Provided by SCS Agency Inc

RISK ADVISOR

June 2023

COMMERCIAL

10 Essential Cybersecurity Controls

Cyber incidents—including data breaches, ransomware attacks and social engineering scams—have become increasingly prevalent, impacting organizations of all sizes and industries. As such, here are 10 essential cybersecurity controls that organizations can implement to help manage their cyber exposures:

1. **Multifactor authentication (MFA)—**While complex passwords can help deter cybercriminals, they can still be cracked. MFA can help prevent cybercriminals from gaining access to employees' accounts and using such access to launch potential attacks.
2. **Endpoint detection and response (EDR) solutions—**EDR solutions continuously monitor security-related threat information to detect and respond to ransomware and other malware.
3. **Patch management—**Patches modify operating systems and software to enhance security, fix bugs and improve performance. Created by vendors, patches address key vulnerabilities cybercriminals may target. The patch management process can be carried out by organizations' IT departments, automated patch management tools or a combination of both.
4. **Network segmentation—**Network segmentation refers to dividing larger networks into smaller segments (also called subnetworks) through the use of switches and routers, permitting organizations to better monitor and control the flow of traffic between these segments.
5. **End-of-life (EOL) software management—**EOL software has vulnerabilities that cybercriminals can easily exploit. Proactive EOL software management is necessary to prevent unwelcome surprises and maintain organizational cybersecurity.
6. **Remote desk protocol (RDP) safeguards—**To safeguard their RDP ports, organizations should keep ports turned off whenever they aren't in use, ensure they aren't left open to the internet and promote overall interface security through the use of a virtual private connection and MFA.
7. **Email authentication technology—**It's paramount that organizations utilize email authentication technology, which monitors incoming emails and determines the validity of these messages based on specific sender verification standards that organizations have in place.
8. **Secure data backups—**One of the best ways for organizations to protect sensitive information and data from cybercriminals is by conducting frequent and secure backups.
9. **Incident response planning—**Cyber incident response plans can help organizations establish protocols for detecting and containing digital threats, remaining operational and mitigating losses in a timely manner amid cyber events.
10. **Employee training—**Employees are widely considered organizations' first line of defense against cyber incidents. Training should center around helping employees properly identify and respond to common cyberthreats.

In today's evolving digital risk landscape, it's vital for organizations to take cybersecurity seriously and utilize effective measures to decrease their exposures. For more risk management guidance, contact us today.

Employee Well-being as an Enterprise Risk

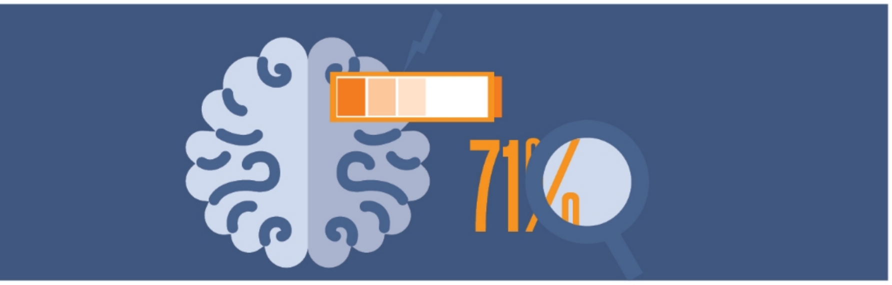
Employee well-being refers to the overall state of workers' physical, mental and emotional health, which can often be influenced by various workplace dynamics (e.g., workload, connections with co-workers and available resources). Employee mental health and well-being can impact employers in various ways, including:

- **Business performance**—According to the National Center for Biotechnology Information, mental health concerns in the workplace can contribute to increased absenteeism rates, lost productivity, decreased customer satisfaction and reduced profits.
- **Stakeholder perception**—Environmental, social and governance topics have become a rising concern among stakeholders (e.g., employees, customers and investors), making it increasingly vital for businesses to ensure environmentally and socially responsible practices—including promoting employee well-being.
- **Workplace safety**—According to the National Safety Council, instances of both moderate and severe mental health distress have been linked to a greater risk of workplace accidents.

To promote employee mental health and well-being, businesses should consider the following measures:

- **Foster a supportive workplace culture.** It's critical for employers to show their employees that they value them beyond their work contributions and are invested in their overall health and happiness.
- **Establish a long-term strategy.** Employers need to have strategic plans for promoting employee mental health and well-being, such as:
    - Conducting routine well-being awareness training and mental health screenings with all employees
    - Providing employees with a variety of well-being resources and helplines
    - Having managers conduct monthly check-ins with employees to discuss any issues that may be negatively impacting their mental health and find proper solutions
    - Educating managers on how to recognize symptoms of mental health distress and mental illness among employees, as well as how to effectively respond to a mental health crisis
    - Creating an employee assistance program to allow employees to seek additional help for mental health concerns as needed
    - Offering greater work flexibility (e.g., remote work and flexible hours) or extra paid time off to help employees maintain work-life balance

By understanding how employee well-being impacts key business objectives and making a conscious effort to keep workers happy and healthy, employers can reduce their workplace well-being exposures and maintain successful operations. For more risk management guidance, contact us today.



The Centers for Disease Control and Prevention found that **71% of U.S. adults** experience adverse symptoms of stress, such as feeling overwhelmed or anxious, each year.