Risk Strategy Solutions

September 2025

COMMERCIAL

Risk Advisor

Preventing Workers' Compensation Claims From Remote Work Environments

The shift to remote work during the COVID-19 pandemic led to changes in workplace dynamics, with many employees continuing to work from home either full-time or in hybrid arrangements. This evolution has introduced new occupational safety challenges, particularly in monitoring ergonomics and safe work habits outside traditional office settings. As a result, employers may face risks of employees suffering work-related injuries stemming from remote work that can lead to complex workers' compensation claims. To protect employees and reduce liability exposures, it's essential for organizations to recognize remote work's safety implications and implement proactive measures to address them.

Common Remote Work Injuries

Remote work can lead to increased workloads and irregular schedules, making employees more susceptible to eyestrain from increased screen time, stress, fatigue and burnout. Poor ergonomic setups—such as working from couches or unsupported chairs—can result in musculoskeletal issues, with many reporting new or worsened pain in their shoulders, back and wrists. Additionally, home cleanliness standards may differ from office standards, and cluttered home workspaces can create physical hazards like loose cables or rugs that can lead to slips, trips and falls. As such, common occupational injuries from remote work include:

- Back and neck sprains and strains
- Repetitive motion injuries (e.g., carpal tunnel syndrome, arthritis and tendinitis)
- Chronic headaches and vision problems
- Stress fractures and broken bones, especially those affecting the arms and legs

Strategies to Mitigate Remote Work Injuries

To help keep their employees safe and reduce exposures to workers' compensation claims, employers should develop comprehensive remote work policies that outline effective occupational safety measures. Strategies to consider include:

- Requiring employees to follow traditional work schedules (e.g., 9 a.m. to 5 p.m.) or establishing maximum daily working hours (e.g., up to eight hours per day)
- Regularly training staff on ergonomic best practices, such as maintaining proper posture, placing frequently used items nearby to avoid overreaching, alternating between sitting and standing throughout the day, rotating among different job tasks or assignments to avoid using the same muscle groups for prolonged periods, and taking scheduled breaks to stretch and move away from their screens
- Providing guidelines for appropriate workstations to improve ergonomics, including a supportive chair, a desk with sturdy legs and a flat surface, proper lighting, monitors placed at eye level, and a keyboard setup that permits relaxed shoulder and wrist positioning
- Setting clear expectations for workstation tidiness and safety by enforcing routine cleaning schedules with trash removal; providing safe equipment storage practices that reduce slip, trip and fall risks; and maintaining sufficient document organization standards

Employers should also consider allocating a percentage of their occupational safety program funding toward remote employees' workstations. In some municipalities, this may be required by law. Employers should consult legal counsel to determine their specific compliance needs.

Conclusion

Remote work can create certain occupational safety risks that can lead to injuries and associated workers' compensation claims. By understanding these remote work hazards and taking steps to address them, employers can help foster a culture of safety and prevent injuries while lowering their exposure to potential liability.

Contact us today for more risk management information.

This document is not intended to be an exhaustive source of information nor should any discussion or opinions be construed as legal advice. Readers should consult legal counsel or a licensed insurance professional for appropriate advice.

Preventing Zero-click Attacks

Zero-click attacks can be devastating for businesses. Unlike other attacks that rely on user actions (e.g., clicking links or sharing credentials), zero-click exploits bypass these steps, making them harder to detect and often more damaging. As cyberthreats grow increasingly sophisticated, these intrusions are becoming more common and pose serious risks to operational continuity and confidential information. Understanding and working to prevent these attacks is crucial for maintaining cybersecurity.

Zero-click attacks occur when hackers send specially crafted data packets that trigger malicious actions without user involvement. These attacks often target devices and systems that automatically process external content, making them dangerous and difficult to detect. Applications with messaging, video conferencing and voice calling features are especially vulnerable to infiltration due to their ability to preview content. Additionally, their use of end-to-end encryption, which hides the contents from all parties except the sender and receiver, complicates efforts to identify and intercept malicious packets. Internet of Things devices are also common targets due to their limited security and constant connectivity.

Because zero-click attacks leave minimal evidence, they can remain undetected for long periods, allowing attackers to inflict significant damage. Hackers often use advanced techniques to install and erase these exploits, which makes investigations and recovery difficult.

Impact on Businesses

Zero-click attacks can affect businesses in several ways, leading to the following ramifications:

- **Stolen funds and assets** through unauthorized access to confidential business records, private stakeholder information and intellectual property.
- **Damaged systems and technology,** as hackers compromise devices to move laterally across corporate networks, escalating their privileges and infiltrating businesses' larger IT infrastructures.
- **Regulatory and legal penalties** may result from these attacks, stemming from claims that businesses failed to protect sensitive data properly. Furthermore, businesses could face substantial regulatory penalties for breaching applicable data privacy laws.

Mitigation Strategies

There are several risk management measures businesses can implement to help lower their susceptibility to zero-click attacks and limit losses if they occur:

- **Keep software updated**. Regularly updating and patching all devices, operating systems, apps and firmware can reduce exposure to zero-click attacks. Using automatic updates and patch management tools can help streamline this process.
- **Use layered security**. Equipping systems with antivirus software, firewalls, intrusion detection and threat monitoring tools can add layers of protection. Artificial intelligence and machine learning can also help spot anomalies that may indicate a zero-click attack is occurring.
- **Segment networks and limit access**. Segmenting networks to contain breaches and enforcing strict access controls can limit hackers' infiltration capabilities, lateral movements and their ability to expand their attacks. Applying the principle of least privilege, where employees only handle systems and data necessary for their tasks, can also help reduce exposure.
- **Encourage cyber hygiene**. Training employees on zero-click threats and best practices (e.g., strong passwords, spotting and reporting unusual activity and removing unused applications) can help build a culture of cybersecurity.
- **Vet vendors and applications**. Carefully assessing third-party software—especially lesser-known providers—for security flaws before purchase can help businesses avoid introducing new vulnerabilities.
- **Create a response plan**. Developing and regularly testing incident response plans that cover various cyberattack scenarios, including zero-click exploits, can help businesses minimize damage if a cyber incident takes place.

Zero-click attacks present several risks. By taking steps to mitigate them, businesses can be better equipped to address this exposure and prevent major losses. Contact us today for more risk management information.

Zero-click attacks are a stealthy form of cybercrime where hackers exploit software vulnerabilities in devices or applications to deploy malicious code without any interaction from the user.