# Likelihood

## Capability

An actor's sophistication, tools, and resources to execute a cyber attack determine their capability. Assessing capability as an independent variable of likelihood means organizations can avoid the pitfalls of devoting time and attention to "paper tiger" threats.

### Attack Methods

Humans are creatures of habit. Although threat actors take great care to avoid detection, at some level they too succumb to this adage. Tracking how threat actors operate exposes patterns that analysts can use to combat their effectiveness.

#### Infrastructure

Sophisticated threats often require an infrastructure to operate. This can be assessed by looking for hop points used during an attack, the command and control network, or the size and scope of a botnet.

#### Technology

Technology used or manipulated for an attack can indicate the capability of a threat actor. More sophisticated actors target SCADA or ICS devices, web-enabled products, or mobile devices in addition to traditional servers and clients.

#### Coding

Nuances and personal preferences in coding not only assist with attribution, but also can indicate actor sophistication.

#### Maturity

The maturity of the actor takes into account their planning process, pre-attack activities (research/recon/social engineering), and post attack actions (such as tool updates or incorporating lessons learned).

#### Targets

Capability can be assessed by looking at what is targeted. Does the actor rely on mass phishing emails, identify specific targets (network, website, employee, mobile platform) or exploit a specific vulnerability (Adobe, Windows, SQL, etc.)?

### Resources

Understanding what is available to threat actors offers context to the sophistication of their attacks. Leverage government, industry, and intelligence service provider information sharing arrangements to learn about actors resources.

#### Money

Obtaining and maintaining capabilities incur costs. Well-resourced/sponsored threat actors are often more dangerous than less resourced actors, with other variables being equal.

#### People

From collaborators and co-workers to teachers and mentors, the number and type of people involved in a campaign can be indicative of its capability.

#### Tools

Tools often hint at the capability of an actor, but the lack of a custom tool does not always imply a novice attacker. Most sophisticated actors will use the right tool for the job; if open source tools will work, there is no need to customize one.

#### Training

The type and quality of training available to the threat actor can help determine their capability. Online videos, IRC channels, certification courses, military training, or formal academic education all yield different levels of sophistication.

## Intent

The actor's purpose and the expected outcome of the cyber attack determine the intent. Prioritizing actors by their intent allows analysts to focus on the most relevant threats.

### Motive

Why do threat actors attack? Determining an actor's motive provides insight into the possible direction of their behavior, and determines their interest in targeting the organization.

#### Intrinsic (personally rewarding)

Fame, bragging rights, thirst for knowledge/access, justification of skills, satisfying boredom, patriotism, and hactivist allegiance; all reasons a hacker might be motivated to target an organization.

#### Extrinsic (receive external reward or avoid punishment)

Extrinsic motives revolve around two key concepts: reward or avoiding punishment. These motives include everything from state-sponsored denial and deception operations, misinformation campaigns, and psychological operations to financial incentives from competing businesses, organized crime, and blackmail.

### Targeted Data

Understanding what a threat actor is after will factor into determining their intent to target the organization.

#### Personally Identifiable Information (PII)

Are the attackers stealing personal information from your customers? From your employees? Determining if this type of information is vulnerable can help assess the likelihood that the actor targets the organization.

#### Research and Development

Some actors exist to steal corporate R&D data. Organizations with heavy R&D missions are more likely to be targeted by actors specializing in corporate espionage or supporting nation-states.

#### Business Process

Certain categories of actors, especially insider threats, target the inner workings of the organization. From hiring and firing information to time cards and audit findings, organizations likely will be targeted if this information is accessible.

#### Industrial Control Systems

Certain actors specialize in compromising industrial control systems and the associated human-machine interface. Organizations operating these systems should prioritize these threat actors accordingly.