

7 STAGES of a successful cyberattack ...and how to stay ahead of attackers

To combat cyberattacks, you need to understand attackers' steps—from *their* perspective. IBM® X-Force® Incident Response and Intelligence Services (X-Force IRIS) researchers have developed a framework to capture all the steps attackers take to penetrate your network.



STEP 1 SETTING SIGHTS ON THE GOAL

Attackers identify a target and create an initial attack plan. Targets may be selected:

- For immediate financial gain
- To obtain valuable intellectual property
- For ideological reasons

STEP 2 PREPARATIONS BEGIN

Attackers prepare their offensive by:

- Conducting external reconnaissance
- Aligning tactics and techniques to the target
- Preparing attack tools
- Establishing an attack infrastructure

▶ [Listen to the podcast.](#)



STEP 3 LAUNCHING THE ATTACK

Attackers attempt to compromise at least one host on the target network via:

- End-user desktop
- Phone, tablet or IoT device with access to the network
- Server or mainframe at the core of the infrastructure

Covering their tracks

Attackers may try to achieve operational security by disguising their preparations.



STEP 4 DETERMINING THE OUTCOME

The attackers take stock, by:

- Evaluating attack success
- Refining mission objectives

▶ [Read the blog post.](#)



If attack fails...

Return to Step 1 and reassess the requirements needed for a successful attack.



STEP 5 ACCESSING YOUR ENVIRONMENT

The attackers enter your infrastructure by:

- Executing an initial compromise
- Establishing a foothold



STEP 6 EXPANDING ACCESS

Attackers expand the scope of their incursion with:

- Privilege escalation
- Lateral movement
- Internal reconnaissance
- Persistent presence

Evading detection

Whenever attackers are inside your network, they're trying to hide their presence with log deletion and other tactics.

▶ [Read the white paper.](#)



STEP 7 DECLARING A WIN

After compromising the network, the attackers move toward their goal, such as:

- Data theft
- Destruction or disruption of business operations

Stay steps ahead of attackers

The X-Force IRIS Cyberattack Framework moves beyond traditional attack frameworks, helping you anticipate attackers' every move.

▶ [Read the ebook.](#)

▶ [Visit the X-Force IRIS website.](#)