Cyber threats generally have one thing in common; at some point a human interacts with the threat. This interaction must be a part of threat prioritization to understand an attacker’s most commonly targeted vulnerability: people.

**Cyber Footprint**
The greater an organization’s online exposure, the more opportunity an attacker has to find vulnerabilities. Consider the organization’s infrastructure, supply chain, online exposure, and components most susceptible to attacks.

**Relevance**
From leadership to rank-and-file employees, the Internet offers a communication platform that allows anyone to make their organization more visible to threat actors.

**Access**
Employees with administrator privileges or access to sensitive data are more attractive targets for threat actors. Determining who has what access can significantly aid in identifying the risk to employees.

**Infrastructure**
The unknown provenance of software and hardware complicates risk determination in the cyber environment. Overcoming this limitation requires researching where, when, and how an organization’s infrastructure is most susceptible to cyber threats.

**Online Presence**
The content and services an organization provides on the Internet serve as attractive targets for threat actors. Analysts can assess severity of risk based on this insight into likely attack vectors.

**Website**
Analyze how threat actors might leverage an organization’s website to plan and execute an attack. This includes compromising customer account log-ins, collecting employee contact information, defacing the site, or denying legitimate access to it.

**Extracurricular Activities**
Be mindful of the activities employees participate in outside of work. Employees’ status with external institutions, such as non-profits, may increase their risk of being targeted.

**Motivation**
There always is a rhyme or reason for why people enable cyber attacks. Whether it’s ignorance, financial trouble, disgruntlement, or boredom, by knowing these vulnerabilities analysts can diminish their effectiveness through prevention.

**Physical and Network-Based Access**
Individuals have varying access to both physical and network-based sections of an organization that threat actors can leverage to execute an attack. Assess which employees are at higher risk of being targeted based on their access.

**Position**
As with access points, consider how threat actors can exploit the different roles people play throughout the organization, from network administrator or HR representative to CEO, supply chain manager, or a recently fired employee.

**Supply Chain**
The most stringent network defenses can be subverted by counterfeit equipment or software. Understanding and assessing threats to the organization’s supply chain provides additional data points to measure risk of compromise through the organization’s network infrastructure.

**Hardware**
Develop a blueprint of where network appliances, workstations, and third party equipment connect to the organization’s network and identify the most likely risks for cyber threat activities.

**Software**
Most organizations rely on software to accomplish day-to-day operations. A robust threat prioritization assesses the risks associated with relying on particular software, which network users require access to high-risk software, and the organization’s ability to detect if a software vulnerability has been exploited.

**Website**
Analyze how threat actors might leverage an organization’s website to plan and execute an attack. This includes compromising customer account log-ins, collecting employee contact information, defacing the site, or denying legitimate access to it.

**Additional Exposure**
An organization’s public relations and marketing departments track how social media and other aspects of the Internet help bring attention to the organization. Threat prioritization efforts also should track how this attention affects its cyber threat environment.

**Additional Services**
FTP, Telnet, VPN access, webmail, remote desktop, and other web-based services used by an organization increase the risk of potential cyber attacks, and should be factored into threat prioritization.