Executive Risk Newsletter

Q4 2022

presented by Winters-Oliver Insurance Agency

Preventing Business Email Compromise Scams

Cybersecurity has become a priority topic of discussion inside corporate boardrooms and C-suites. While cybersecurity may have been viewed as an “IT problem” in the past, it is now often considered a part of overall enterprise risk management.

An increasingly frequent and complex cybersecurity threat is business email compromise (BEC) scams. According to the Federal Bureau of Investigation (FBI), this tactic has resulted in more than $43 billion in losses since 2016.

In a BEC scam, cybercriminals send an email that appears to come from a known source—such as a senior-level employee, vendor, business partner or another organization—making a legitimate request in order to obtain unwarranted access to organizational systems, funds or data. The FBI has identified the following as the five major types of BEC scams:

1. **CEO fraud**—In this type of scam, attackers position themselves as the CEO or executive of a company and typically request funds to be transferred to an account they control.
2. **Account compromise**—This attack entails an employee’s email account being hacked and used to request vendor payments. The money is then sent to fraudulent bank accounts owned by the attacker.
3. **False invoice scheme**—The scammer will act as if they are a supplier and request fund transfers to fraudulent accounts.
4. **Attorney impersonation**—This scam occurs when an attacker impersonates a lawyer or legal representative, commonly targeting lower-level employees who wouldn’t have the knowledge to question the validity of the request.
5. **Data theft**—This type of attack typically targets HR employees to obtain personal or sensitive information about individuals within the company.

To mitigate the risk, organizational leaders should:

- **Educate employees.** Train employees on how to detect and prevent BEC scams.
- **Implement effective payment protocols.** Analyze invoices and fund transfer requests to ensure their validity.
- **Restrict access to sensitive data.** Only provide trusted, experienced employees with sensitive data. Implement access controls and multifactor authentication measures.
- **Utilize security features.** Ensure all organizational devices have adequate security features, including access to a virtual private network, antivirus and malware prevention programs, email spam filters, data encryption capabilities and a firewall.
- **Have a plan.** Create an effective cyber incident response plan to minimize damages.

BEC scams can result in stolen data, financial hardship and potentially severe reputational damage. Board members should be proactive in protecting their organization against such risks. For more risk management guidance, contact us today.

EEOC Issues Revised Guidance on Workplace COVID-19 Screening

The U.S. Equal Employment Opportunity Commission (EEOC) has updated its guidance about conducting COVID-19 tests on employees and other pandemic-related issues. According to the EEOC, the changes were made to acknowledge that pandemic circumstances have evolved.

In the updated guidance, employers covered under the Americans with Disability Act must assess whether the current pandemic and workplace circumstances justify COVID-19 viral testing for on-site employees. Employers must show that the testing is a job-related business necessity.

The EEOC suggests employers consider the following factors:

- The level of community transmission
- The vaccination status of employees
- The accuracy and speed of processing for different types of COVID-19 viral tests
- The degree to which breakthrough infections are possible for employees who are up to date on vaccinations
- The ease of transmissibility of the current variants
- The possible severity of illness from the current variants
- The types of contact employees may have with others in the workplace or elsewhere

For more information on the updated guidance, visit the EEOC website.

The Growing Issue of Age Discrimination

Age discrimination, or ageism, in the workplace involves treating an applicant or employee unfavorably because of their age. While the Age Discrimination in Employment Act forbids age discrimination against people aged 40 or older in all aspects of employment—including hiring, firing, pay, job assignments, promotions, layoffs, training and benefits—it's still a common occurrence. According to a survey by the American Association of Retired Persons (AARP), nearly 80% of older employees say they've seen or experienced age discrimination in the workplace.

Age discrimination can have devastating effects on both employees and employers. According to the World Health Organization, around 6.3 million cases of depression globally are attributed to ageism. It can also cause a decline in employee motivation, resulting in decreased productivity and reduced work quality.

The economy also suffers when age discrimination occurs. AARP found the United States lost out on potentially $850 billion in economic growth in 2018 because of discrimination against older workers, based on the effects of lost jobs for older workers on the gross domestic product, wages and salaries. This figure is predicted to grow to $3.9 trillion by 2050. In addition, the 2019 Hiscox Ageism in the Workplace Study found that between 2010 and 2018, employers paid over $810 million to settle age discrimination charges with the U.S. Equal Employment Opportunity Commission. That number doesn't include litigation costs.

The Bureau of Labor Statistics expects nearly 40% of adults ages 65 to 69 and nearly 25% of adults ages 70 to 74 will still be working by 2030—up from 33% and 19%, respectively, in 2020. As the aging workforce continues to grow, it's important for organizations to take the following steps to prevent age discrimination in the workplace:

- **Assess organizational culture, practices and policies.** Evaluate current culture, practices and policies to eliminate outdated assumptions about older workers.
- **Examine recruitment practices.** Train recruiters and interviewers to avoid ageist assumptions. Applications should also eliminate age-related information—such as date of birth or when a person graduated—and interview panels should include people of all ages.
- **Include the topic of age in diversity and inclusion efforts.** Educate employees about ageism in the workplace. Since age discrimination often goes unreported, spreading awareness may increase the likelihood that employees who witness instances of ageism will report it.
- **Respond to claims immediately.** Handle ageism complaints swiftly and seriously.

As the workforce continues to age, business leaders should be proactive in recognizing and preventing age discrimination in the workplace. For more risk management guidance, contact us today.