MACKAY
Corporate Insurance Brokers

October 2025

COMMERCIAL
Insurance Profile

5 Workplace Safety Trends to Watch For

Keeping employees safe and minimising the risk of accidents and injuries remain top priorities for organisations across sectors. While some aspects of occupational safety remain constant, others continue to evolve. As such, it's essential for employers to stay informed about current workplace safety trends and adjust their risk management strategies accordingly. The following five trends have been influencing the occupational safety landscape recently:

1. **Bolstering safety through technology**—Employers are increasingly adopting safety technologies to reduce risk and respond to hazards more effectively. Artificial intelligence-powered wearable smart devices and sensors can detect fatigue, ergonomic issues and environmental risks in real time. Virtual reality is also being used to simulate workplace scenarios and improve training. To mitigate safety concerns, organisations should integrate these tools into their risk management strategies and consult IT professionals to ensure proper implementation.

2. **Prioritising mental health**—The rise in poor mental health among employees is impacting workplace safety, as stressed individuals may be less focused, engaged and aware of hazards, which could lead to poor decisions and increased risk. To mitigate this, employers should foster a working environment that promotes overall well-being and encourages open communication around mental health. Regular staff check-ins and dedicated well-being initiatives (eg stress management programmes and mental health days) can support this goal.

3. **Supporting remote worker safety**—Remote work has introduced new safety challenges. Employees often face heavier workloads and irregular hours, increasing the risk of eyestrain, stress and fatigue. Poor ergonomic setups (eg unsupportive chairs) can also lead to musculoskeletal issues. To mitigate these risks, employers should embed safety measures into remote work policies, offer ergonomics training and consider funding appropriate workstation equipment.

4. **Promoting safety through sustainability**—Environmental factors play a growing role in workplace safety. Environmental neglect can expose employees to long-term health risks, including respiratory and cardiovascular conditions. However, by aligning operations with current environmental standards, employers can foster a healthier workforce and strengthen their reputation. Key initiatives include adopting energy-efficient equipment, improving air and water filtration, managing waste responsibly, using sustainable personal protective equipment and offsetting carbon emissions.

5. **Building a culture of safety**—Building a strong safety culture is becoming a strategic focus for many organisations. Beyond preventing injuries, it can boost morale, enhance productivity and reinforce compliance. Employers are increasingly involving leadership in safety initiatives and encouraging staff to take an active role in identifying and addressing risks. Common approaches include regular safety meetings, visible signage, written resources and recognition for safety-minded employees.

Conclusion

As the modern workplace continues to evolve, safety is no longer limited to physical hazards. Today's safety trends extend to mental health, remote working conditions, environmental responsibility and broader operational factors. To stay resilient, organisations must remain agile and proactively adapt to these developments to build safer and more sustainable working environments.

Contact us today for further workplace safety guidance.

5 Cyber-security Mistakes and How to Avoid Them

All organisations, regardless of their size or industry, are potential targets for cyber-attacks. These events can lead to significant financial, operational and reputational damage that can be difficult or impossible to recover from. Fortunately, strong cyber-hygiene practices can reduce the likelihood of data breaches and other cyber-incidents, and many of these practices are relatively low-cost and easy to implement. Below are five common cyber-security mistakes organisations make and actionable solutions for each.

1. **Relying on weak or reused passwords**—Users often choose simple passwords they can easily remember and may reuse them across multiple devices or accounts. However, weak or repeated passwords make it easier for cyber-criminals to gain unauthorised access to devices, networks and accounts, increasing the likelihood of breaches. Employers should require strong, unique passwords and mandate that login credentials be changed regularly. Passwords should avoid common or predictable patterns (eg "password," "123456") and include a mix of upper and lowercase letters, numbers and special characters. Using a verified password manager can help employees store and generate secure credentials.

2. **Not updating software**—Delaying or neglecting software updates leaves systems vulnerable to known security flaws that cyber-attackers can exploit to gain unauthorised access. Updates and patches help close these gaps. Employers should require automatic updates on all devices and applications and regularly check for and install updates, especially for security software that protects against viruses. Staying informed about critical releases from software vendors ensures timely implementation and helps keep systems protected.

3. **Neglecting employee training**—Human error remains a leading cause of security breaches, often driven by employees being unaware of common cyber-threats like phishing. Without proper training, staff may mishandle data or unknowingly compromise systems. Employers should provide cyber-security training at onboarding and regular intervals, using interactive sessions with real-life scenarios. Encouraging open discussion and questions helps build a culture of awareness and reduces risk.

4. **Not using multifactor authentication (MFA)**—Relying on a single password for account and device security increases the risk of unauthorised access, especially if the password is weak or reused across systems. MFA adds an extra layer of protection by requiring users to verify their identity through a second method, such as a time-based code sent via text or email. Employers should enable MFA on all business accounts and devices that support it, particularly those handling sensitive data. Staff should use authentication apps or hardware tokens and regularly review MFA settings to maintain strong security.

5. **Using unsecured public Wi-Fi**—Public Wi-Fi networks can expose users to cyber-threats, including data interception and man-in-the-middle attacks. Employees should avoid accessing sensitive information on unsecured networks and only connect to trusted sources. To reduce risk, they should disable automatic connections and file sharing settings, use a virtual private network (or VPN), and ensure firewalls are enabled to block malware and other threats.

Conclusion

Cyber-attacks are a significant threat to organisations of all sizes. However, by recognising and addressing poor cyber-hygiene habits and implementing robust cyber-security measures, organisations can improve their cyber-security posture and reduce the risk of costly cyber-attacks.

Contact us today for further cyber-security guidance and cyber-insurance solutions.

Phishing remains the most common and disruptive cyber-threat, affecting 85% of UK businesses that experienced a breach this past year, according to the 2025 Cyber Security Breaches Survey. Yet many of these incidents are preventable through basic security measures and improved employee awareness.