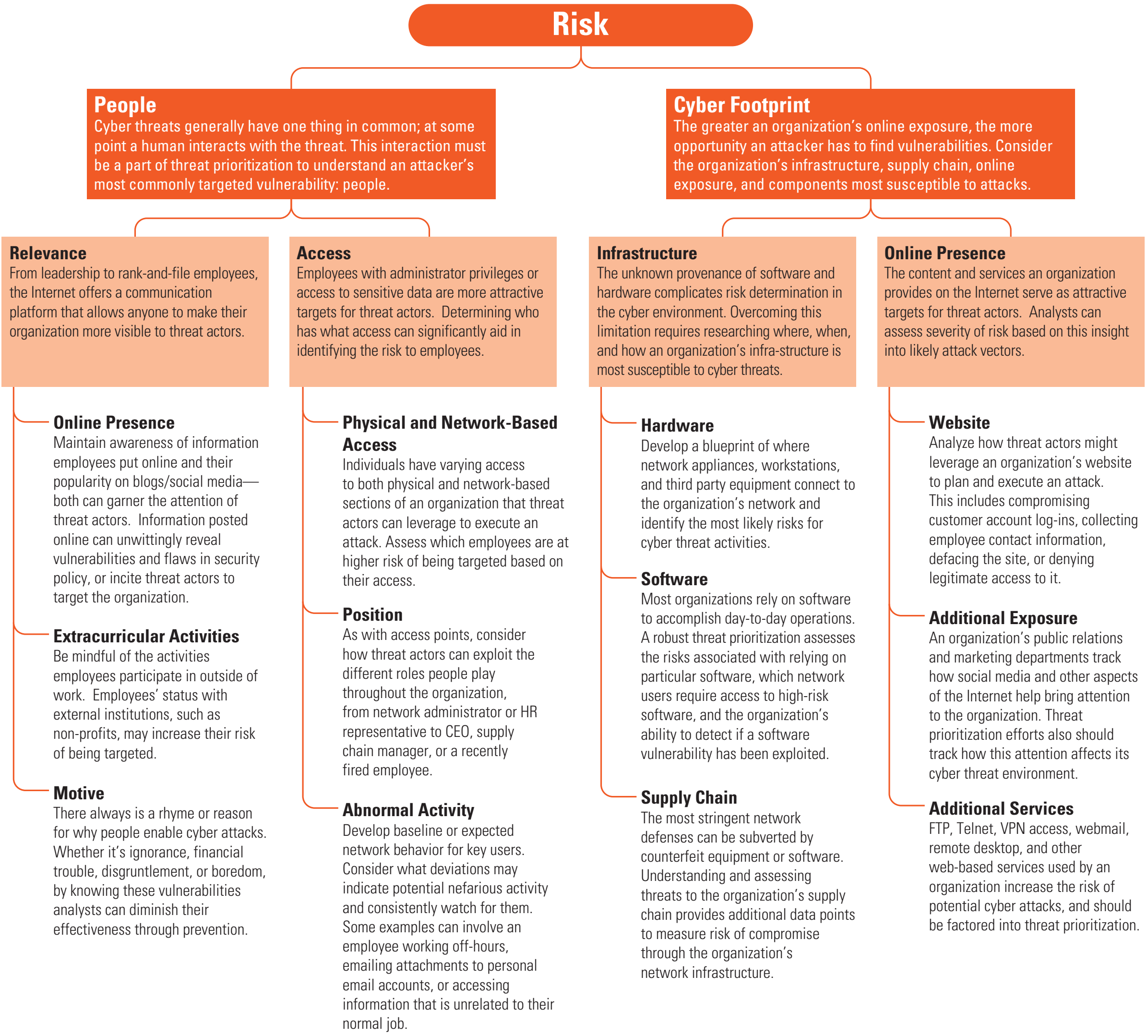
Risk

Assessing how people and the organization’s cyber footprint make the organization vulnerable to cyber attacks determines what areas within it are the most at risk of being targeted. One CITP participant’s CEO is active with companies and institutes that are separate from the organization. The CITP participant’s cyber intelligence analysts maintain an awareness of these activities, so when hacktivists publicly threatened attacks against one of the institutes, the analysts knew this could have implications for their organization and altered network defenses to prepare for a potential attack.



Risk

People
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.

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.

Online Presence
Maintain awareness of information employees put online and their popularity on blogs/social media—both can garner the attention of threat actors. Information posted online can unwittingly reveal vulnerabilities and flaws in security policy, or incite threat actors to target the organization.

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.

Motive
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.

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.

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.

Abnormal Activity
Develop baseline or expected network behavior for key users. Consider what deviations may indicate potential nefarious activity and consistently watch for them. Some examples can involve an employee working off-hours, emailing attachments to personal email accounts, or accessing information that is unrelated to their normal job.

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.

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 infra-structure is most susceptible to cyber threats.

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.

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.

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.

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.

Indicators of Success

- Whether it is an employee alerting about a suspicious email they received or a vendor providing a list of bad IPs, analysts have engaged enough with individuals associated with the organization that they actively contact the analysts about issues that could alter how threats are prioritized.
- Employee feedback influences threat prioritization because analysts offer feedback mechanisms via all of their cyber intelligence communication platforms; emails, analytical products, briefings, or awareness campaigns.
- If the CEO or a junior analyst blogs about topics that likely will bring the attention of threat actors, analysts are aware of these activities and consider the position, influence, popularity, and online presence of these individuals in order to predict how they should change the organization’s security posture.
- Analysts become aware of the fact that every vulnerability is not a threat worthy of further analysis and mitigation.
- Analysts understand the organization’s operating environment well enough that with system updates and patches, they alleviate ~80% of threats; freeing them to focus on the ~20% that could significantly impact the organization.
- Analysts recognize their organization is only as secure as its supply chain. If it acquires software and analysts don’t know who did the actual coding, the code’s reliability, or to what extent it has been error tested, then they won’t know how threat actors could use potential vulnerabilities within the code to conduct an attack.
- Analysts incorporate timing into their prioritization efforts to align increases in network defenses with the different times during the year (holidays, system upgrades) when the organization’s network is most vulnerable.