Privacy threat prevention through security controls

A Privacy threat means any threat or connected series of threats to unlawfully use or publicly disclose private information. - <https://www.lawinsider.com/dictionary/privacy-threat>

Security controls: a safeguard or countermeasure prescribed for an information system or an organisation designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements. -<https://csrc.nist.gov/glossary/term/security_control>

Therefore privacy threat prevention through security controls is using security controls to prevent private information from being leaked and publicly released or using the information to blackmail organisations.

There are three types of security controls: physical, administrative and technical. These are categories for specific security measures put in place to prevent access to private information.

Physical security controls:

Physical security controls consist of guards, cameras, fences and alarm systems. These are stop people from physically breaking into the facility and stealing or damaging information. These means of security however only protect from physical interactions which are less likely compared to other attacks. – information from <https://www.cbtnuggets.com/blog/certifications/security/top-7-physical-security-controls> Matt McClure 02/02/2021

Administrative security controls:

These controls are more about ensuring your employees don’t leak information by accident or on purpose. Policies are used to ensure data is protected and to also limit who can access certain information. A list of policies would be: Password policies ensure passwords are used, changed and are complex; Access control policies limit access to certain resources, usually employees only have access to resources necessary for their role; Data collection policies include where information can be stored and to also make sure it is encrypted; device usage policies outline what can be done on company owned devices like laptops and mobile phones. Training can also be used to make sure employees don’t get tricked by phishing or social engineering attacks. – information from <https://firewalltimes.com/administrative-security-controls/> Catherine Reed 15/09/2021

Technical security controls:

Technical security controls are used to prevent any breach via technical means. The usual technical controls are: encryption, firewalls, anti-virus software and data backups. Encryption protects information by converting it into ciphertext which then requires a key to decipher so it is hidden if an intruder manages to access it. Firewalls monitor incoming and outgoing network traffic. When a packet enters the firewall, it is inspected, if it breaches the firewall’s rules it is prevented from entering. Anti-virus software scans the device or any downloaded files for viruses and other malware. Data backups are a corrective security control, if any data is lost to physical or technical issues then a backup is always available so a minimal amount of data is lost. – information from <https://firewalltimes.com/technical-security-controls/> Michael X. Heiligenstein 14/10/2021