I'm human

# Best practice for physical security cyber awareness

## Cyber awareness challenge 2024 best practice for physical security.  Dod cyber awareness challenge 2024 which of the following is a best practice for physical security.  Best practice for physical security cyber awareness 2024.  Best practice for physical security cyber awareness 2025.  Dod cyber awareness which of the following is a best practice for physical security.  Cyber awareness challenge best practice for physical security.  Cyber awareness challenge 2025 which of the following is a best practice for physical security.

While physical security is often overlooked, Chief Information Security Officers (CISOs) play a vital role in enterprise physical security strategies. They are responsible for protecting people, property, and physical assets from harm, which can trigger cyber incidents and breaches. As IT systems become increasingly interconnected with physical security systems, CISOs must ensure these systems are hardened to prevent vulnerabilities. Physical access to IT assets is a critical concern, and CISOs must work with facilities teams and other stakeholders to implement measures that protect access. Effective communication and coordination between CISOs and physical security experts are essential for achieving business continuity, disaster recovery, and facilities design goals. This includes securing physical access, network and data center assets, power, and fire prevention, as well as monitoring cameras and surveillance images to ensure compliance with regulations. Ensuring control over physical access to sensitive systems is crucial for CISOs, particularly in data centers, IT facilities, and computer rooms within office spaces. To achieve this, they should limit access to only necessary personnel and enforce strict guidelines for contractors working in these areas, including logging and reviewing access daily. According to David Ortiz, the approach to security measures should be tailored based on risk levels of each facility. "Facilities that house critical information should have tighter controls than those with less sensitive assets," Justin Fier advises, emphasizing the importance of understanding data and resource storage locations within facilities, assessing potential risks if breached, and hardening physical protections accordingly. Even in seemingly low-risk office settings, an attacker might find a foothold into the corporate network through any available network jack. A CISO should be heavily involved in designing a comprehensive physical security architecture that includes defense-in-depth measures to prevent unauthorized access to IT environments. Remote and hybrid work may have changed how people perceive offices but still requires adequate controls for physical security, such as port security, wireless access point security, badge access controls, and camera surveillance. Moreover, CISOs should consider the ease with which an attacker can move laterally across physical spaces and through restricted zones, ensuring that proper measures are in place to prevent initial access leading to continued unauthorized presence. As Alethe Denis notes, once an adversary gains initial access to a building or restricted area, they might go undetected unless specific security protocols are implemented. The goal is to achieve integrated control over physical and cyber elements, including OT environments, IoT devices, and surveillance systems, with ready access to critical data for investigation purposes. This comprehensive approach ensures that all aspects of an organization's facilities and operations are safeguarded against potential threats. Assets across a network should have varying levels of security as individuals move through different physical areas within buildings. Access restrictions should become more stringent as one approaches sensitive rooms or areas. Ideally, this would be achieved through measures such as badge access for stairwells and elevators, controlled elevator floor selection buttons, and observant employees who prevent tailgating. This approach limits lateral movement and potential damage by an attacker beyond a public lobby or delivery area. Physical security oversight by CISOs shouldn't be limited to facilities owned by the organization. They should also consider how they'll protect assets in co-located facilities or data centers. For such locations, individual racks need to be secured and controllable through badge readers or other means. Data centers should have cameras, guards, and other controls to ensure security. Even when physical handling of systems is abstracted away from the organization, as in public cloud or SaaS resources, CISOs still need to consider how the systems that house them are physically controlled. This includes understanding the importance of contracts and service level agreements, and the value of third-party audit attestation. CISOs working with organizations that manage critical infrastructure must also consider how cyber activity could adversely impact physical environments. Cyberattacks in industrial settings can pose a significant threat to physical safety by infiltrating devices and disrupting critical infrastructure like water treatment plants or power grids. The convergence of IT and OT environments means CISOs must be mindful of physical-cyber connections in their facilities, even if they aren't operating in an industrial business. Unauthorized access to industrial machinery can cause malfunctions that seriously injure workers. Basic physical plant assets could be controlled or managed remotely, posing potential threats. IoT devices are also critical for consideration. They often expose sensitive areas and can control or monitor various systems. Preventing IoT devices from being used as entry points into an IT environment requires unique defense measures due to their widespread presence in non-secure areas. Modern CISOs face a broad range of physical security challenges that go beyond securing traditional facilities. Their role extends to managing the physical security implications of both OT and IoT systems within their organizations' ecosystems, reflecting the increasing importance of holistic cybersecurity strategies that account for all levels of interaction between the physical and cyber worlds. The Internet of Things (IoT) has expanded into the physical realm, bridging information and action. However, this also makes IoT systems an attractive target for physical attacks, as noted by Taylor of Radware. Control over various devices such as cars, boats, airplanes, factories, elevators, etc., requires internal monitoring capabilities to detect malicious actions like unauthorized software changes or virus infections. In the event that someone destroys the IoT device with a baseball bat, having a disaster recovery plan in place is crucial. The traditional 'edge' of the network has changed, and the Chief Information Security Officer (CISO) must consider threat models and control measures specific to their business context and acceptable risk levels. This involves working closely with supply chain partners to ensure hardware integrity and educating employees on physical, personal, and operational security best practices. The post-pandemic realities of remote work have amplified concerns over distributed devices. CISOs must expand their scope of physical security oversight to include remote devices. Securing physical IT assets has become a growing challenge for CISOs due to the popularity of remote and hybrid work, making device loss, misuse, or theft more likely. CISOs should also address the issue of securing at-home devices, such as routers, which are increasingly targeted by threat actors, as seen in campaigns like Volt Typhoon. Hardened devices sent to priority target individuals like C-suite executives and privileged administrators may be a necessary measure. Facilities teams handle day-to-day administration of physical access control and building protection, but CISOs should ideally collaborate with them to understand the risk posture of each facility's entry points. This includes knowing if entry is monitored by a reception area, has badged access, or uses closed-circuit TV (CCTV) for recording. CISOs should offer input into designing these access controls and finding ways to integrate them into logical access as well. Coordination can aid investigations and smooth offboarding of employees, ensuring physical and logical access controls work together when credentials are lost or an employee is terminated. While monitoring surveillance systems may fall outside the CISO's purview, they often have a vested interest in designing and hardening these systems to protect their domain expertise. CISOs must play a key role in video surveillance management due to varying privacy concerns, regulatory responsibilities, and sensitivities that come with it. They should collaborate closely with legal teams to ensure compliance with laws and regulations around video surveillance, which can vary by region. Modern video surveillance is also part of the IT environment, making these systems another cyber-attack surface for CISOs to worry about. CISOs need input into the architecture of these systems as they are often connected to the main corporate network, leaving them vulnerable to being watched by other users or threat actors. Camera footage can help bridge the gap between physical and logical systems in incident response. However, budgetary constraints and clear ownership of responsibility often limit CISOs' ability to address these physical security considerations. To gain credibility and esteem, CISOs should take a common sense, budget-smart approach when making recommendations, working closely with the CSO and/or facilities team to coordinate responsibilities and avoid stepping on each other's toes. A balanced list of goals and desired physical security controls can help determine the best path forward. Physical security is often overlooked but can be breached with little technical knowledge. It encompasses protection from various threats, including fire, flood, natural disasters, burglary, theft, vandalism, and terrorism. Best practices include knowing your device's serial number and MAC address to aid in recovery if it's lost or stolen, and encrypting your device to protect sensitive information. Windows 10 and macOS device encryption can protect your files. Regular backups are also recommended to keep important data intact. You can track your iPhone through Apple's Find My iPhone, or use the Android Device Manager for Android devices. These services provide GPS location tracking, lock options, and wiping capabilities. Using Administrator accounts on computers is not secure, as they allow malicious software to install. Instead, use non-privileged accounts for daily activities and only switch to Administrator when necessary. Setting a password on your devices helps keep data safe. Locking your screen before leaving it unattended also protects your device.