LAYER 8 SECURITY
THE HUMAN FACTOR

Physical Cyber Security Audit

Physical cyber security focus on the strategy, application, and preservation of countermeasures that can defend the physical resources of an organisation.

The primary threats to physical security include possible acts of human failure or error, inadvertent acts, deliberate acts of espionage or trespass, impacting the security of an organisation.

Physical and subsequent, human cyber security is often a second thought when it comes to information security.

Hacking into network systems is not the only way that sensitive information can be stolen or used against an organisation. Physical cyber security must be implemented correctly to prevent attackers from gaining physical access and take what they want. All the firewalls, cryptography and other security measures would be useless if that were to occur. The challenges of implementing physical security are much more problematic now than in previous decades.

Laptops, USB drives, tablets, flash drives and smartphones all can store sensitive data that can be lost or stolen. Organisations have the daunting task of trying to safeguard data, equipment, people, facilities, systems, and company assets. The organisation could face civil or criminal penalties for negligence for not using proper security controls.

The objective of physical security is to safeguard personnel, information, equipment, IT infrastructure, facilities, and all other organisational assets. The strategies used to protect the organisation's assets need to have a layered approach. It is harder for an attacker to reach their objective when multiple layers must be bypassed to access a resource.

A deliberate act of espionage could include a competitor entering an organisation with a camera or a disgruntled employee physically stealing sensitive data for malicious intent. It could also include software attacks, acts of theft, vandalism, sabotage, information extortion, and compromise of intellectual property.

The outcome of the physical cyber security audit encompasses the identified risks and mitigation strategies to reduce the overall physical cyber security risk incorporating the following four facets:

- Identification and classification of your assets and resources (what to protect)
- Identification of plausible threats (who to protect it from)
- Identification of plausible vulnerabilities (the likelihood)
- Identification of the expected impact if bad things happen (the consequences)

The spreadsheet on the following pages shows the program contents.

The contents encompass the Service Purpose, Activity, Outcome and Measurement for the following categories of the audit:

- Policies and Procedures
- Destruction and Management
- Workplace
- Verbal activities
- Secure Storage
- Tailgating access management
- Contractor management
- Accounts and Password management
- Device management.

If you would like further information / clarification, or if you would like us to provide a proposal for the aforementioned work, please contact us at:

Web: https://layer8security.com.au
Web: https://cyberescaperoom.com.au
Email: information@layer8security.com.au
Phone 1300 706 536

Service code	Service Purpose	Service Activity	Service Outcome	Service Measurement
L8S - Destruction	**Confidential electronic media & document management, disposal,** and destruction	Is there a confidential document management procedure? Number of employees who properly follow data disposal destruction procedures. Digital devices that are disposed of (donated, thrown out, resold) containing sensitive data. Proper wiping procedures. Identify any rubbish bins or dumpsters for any sensitive documents that were not shredded.	Identifying the issues pertaining to staff and their management of confidential document will assist in alleviating the threats associated with inappropriate management and destruction of classified information.	How many staff, and what type of documentation is unsecured.
L8S - Workplace	**Workplace / desk** security Walk through - identify security breaches, unattended devices, etc.	Nightly work through. Desk Analysis. Unlocked devices and screens. Passwords viewable Photocopier containing documents Unsecure bins containing documents USB drives left lying around Whiteboard & other presentation media uncleaned Doors and windows left unsecured Desks secured	To identify the staff responsible and educate them of proper procedures.	Identify if the workplace is secure, drawers locked, devices secured, etc. The type / classification of data is also measured to see the potential threat / loss the organisation would incur.
L8S - Verbal	Identify any **conversations** that can be overheard in unsecured locations	Monitoring of verbal communications and conversations via eaves dropping in public places, lunchrooms etc.	To identify the staff that verbally may compromise security with their verbal communication in non-secure locations.	How many staff undertake verbal communications in unsecured locations?
L8S - Secure Storage	Secure **Storage** of devices, documents, and trash	To identify if the staff are disposing of confidential devices and paperwork in a manner that is suitable to its classification, Secure and manage server rooms, communications room(number of access doors to such rooms, windows, locks, fireproof, etc) Secure storage and protecting of Network infrastructure, including controlling physical access to network devices,	To reduce the impact / risk of incorrect practices associated with storage of devices and documents	Identify the staff, departments that are not following procedures

Service code	Service Purpose	Service Activity	Service Outcome	Service Measurement
L8S- Tailgating	Physical - **tailgating**, unaccompanied access, security pass usage, visitor, and contractor access management	Physical security analysis to identify weaknesses in staff behaviour and attitude. Secure access passes loss or theft of passes	Security team does a walkthrough of organisational facilities by tailgating, checking each work environment/department to ensure that individuals are following organizational security policy	Level of access and threat level is determined using a risk matrix scale
L8S - Contractor	**Contractor Scamming** to identify staff susceptibility to be scammed by people pretending to be a contractor trying to gain access into the building	Staff, masquerading as contractors, delivery drivers, maintenance people, will attempt to enter the organisation utilising standard social engineering techniques	To identify any staff that are not vigilant with regards to social engineering attacks	attempts vs success and the amount of information collected
L8S - Password Audit	Identify if **passwords** have been compromised and are currently being sold on the Dark Web as well as identify written down passwords that are stored insecurely	Security team does an analysis of compromised passwords for specified domain that are available on the dark web as well as a walkthrough of organizational facilities, checking each work environment and looking to ensure that individuals are following organizational policy	Identify the staff who have troubles with their passwords and must write them down.	Number of staff locations with passwords or confidential information written on Postit Notes or pieces of paper left on the desk

Service code	Service Purpose	Service Activity	Service Outcome	Service Measurement
L8S - Policies & Procedures	**Policies and procedures** cover the protection of physical assets, (both electronic, paper based and human), adequately address an organisation's physical cyber security risk. This encompasses physical security policies and procedures of use, management, monitoring, human behaviour, for facilities and systems, ICT equipment, media, and physical paper-based information as well as the ability of external threats to access facilities.	**Policies and Procedures -** encompassing: Policies & management of Clean Desk Acceptable use policy Management & Destruction Policy BYOD management & Policy Management of Shadow IT Management of lost document, device policy and history Security vetting of contractors Visitor & contractor access Policies Cleaners security vetting Monitoring of Exfiltration of data and Documents Monitoring of People accessing facilities & systems Physical access to buildings & other facilities Secure conversation policy Data Centre, Network & communications security & Secure containers External observation ICT device and access management External user device management & policy Register of equipment taken in and out of the organisation	The outcome of this component, in conjunction with the other components, it to identify any holes or issues within the policies and procedures, as well as the way staff, contractors and visitors address these policies.	To ensure the controls, policies and procedures are correctly established and that staff can follow these.
L8S - Device security	To identify the staff who leave **devices** unsecured allowing for easy theft of device and information	The ability for someone to watch staff enter secure data, Identifying if devices are left logged in when person is away, Are there any suspicious devices left lying around, Are devices correctly password / MFA protected, IOT accessibility and security Walk through parking lots and secure parking to identify devices left within cars	To identify and educate staff as to what they should do to protect their devices and the contained corporate data	Measure the number of devices, who they belong to, the potential data / threat of this data.