Intusive application practices :

Summary: unauthorized access to work information via a malicious or privacy-intrusive application

Place mock enterprise contacts on devices, then attempt to install and use unmanaged applications that access and back up those entries.

(https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-22.pdf) 59-60

Account credential theft through phishing:

credential phishing is specific kind of phishing cyberattacks that is aimed at getting users to share their credentials (typically passwords or usernames) so that the attacker can steal and use them to gain unauthorized access to email accounts, business system

https://www.rsa.com/fr/resources/blog/passwordless/credential-phishing-what-it-is-and-how-to-prevent-it/

Outdated phones:

malware successfully exploits a code execution vulnerability in the mobile os or device drivers, the delivered code generally executes with elevated priviliges and issues commands in the context of the root user or the OS kernel

sensitive data transmissions

Data transmission is the process of sending digital or analog data from one device to another

this process is key to how the internet works and how information moves across network

users and product developers need to be confident that whenever sensitive data is in transit, it is protected against eavesdropping and tampering

it could be a physical (wired) connection across a network, a wireless or bluetooth connection between devices or a broadcast radio frequency transmission

the mechanism used should protect both communiations over public (untrusted) networks and ithin private (trusted networks)

https://www.yomu.ai/blog/data-transmission-security-2025-guide

https://www.ncsc.gov.uk/collection/technology-assurance/principles-product-design-and-functionality/3-protect-sensitive-data-in-transit

Brute-force attacks to unlock a phone:

a brute force attack is a hacking method that uses trial and error to crack passwords, login credentials and enryption keys reliable tactic for gaining unauthorized acces to individual accounts and organizations systems and networks

hacker tries multiple usernames and passwords often using a computer to test a wide range of combinations

https://www.fortinet.com/uk/resources/cyberglossary/brute-force-attack

Application credential storage vulnerabily

Credential managment secures and cotrols access the digital credentials like password, API keys, and cryptography certificates

without effective credential system companies risk unauthorized access

Unmanaged device protection

Unmanaged devices are network-connected devices that lack active monitoring, management, or control by IT or security teams.

They are often personal devices or third-party devices that employees or contractors use, which fall outside of the organization’s standard management and security policies.

These devices can pose significant security risks due to lack of visibility and control.

https://www.venn.com/learn/unmanaged-devices/

Lost or stolen data protection

Lost or stolen mobile devices gives an adversary unhindered access to the device, and if there’s an insecure or no PIN in place, access to the data on the device as well.

https://pages.nist.gov/mobile-threat-catalogue/physical-threats/PHY-0.html

Protecting enterprise data from being inadverently backed up to a cloud service

enterprise data protection refers to the strategies, processes, tools, and methodologies to safeguard an organization's data from breaches, theft, or loss.

This involves many tasks, including data encryption, backup, tokenization, and business continuity planning.

https://www.digitalguardian.com/blog/guide-enterprise-data-protection-best-practices