L. Bean case stands for in the context of human resources liability is that employers must evaluate complaints holistically and include analyzing off-duty conduct of co-workers when necessary to avoid creating a severe and pervasive hostile work environment. Employers cannot control the off-duty conduct of employees. However, once they are made aware of it, they also must be cognizant of how their response to employee off-duty conduct can be highly consequential (as explore further *infra*).

Relatedly, employee free speech in and outside the office has the potential to cause a human resources disaster and should be addressed in a uniform, content neutral manner.

While the First Amendment guarantees the right to free speech and religion, private employers may regulate speech in their workplace as they see fit so long as it is not done in a discriminatory

manner. Additionally, employers should be wary of laws that indirectly protect certain types of speech.

For example, the National Labor Relations Act (NLRA) governs how employers and unions dela with each other and individual employees. It also protects certain activities and speech between employees, union, and non-union about their conditions of employment. Discussion of workplace safety, work environment, management, and wages are examples of protected speech. The National Labor Relations Board (NLRB) is responsible for enforcing grievances filed for adverse actions taken for engaging in such protected speech.[39]

Additionally, anti-discrimination and whistleblower protection laws prohibit employers from taking retaliatory action against employees for reporting harassment, discrimination, or unsafe work conditions or other violations of law.

Purely political speech, however, may be restricted by private employers in the workplace if it is not prohibited in a discriminatory manner.

Online Harassment

Employers may find at times that online harassment of an employee makes its way into the workplace. Often, the goal of the harasser in their campaign to damage the reputation of their target is to cause the target to be fired due to off-duty conduct. As noted above in the *Crowley* example however, employers also have an affirmative duty to create a workplace that is free from discrimination and harassment. Yet, as the standardized workplace transitions online, issues arise when staff continue to experience hate and abuse on the internet.

Over 44% of Americans report that they have experienced some kind of online harassment.[40] Those with public-facing jobs such as journalists or politicians may experience online abuse as par for the course in their day-to-day.

The sheer volume of harassment and the ease at which harassment can be delivered anonymously at times make it extremely difficult for an employer to discern when additional investigation is warranted and when a given harasser simply needs to be blocked and ignored.

As an organization, the human resources team can plan and develop a strategy for handling employee online harassment in the same way that other crises can be planned and prepared for.

The plan can include a formal acknowledgment of the harm to the employee, especially for those in protected classes and who may feel targeted and isolated, facilitating employees to bring these issues forward is the first step toward addressing and remediating the problem.

Next, the crisis response team should assess the scope of the harassment and the nature of it. At times, this could require an investigation into the veracity of the allegations of the harasser. For example, online harassers might attempt to send a target's employer nude photographs of the target to humiliate them or perhaps allege that the target did something illegal or against corporate policy. The investigation team should consider how public the harassment is and whether the brand is implicated in

their response to the harassment.

Finally, the team should create protocols and offer training opportunities. If an employee finds they are being harassed online, there should be a clear set of concrete steps that they can utilize to get help from the employer. This may require the employer to develop an internal reporting system to facilitate the ability of employees to report more easily. This process should include clear documentation and escalation procedures to avoid future liability due to mishandling.

Consumer and Public Relations Crisis Management

One risk that could mean life or death for many companies is damage to reputation.[41] If a public relations crisis were to occur, it is extremely important that the company address it quickly and decisively before things spiral out of control. Public relations should have a team devoted to planning and responding to crisis that is as prepared as those teams devoted to physical threats. The following steps can help prepare for public relations disasters.

1. To the extent possible, brace for impact.[42] Sometimes, a company can anticipate when something will become a public relations disaster. For example, in August of 2021, Delta Airlines announced that it was going to require that employees pay an additional $200 per month for health insurance if they refused to get COVID-19 vaccines.[43] When Delta released the vaccine-related health insurance surcharge publicly, its stock price fell by over five percent (5%). When the damage has already been done, the best line of action is ensuring quick and definitive communication with the public, responsive to their reaction.

2. Reflect on what has happened by gathering as much information as possible. Before responding publicly, understand the social climate of what has happened and consider the company as a participant in a national conversation.

3. Once you understand the nature of the crisis, the social and political context, and your company's perspective enact a three-pronged strategy in publicizing your response. (1) Admit that there is an issue in your response. (2) Explain how the company handled the situation. (3) Lay out what leadership will do if the same or similar situation were to arise again.[44]

It can take decades to rebuild a company's reputation and only moments to ruin it. Having a well develop plan for approaching potential public relations crisis is of the utmost importance.

Responding to Nefarious Internet Campaigns (Trolls)[45]

Social media is a powerful tool that allows people to share their true perspectives about brands, social events, and the news, both positive and negative. Often, these opinions are less constructive and instead are rude, outrageous, or simply wrong. Feuds on X (formerly Twitter) are common and viral campaigns across social media platforms spurred by a simple hashtag can back companies into a public relations corner: either respond swiftly and decisively or risk being cancelled. Although viral trolling campaigns may gain momentum in the spirit of jest, silence, or worse negative backlash from the target company thrust into the limelight, it can be far more damaging from a public relations perspective than

by responding in a calculated manner.

This is easier said than done, depending on the demand of the trolling campaign. For example, in 2017 a man named Bradley Reid posted on Cracker Barrel's corporate Facebook page publicly asking why his wife, Nanette had recently been fired from her retail manager position that she had held at an Indiana Cracker Barrel for over eleven (11) years.[46] Internet pranksters quickly picked on Brad's comment and flooded the Cracker Barrel Facebook page with comments about "Brad's Wife." After a comedian picked up on the trend and brought the discussion to X (then Twitter), the hashtag #JusticeforBradsWife was born and many memes[47] followed soon thereafter directing the attention of millions of users online. Ultimately, Brad's Facebook post became internet famous and generated a petition (with over 20,000 signatures) demanding answers from Cracker Barrel as to why Nanette Byrd lost her job in 2017.[48]

Cracker Barrel remained silent throughout the entire discourse. Of course, they could not legally answer the internet harasser's questions and provide the actual reasoning behind why Brad's wife was fired (in many states employee personnel files are confidential by law). Nor did Cracker Barrel legally *need* a reason to fire Brad's wife because Indiana is an at will employment state, and restaurant managers (especially at restaurant franchises like Cracker Barrel) rarely have employment contracts which would change their at will status. Furthermore, engaging with the "angry mob" online by explaining the legal impropriety of their furnishing a reason for Nanette's termination would undoubtedly be met with incredulity and harsh cynicism aimed at the messenger (Cracker Barrel). It was a "no-win" scenario for Cracker Barrel and perhaps silence was the best approach to this scheme at the time.

These schemes are unpredictable, but companies can develop a method for approaching them when they do arise in the same way as preparing for any other crisis.

1. Try to understand where your critics are coming from.[49] Distinguishing between genuine complaints and hecklers is important for formulating a response strategy. If the complaint is well-founded, be honest about your product or service and try to resolve the dilemma with genuine empathy to the extent possible.

2. Ask internally, "how could we make it right?" Even the hypothetical answer to this question will reveal whether your approach could be solved by leaning into the accusations with humor or shutting down communication with an individual.

3. Be responsive (with humor when appropriate). Your brand's social media page will be watching the discourse. Trolling campaigns are more for attention than anything else (though they may appear to be trying to generate a negative image of a brand). They also provide the company to be in the limelight themselves if they choose the proper time to respond with humor.

4. Consider the impact that the event and your response will have on search results for your company and try to generate positivity on your social media platforms in the aftermath to counteract the event. Responses should focus less on changing the mind of the "troll" and more

on how they will appear to future customers or prospective employees.

5. Finally, show that your company cares and encourage critics to take the conversation offline and direct them to an email or phone number where they can file a formal complaint. Ultimately, when humor and silence are out of the question, responding with demonstrable compassion will reflect on your brand the best.

The public are familiar with trolls and social media brand smearing campaigns by now so, depending on the level and joviality of the accusations, companies can harness troll's comments and turn them into something positive. However, they also can quickly become public relations disasters that require premeditated and swift response plans.

Responding to Employee-Caused Public Relations Crises

In a similar vein, social media storms have facilitated the escalation and mass publication of outlandish conduct of individuals. This is particularly true when the conduct in question invokes a particularly sensitive political or social discourse. Indeed, the speed of the circulation on social media is driven by context – if the individual's actions are particularly tone deaf (or in opposition to) a modern social/political issue their actions will be widely published online against their will. The employers of the individuals who "go viral" for their bad behavior are now part of the conversation online. Any disciplinary action, termination, or silence on the employer's part due to the employee's behavior will instantly become part of the "storm." This has the potential to gravely harm a brand's image or alternatively, to harness the support of the critics of the employee.

For example, on May 25, 2020, a video went viral in which Amy Cooper, an insurance investment portfolio manager at Franklin Templeton, confronted a Black man who was birdwatching in Central Park, Christian Cooper. After Mr. Cooper had requested that Amy leash her dog, in accordance with park rules, Amy responded with anger and called the police. Cooper began filming the incident. The video shows Amy saying that she was going to tell the police that "there's an African-American man threatening my life."[50] This comment suggested that she was attempting to weaponize the police against Cooper. Online, this was collectively viewed as a gruesome allusion to the murder of George Floyd at the hands of Minneapolis police earlier in May of 2020. The video of George Floyd's death caused national outrage and sparked significant protesting and campaigning aimed at stopping police brutality directed against Black and Brown people.

The video of Cooper "became intentional news as a racial flashpoint" and online, Cooper was quickly branded as a "privileged white female 'Karen.'"[51] On the same night of the Central Park Incident, Amy's then-employer Franklin Templeton, published the following statement on Twitter (now X) concerning the incident, "[w]e take these matters very seriously, and we do not condone racism of any kind. While we are in the process of investigating the situation, the employee has been put on administrative leave."[52] The following morning, Franklin Templeton posted on Twitter (now X) that they made the decision to fire Amy Cooper, stating "[w]e do not tolerate racism of any kind at Franklin Templeton."[53] In the aftermath of the terminating Cooper, Franklin Templeton also participated in several interviews with the news media about their decision. In a July 6, 2020, interview with Fortune

Magazine, their spokesperson again reiterated that the company "espouses zero tolerance for racism."

Cooper subsequently filed a lawsuit in the Southern District of New York against Templeton under 42 U.S.C. § 1981, the New York State Human Rights Law and the New York City Human Rights Law claiming that she faced the adverse employment action of having an insufficient investigation conducted prior to her termination on account of her race and gender. She also filed a defamation claim among several others. The District Court granted Templeton's motion to dismiss for failure to state a claim on all counts and Cooper appealed to the Second Circuit.

The Second Circuit affirmed the lower court's dismissal. Pertinent to the race and sex-based discrimination claims, the Court stated that,

Plaintiff fails to allege facts giving rise to even a minimal inference of discriminatory motivation with respect to her termination. To the extent that Plaintiff contends that Defendants "implicated the race of their employee with each of [their] communications to the public, by repeatedly connecting [their] stated stance against racism with their termination of the Plaintiff," that argument fails as a matter of law. Defendants' statements made no mention of Plaintiff's race, and even to the extent they could be read as accusing Plaintiff of being a racist, "a statement that someone is a 'racist,' while potentially indicating unfair dislike, does not indicate that the object of the statement is being rejected because of h[er] race. 'Racism' is not a race, and discrimination on the basis of alleged racism is not the same as discrimination on the basis of race.[54]

The Court then continued to address Cooper's defamation claims and alluded directly to the social and political context from which the facts arose. The Court explained that, to the "extent that [Templeton's] statements are read as accusing Plaintiff of being a racist, the reasonable reader would have understood this to be an expression of an opinion *based on the widely circulated video of Plaintiff's encounter with Christian Cooper.*"[55] The Court continues to reveal that national political context is what justified Templeton's "opinion" that the video of Cooper's encounter demonstrated racism.

The Plaintiff sought to salvage her defamation claim by arguing that Templeton's Twitter posts implied the existence of "undisclosed facts upon which their opinion was based." However, in response to this argument the Court made clear that Templeton's May 26 statement,

[W]as [made] "following [Defendants'] internal review *of the incident in Central Park yesterday*," was made less than 24 hours after video of the Central Park incident was circulated widely and "became international news as a racial flashpoint," and "***took place in the midst of an ongoing national reckoning about systemic racism,***"—would be understood by the reasonable reader as being based on the publicly available video of the incident.[56]

Clearly, the publicity of the video and the national social context where anger relating to systemic racism is at a peak heavily influenced the Court's analysis of the law affecting each of Cooper's claims.

The lesson to draw from the "Central Park Karen" case is that the employer of people who become political sensations online (voluntarily or otherwise) is part of the conversation from a public

relations perspective. The employer should be aware of the law and the potential for liability after taking adverse employment actions against the "political sensation," but must consider the social and political atmosphere of the nation *first and foremost* before acting. Under different circumstances, Cooper's defamation claim may have survived a motion to dismiss (had the video of Cooper's incident in the park not been so widely circulated, perhaps the Court could have found Templeton to have implied the existence of undisclosed facts upon which its opinion was based).

Even if an employer knows for certain that their actions are legally sound, it still must consider political context and national perception of the issue.

Conclusion

In summary, there are myriad ways that modern business may experience crisis. What is consistent is that the best way to prepare for these various calamities is through planning, development of a dedicated team with resources, and constant revision and training opportunities that are targeted to procure specific goals. It's impossible to predict when a crisis may emerge, but having a multi-faceted and adaptable plan will be the best strategy to prevent them or to mitigate collateral damage when they do occur.

---

[1] *Past Pandemics*, CTRS. FOR DISEASE CONTROL & PREVENTION, (Aug. 18, 2018) https://www.cdc.gov/flu/pandemic-resources/basics/past-pandemics.html.
[2] *COVID-19 Epidemiological Update – 22 December 2023*, WORLD HEALTH ORG. (Dec. 22, 2023) https://www.who.int/publications/m/item/covid-19-epidemiological-update---22-december-2023.
[3] David M. Cutler & Lawrence H. Summers, *The COVID-19 Pandemic and the $16 Trillion Virus*, JAMA (Oct. 20, 2020).
[4] Such factors include overpopulation, animal husbandry, human encroachment on wildlife habitats, global trade and travel, and climate change.
[5] *Viruses of Special Concern*, CTRS. FOR DISEASE CONTROL & PREVENTION, (Apr. 29, 2019) https://www.cdc.gov/flu/pandemic-resources/monitoring/viruses-concern.html.
[6] Dan Swinhoe, *What is Physical Security? How to Keep Your Facilities and Devices Safe from on-site Attackers*, CSO (Aug. 4, 2021) https://www.csoonline.com/article/566635/what-is-physical-security-how-to-keep-your-facilities-and-devices-safe-from-on-site-attackers.html.
[7] *See* CLIMATE CHANGE ACTION PLAN, U.S. DEP'T OF LABOR (Sept. 9, 2021) https://www.sustainability.gov/pdfs/dol-2021-cap.pdf.
[8] Lauretta Claussen, *Office Safety: 25 Steps to a Safer Office*, (June 1, 2011) https://www.safetyandhealthmagazine.com/articles/recognizing-hidden-dangers-25-steps-to-a-safer-office-2.
[9] EMPLOYER-RELATED WORKPLACE INJURIES AND ILLNESSES (RELEASE) NEWS RELEASE, U.S. BUREAU OF LABOR & STATISTICS (Nov. 8, 2023) https://www.bls.gov/news.release/osh.htm.
[10] Jennie Morton, *Ten Strategies to Prevent Tailgating*, BUILDINGS (Dec. 6, 2011) https://www.buildings.com/safety-security/article/10189918/10-strategies-to-prevent-tailgating.
[11] *See* Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14.5 (2023); Capture or Use of Biometric Identifier (CUBI), TEX. BUS. & COM. CODE ANN. § 503.001 (West 2023); WASH. REV. CODE § 19.375.020 (2023).
[12] *Active Shooter Incidents in the United States in 2021*, FBI https://www.fbi.gov/file-repository/active-shooter-incidents-in-the-us-2021-052422.pdf/view.
[13] Paul LeBlanc & Annette Choi, *United States Tops 400 Mass Shootings in 2023*, (July 24, 2023) https://www.cnn.com/2023/07/24/politics/us-400-mass-shootings/index.html.
[14] Gene Petrino, *How to Put an Effective Active-Shooter Response Plan in to Practice*, SHRM (Oct. 28, 2022) https://www.shrm.org/topics-tools/news/risk-management/how-to-put-effective-active-shooter-response-plan-practice.
[15] *See*, Steve Haines, *Trauma is Really Strange*, (2016), https://student.londonmet.ac.uk/media/london-metropolitan-university/london-met-documents/professional-service-departments/student-services/counselling-service/trauma-is-really-

strange.pdf
[16] Gene Petrino, *How to Put an Effective Active-Shooter Response Plan in to Practice*, SHRM (Oct. 28, 2022) https://www.shrm.org/topics-tools/news/risk-management/how-to-put-effective-active-shooter-response-plan-practice.
[17] Gene Petrino, *How to Put an Effective Active-Shooter Response Plan in to Practice*, SHRM (Oct. 28, 2022) https://www.shrm.org/topics-tools/news/risk-management/how-to-put-effective-active-shooter-response-plan-practice.
[18] Steve Haines, *Trauma is Really Strange*, (2016), https://student.londonmet.ac.uk/media/london-metropolitan-university/london-met-documents/professional-service-departments/student-services/counselling-service/trauma-is-really-strange.pdf
[19] *Id.*
[20] *Id.*
[21] U.S. DEP'T OF HOMELAND SECURITY CYBER SECURITY & INFRASTRUCTURE AGENCY, PLANNING AND RESPONSE TO AN ACTIVE SHOOTER (ed. 2021) https://www.cisa.gov/sites/default/files/publications/Planning%20and%20Response%20to%20an%20Active%20Shooter_2021.pdf.
[22] *Id.*
[23] Joshua Zitser, *A Las Vegas Flight to Hawaii Was Diverted After a Passenger AirDropped a Photo Suggesting There Was a Bomb on the Plane to Other Passengers, Police Say* BUSINESS INSIDER (July 6, 2023) https://www.businessinsider.com/southwest-flight-las-vegas-hawaii-diverted-airdrop-bomb-threat-police-2023-7.
[24] CISA, BOMB THREAT PROCEDURES https://www.cisa.gov/sites/default/files/publications/Bomb-Threat-Procedure-Checklist.pdf.
[25] *See, e.g.*, Jean Carmela Lim, *Passenger Removed from Flight, Arrested After Sending Bomb Threat Via AirDrop*, AEROTIME HUB (July 3, 2023) https://www.aerotime.aero/articles/passenger-removed-from-flight-arrested-after-sending-bomb-threat-via-airdrop; Zach Wichter, *A Young Traveler Sent a Bomb Threat via AirDrop to Fellow Passengers. Now They're Facing Charges*, USA TODAY (Feb. 24, 2023) https://www.usatoday.com/story/travel/airline-news/2023/02/24/airdrop-bomb-threat-flight/11338128002/; Michelle Kaufman, *FBI: Greenfield Man Used AirDrop to Send Fake Messages About an Airplane Bomb During Flight*, WRTV INDIANAPOLIS (Oct. 2, 2022) https://www.wrtv.com/news/local-news/crime/fbi-greenfield-man-used-airdrop-to-send-fake-messages-about-an-airplane-bomb-during-flight.
[26] DEP'T OF HOMELAND SECURITY, CYBERSECURITY & INFRASTRUCTURE AGENCY, CYBER ESSENTIALS (2020) HTTPS://WWW.CISA.GOV/SITES/DEFAULT/FILES/PUBLICATIONS/CYBER%20ESSENTIALS%20TOOLKIT%206%2020201113_508.PDF.
[27] *See* Cal. Rev. Stat. Ann. § 1798.150; 15 U.S.C. § 1681.
[28] MD. COMM. CODE. ANN. § 14-3504(a)(3).
[29] OFF. OF THE COMPTROLLER OF CURRENCY, *How Phishing Works*, https://www.occ.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/phishing-attack-prevention.html#howphishingworks.
[30] *Id.*
[31] *Id.*
[32] Crowley v. L.L. Bean, 303 F.3d 387, 410 (1st Cir. 2002).
[33] *Id.* at 392.
[34] *Id.* at 399.
[35] *Id.* at 394.
[36] *Id.*
[37] *Id.*
[38] *Id.* at 398.
[39] 29 U.S.C. §§ 151-169.
[40] Viktorya Vilk, *What to do When Your Employee Is Harassed Online*, HARVARD BUSINESS REV. (July, 31 2020) https://hbr.org/2020/07/what-to-do-when-your-employee-is-harassed-online.
[41] Brian O'Connell, *Risk Managers: What's Your Plan for A Public Relation's Crisis?*, SHRM (Oct. 12, 2021) https://www.shrm.org/topics-tools/news/managing-smart/risk-managers-whats-plan-public-relations-crisis.
[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] A "troll" in this context is defined by Miriam Webster as either a noun or verb describing the act or person who

antagonizes others online by "deliberately posting inflammatory, irrelevant, or offensive comments or other disruptive content." *Troll*, MERRIAM WEBSTER ONLINE, https://www.merriam-webster.com/dictionary/troll.

[46] *See* Maura Judkis, *Why Did Cracker Barrel Fire Brad's Wife? The Internet Demands Answers*, WASH. POST (Mar. 24, 2017) https://www.washingtonpost.com/news/food/wp/2017/03/24/why-did-cracker-barrel-fire-brads-wife-the-internet-demands-answers/.

[47] Memes are either "an amusing or interesting item (such as a captioned picture or video) or genre of items that widely spreads online especially through social media" or "an idea behavior, style, or usage that spread from person to person within a culture." *Meme*, MERRIAM WEBSTER ONLINE, https://www.merriam-webster.com/dictionary/meme.

[48] Suzanne Lucas, *Why You Should Stop Harassing Cracker Barrel About Brad's Wife*, BUSINESS INSIDER (MAR. 25, 2017) https://www.inc.com/suzanne-lucas/why-you-should-stop-harassing-cracker-barrel-about-brads-wife.html.

[49] *See* FORBES' COMMUNICATION PANEL, *Dealing with Social Media Trolls on Your Company Page? Here's 11 Ways to Handle Them*, FORBES (Jun. 24, 2019) https://www.forbes.com/sites/forbescommunicationscouncil/2019/06/24/dealing-with-social-media-trolls-on-your-company-page-heres-11-ways-to-handle-them/?sh=586582856519.

[50] Jonathan Stempel, *Woman Who Called Police on Black Bird-Watcher in Central Park Loses Employment Appeal,* REUTERS (Jun. 8, 2023) https://www.reuters.com/world/us/woman-who-called-police-black-bird-watcher-central-park-loses-employment-appeal-2023-06-08/.

[51] Cooper v. Templeton, 629 F. Supp. 3d 223, 228 (S.D. N.Y. 2022), *aff'd sub nom* Cooper v. Franklin Templeton Invs., No. 22-2763-CV, 2023 WL 3882977 (2d Cir. June 8, 2023). The quoted material is drawn directly from Amy's first amended Complaint in her employment discrimination suit against Templeton.

[52] *Id.*

[53] *Id.*

[54] Cooper v. Franklin Templeton Invs., No. 22-2763-CV, 2023 WL 3882977, at *3 (2d Cir. June 8, 2023) (cleaned up).

[55] *Id.* at *4 (emphasis added).

[56] *Id.* (emphasis added).