Cyber threats, in plain terms.

A cyber threat is anything that could deliberately harm your systems or data. Most real-world attacks come from a small set of types: phishing and social engineering, malware and ransomware, credential attacks and account takeover, privilege escalation and lateral movement, data exfiltration and destruction, and insider threats. They rarely act alone; a typical breach chains several together.

HOW IT WORKS

01 Phishing and social engineering

Social engineering means manipulating a person into doing something unsafe, and phishing is its most common form: a message that impersonates someone you trust to steal a password or trigger an action. The variants matter:

- Spear phishing targets a specific person with details that make it convincing.
- Whaling goes after executives, whose access and authority are worth more.
- Business email compromise (BEC) skips the malware and simply asks, as your CEO or a supplier, to change bank details or wire money. It is consistently one of the costliest attacks for businesses of every size.
- Spoofing is the enabler: forging a sender address, a domain, or a caller ID so the message looks legitimate.

Phishing is the single most common way attacks begin, because it targets people rather than patched software. The defenses are multi-factor authentication (so a stolen password is not enough), email authentication (SPF, DKIM, and DMARC to stop domain spoofing), training, and a rule that any request to move money is confirmed on a second channel.

02 Malware and ransomware

Malware is any software written to do harm: viruses, worms, trojans (malware disguised as something useful), spyware, and more. It usually arrives through a phishing attachment, a malicious download, or an unpatched, internet-facing system.

SOURCES

[1] Cyber Threats and Advisories

[2] Computer Security Resource Center Glossary

[3] MITRE ATT&CK

[4] Data Breach Investigations Report

Ransomware is the variant that has reshaped the threat landscape. It encrypts your files and demands payment for the key, and modern operators also steal a copy first so they can threaten to publish it, known as double extortion. For most organisations, ransomware is less a mystery of exotic exploits and more a failure of the basics: an unpatched service, a phished credential, no multi-factor authentication, and backups that were never tested.

The defenses are patching, endpoint protection that can detect and stop malicious behaviour, least-privilege access so one infected machine cannot reach everything, and tested, offline-capable backups.

03 Credential attacks and account takeover

Attackers would rather log in than break in. Credential attacks turn passwords into access:

- Password cracking takes stolen password hashes offline and guesses them at scale.
- Credential stuffing replays username-and-password pairs leaked from other breaches, betting that people reuse them.
- Brute forcing simply tries many passwords against a login.

The result is account takeover: the attacker holds a valid account, which raises none of the alarms that malware does. This is why multi-factor authentication is the highest-value control most organisations can turn on, and why unique passwords in a password manager matter. Phishing-resistant methods such as hardware keys or passkeys close the gap that one-time codes leave open.

04 Privilege escalation and lateral movement

A first foothold is rarely the goal. Privilege escalation is how an attacker turns a limited account into an administrator, by abusing a misconfiguration, an unpatched flaw, or excessive permissions nobody reviewed. Lateral movement is how they spread from that first machine to the systems that actually hold value.

Most damaging breaches are a chain: a phished credential, then privilege escalation, then lateral

movement to the data. The defenses are least privilege (so a compromised account can reach very little), network segmentation (so movement is slow and noisy), and monitoring that notices the movement while it is happening. This is also what a penetration test exercises: not whether one door is locked, but whether an attacker who gets through it can reach anything that matters.

05 Data exfiltration, leaks, and destruction

These are the outcomes attackers are usually after:

- Data exfiltration is the deliberate theft of data, copied out to systems the attacker controls, often slowly to avoid notice.
- Data leaks are the accidental cousin: a public cloud bucket, an over-shared file, a database left exposed to the internet. No attacker skill required, and just as damaging.
- Data destruction is data deleted or encrypted to cause harm or cover tracks, as ransomware and some insider attacks do.

The defenses are knowing where your sensitive data lives, least-privilege access to it, encryption, watching the paths data leaves by (data-loss prevention), and backups you have actually tested restoring.

06 Insider threats

Not every threat comes from outside. An insider threat is a current or former employee, contractor, or partner who misuses legitimate access, whether maliciously (stealing data on the way out, sabotage) or negligently (falling for phishing, mishandling data, misconfiguring a system). Negligent insiders cause far more incidents than malicious ones.

Insiders are hard precisely because their access is supposed to be there. The defenses are least privilege and regular access reviews, prompt offboarding when someone leaves, logging and monitoring of sensitive actions, and a culture where reporting a mistake early is safe rather than punished.

See which of these threats actually reach your data.

securelayer7.net/learn/threats/types-of-cyber-threats

Open online