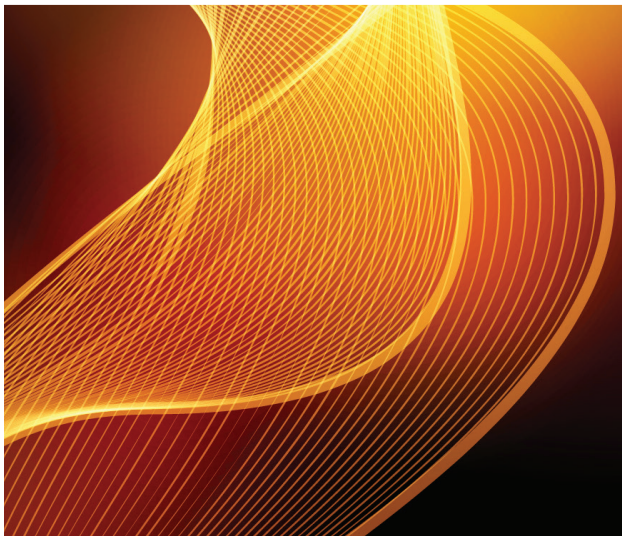


Implementation Framework – Cyber Threat Prioritization

Troy Townsend
Jay McAllister

September 2013

This material is based upon work funded and supported by ODNI under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM-0000620

Implementation Framework – Cyber Threat Prioritization

Background

The Software Engineering Institute (SEI) Emerging Technology Center at Carnegie Mellon University studied the state of cyber intelligence across government, industry, and academia to advance the analytical capabilities of organizations by using best practices to implement solutions for shared challenges. The study, known as the Cyber Intelligence Tradecraft Project (CITP), defined cyber intelligence as the acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities to offer courses of action that enhance decision making.

A significant challenge that emerged from the CITP was the way in which analysts prioritize cyber threats. The SEI team observed a diverse array of approaches, from analysts relying on the media and third-party intelligence service providers to using data-centric models based on a narrow scope of factors.

When threat prioritization models are too narrow, they prevent analysts from effectively monitoring the changes and evolution of the most relevant and severe cyber threats. This hinders cyber intelligence and security professionals from proactively implementing defenses to guard against the latest attack trends and techniques. Among the CITP's government participants, most intelligence analysts prioritized cyber threats by the likelihood of an actor executing an attack, which they quantified through the summation of an actor's sophistication (capability) measured against their desire to target the organization (intent). The SEI team noted that as these analysts transitioned to the private sector, so too did this approach. Conversely, private sector CITP participants without experienced government intelligence analysts tended to discount the utility of knowing the threat actor and prioritized cyber threats by the impact attack methods had on the organization or the risk attack methods posed because of the organization's known vulnerabilities.

This Cyber Threat Prioritization Implementation Framework leverages the best practices of CITP participants and SEI expertise to offer a holistic approach to prioritizing cyber threats using a customized, tiered threat prioritization framework. The framework breaks down cyber threats into three core components: the likelihood of threat actors executing attacks, the impact threats have on an organization's business, and the risk threats pose because of an organization's known vulnerabilities. By assessing threats according to these components, analysts come to fully understand the causes and effects of relevant threats, which significantly improves the efficiency of their organization's cyber intelligence efforts because they have the necessary context to accurately align analytical and security resources to the current and future cyber attacks posing the most legitimate threats to the organization. Instead of prioritizing a cyber threat solely on the capability and intent of threats actors, the framework enables analysts to see the utility of also understanding the threat's relevance to their organization, strengthening their threat prioritization as they come to realize that a somewhat capable actor with a desire to deface websites should not be considered in the same category as a highly capable actor intent on extracting confidential, strategic documents for extortion or blackmail.

Implementation

Here's how analysts can leverage the Cyber Threat Prioritization Implementation Framework to augment their organization's cyber intelligence efforts:

1. Adopt these definitions:

   Threat = Likelihood + Impact + Risk

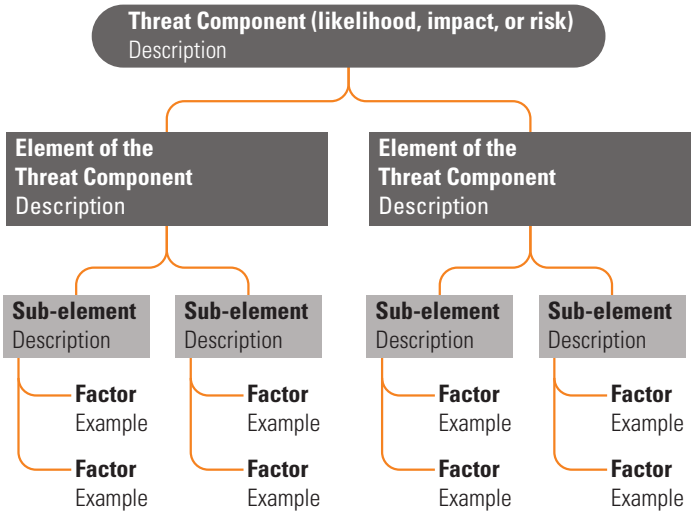
   Likelihood = Capability + Intent

   Impact = Operations + Strategic Interests

   Risk = People + Cyber Footprint

2. Become familiar with the provided spider graphs to gauge the factors that comprise each of the three threat components.

   Spider graph key: Title of threat component
   Description and example from a CITP participant



Indicators of Success
Examples of how assessing threats according to this element and its sub-elements and factors augments an analyst's cyber intelligence capabilities.

3. Identify cyber threats using the three core components of a threat.

   Examples: Likelihood: Threat actors - State-sponsored, competitors, criminals, hactivists, recreational hackers

   Impact: Attack types - distributed denial-of-service (DDoS), stealing intellectual property (IP), damaging/ incapacitating network assets

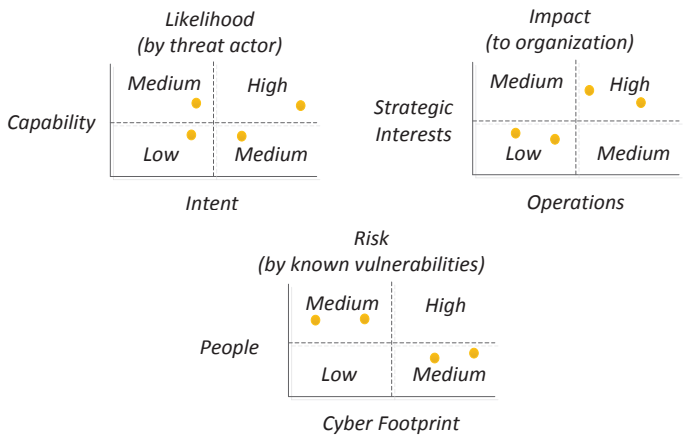
   Risk: Known vulnerabilities - High-profile employees, unpatched devices, unsecured remote access

4. Assess the likelihood, impact, and risk of the cyber threats. Use the factors and sub-elements in each threat component's spider graph to rate the corresponding elements as a low, medium, or high priority attribute of the threat. The average of these ratings then determines the likelihood, impact, and risk of the threat, which combine to indicate whether it should be considered a low, medium, or high priority threat.

   Example: An organization wants to know how it should prioritize its analytical and network defense efforts for a possible recreational hacker DDoS attack on the organization's secure payment site. Analysis indicates the likelihood of the recreational hacker executing the attack is high due to his attack methods and resources. However, the impact of the DDoS attack is assessed as low because the secure payment site has minimal impact on the organization's operations and strategic interests due to it still being in internal beta testing. This also means the risk associated with the attack is low because of the secure payment site's limited interaction with people and cyber footprint. Therefore, this threat, which initially appeared to be a high priority, now can be classified as a medium to low threat requiring minimal analytical and network defense attention.

Note: Always factor timing into the threat prioritization assessment. When a threat actor or organization does something can be just as important as why or how. A threat actor may have no desire to target an organization, but since it is a national holiday, the organization becomes a target of opportunity for the actor to test a new tool simply because none of its network security employees are at work.

5. Plot all threats for each component on graphs similar to the following:



Use all three graphs to holistically evaluate the overall cyber threat environment to efficiently align analytical and security resources to the current and future cyber attacks that pose the most legitimate threats to the organization.

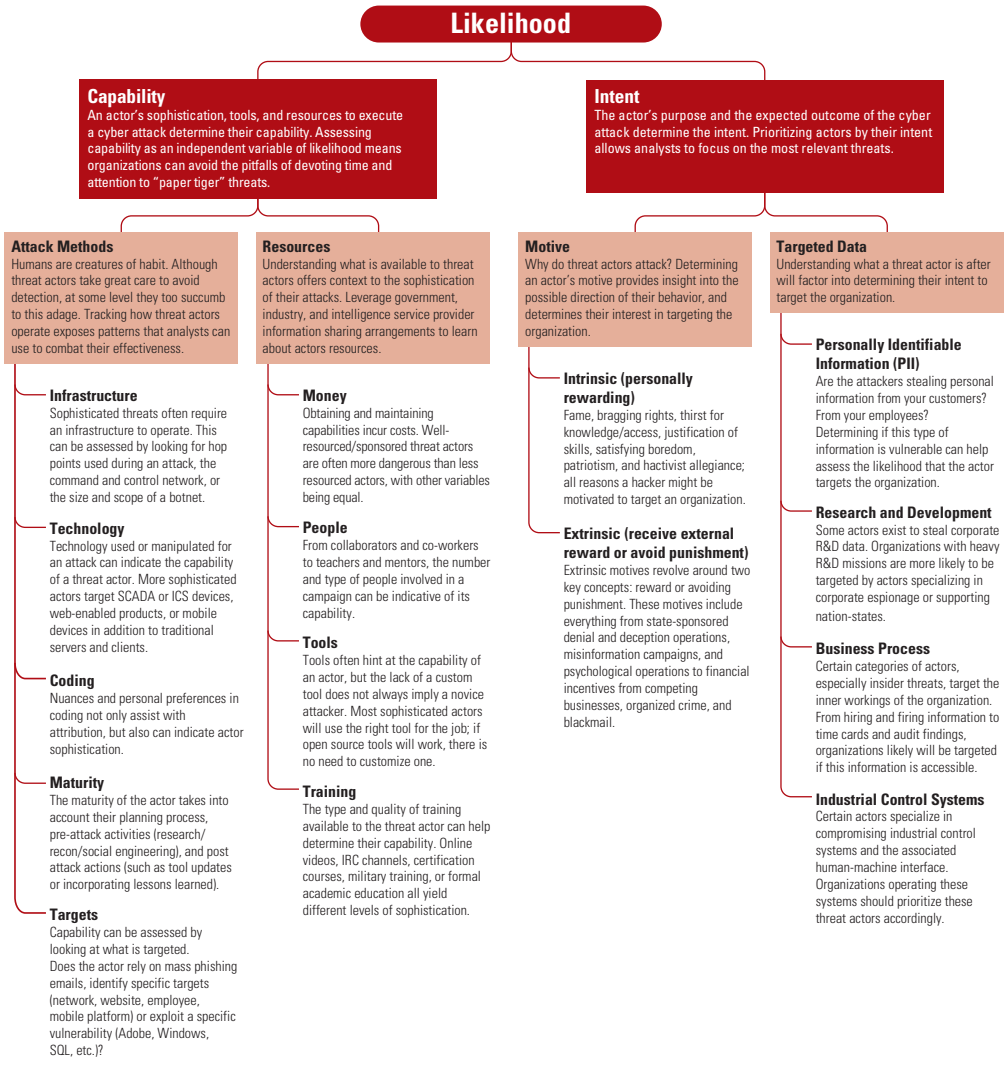
Example: If cyber intelligence analysts rate all components of a threat actor executing a worm (likelihood) against an organization's network servers for industrial espionage purposes (impact) that has no worm mitigation in place (risk) as a high priority threat, then the organization should immediately position itself to focus on this threat over others where the likelihood is equally as high, but impact and risk are lower.

Overall Indicators of Success

- Threat prioritization influences which potential threats get addressed by security operations and how network security resources are allocated.
- Collection management is streamlined and organizations are able to better communicate their requirements to third party intelligence vendors.
- Cyber threats are widely communicated to the organization and employees are aware of the most relevant threats.
- Cyber threats are proactively monitored and prioritized, with updates available to inform security operations, intelligence analysts, and decision makers.
- Analytical production aligns with threat prioritization. For instance, the organization develops a tiered system to communicate threat information to stakeholders:
    - Tier 1: Potential threat averages a high rating. Analysis required within 90 minutes.
    - Tier 2: Potential threat averages a medium rating. Analysis required within 8 hours.
    - Tier 3: Potential threat averages a low rating. Analysis required between 3 and 5 days.
    - Tier 4: Potential threat does not compute a rating, but is an indirect threat for anyone using the Internet. No specific timeframe for analysis.
- Analysts use threat prioritization to do predictive analysis, like developing scenarios to test how defenses will react to the full spectrum of cyber threats.

Likelihood

Understanding the capabilities and intentions of cyber threat actors determines the likelihood of them targeting an organization. To determine this likelihood, a CITP participant from industry monitored open source publications from an organization known to sponsor cyber threat actors who frequently targeted the organization. Analyzing this accessible data provided insight into the motivations of the sponsored cyber threat actors, allowing the CITP participant to narrow down the types of data likely to be targeted, and work with network security experts to create diversions, honey pots, and employ other measures to proactively defend against the threat.

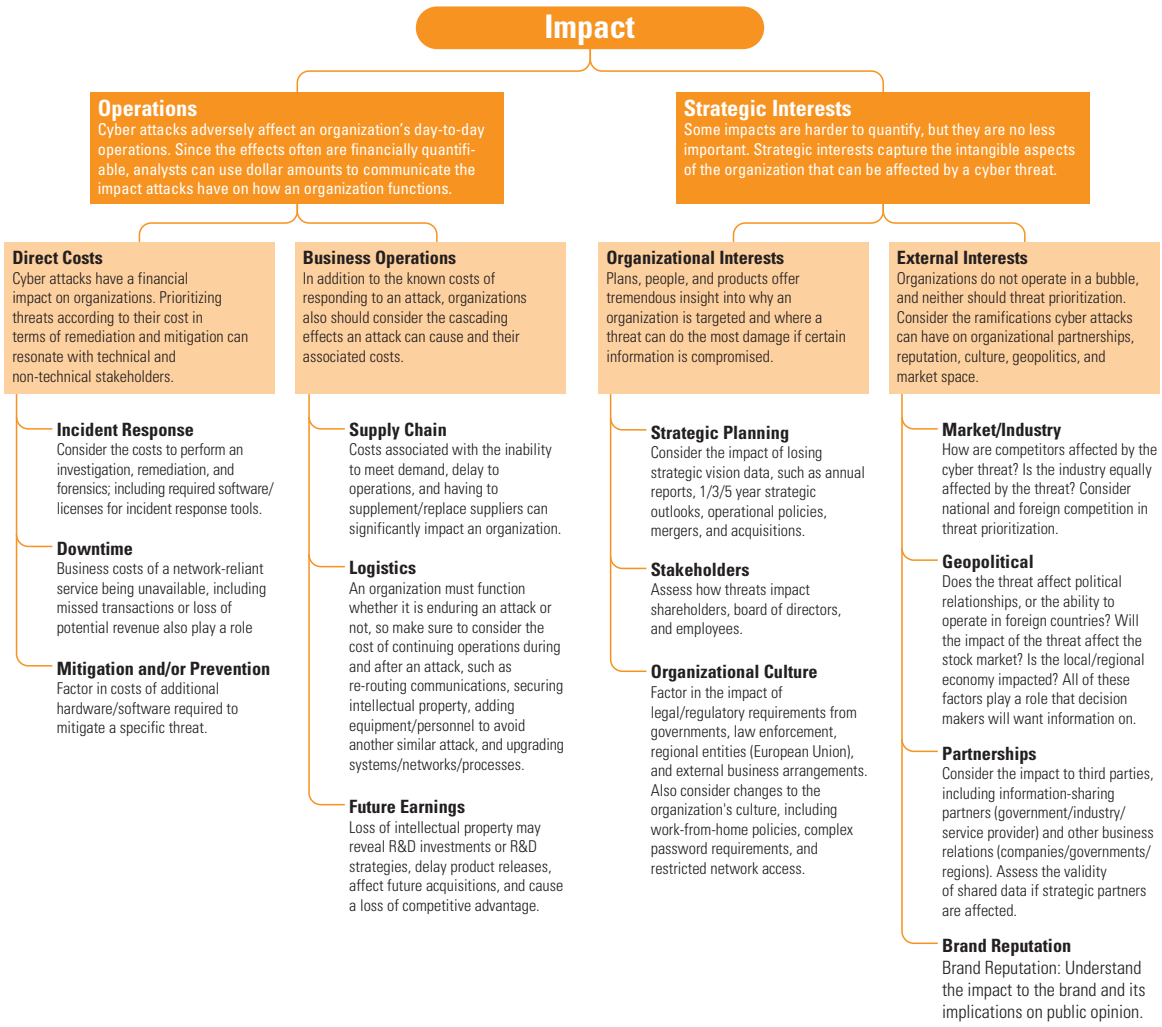


Indicators of Success

- Analysts have a repository of current and historical threat actor tactics, techniques, and procedures (TTPs) to generate profiles that are fed into data collection platforms to separate known threats that automated defensive actions can mitigate from unknown threats requiring an analyst's attention.
- Analysts gain perspective on the tools threat actors use to assess how they access an organization or if they outsource tool development. A basic netflow analysis could show the majority of attacks come from well known, prepackaged scripts, which analysts can easily combat using remediation efforts posted on open source websites.
- Analysts realize that sophisticated actors use the lowest common denominator for attacks. If a threat actor can use an off-the-shelf tool to accomplish their goal, they'll wait to deploy customized tools on harder targets.
- Analysts understand that the targeting of Adobe or Windows software vulnerabilities usually equates to a threat of lower sophistication than one targeting Windows operating systems.
- Analysts understand threat actors' intentions well enough to assign them to different categories, such as nation-state, criminal, hactivist, recreational, or competitor; enabling them to identify the most likely threats their organization faces through profiling.
- Analysts realize that if a threat actor is targeting their organization for fame, the likelihood increases for the actor to choose a DDoS attack to the organization's website as the attack method.
- From their organization being the first result in a Google search to knowing over what holidays certain actors like to conduct attacks, analysts recognize the importance of timing when it comes to assessing the overall likelihood of a threat.

Impact

Analyzing the effects cyber attacks have on an organization's operations and strategic interests provides quantifiable, business-related information to justify its impact on the organization. A CITP participant quantified the impact of cyber threats to their leadership by assessing how much money the organization would pay to reroute its product distribution channels after a hacker compromised the network and disclosed specific travel routes to competitors intent on disrupting this distribution.

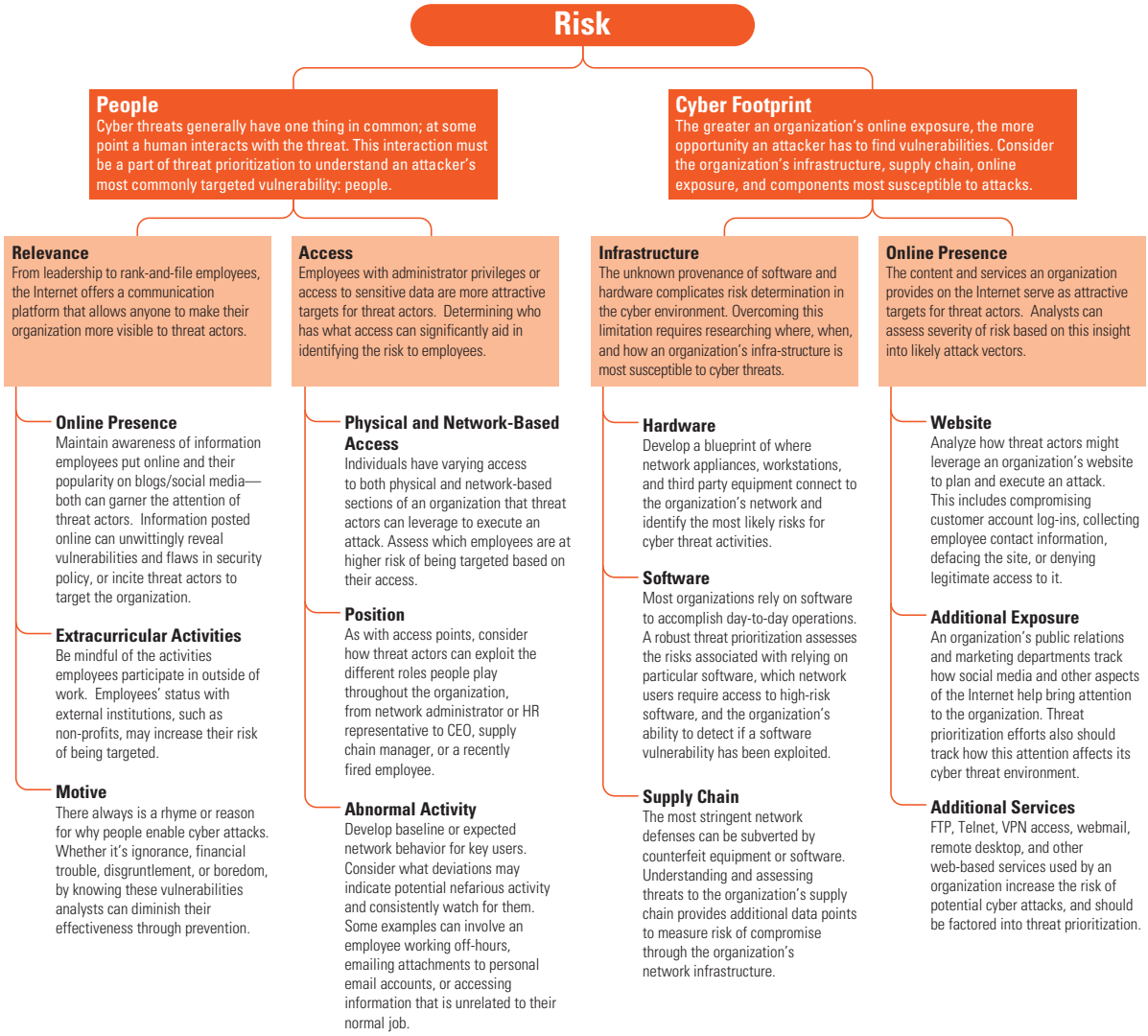


Indicators of Success

- Internally, analysts establish frequent communication with the business units responsible for operations to discuss threats, alter threat prioritization, and predict new threats. These business units can include R&D, physical security, risk management, IT, human resources, insider threat, and business intelligence.
- Analysts identify and remediate the cascading effects a cyber attack could have by targeting one part of the organization's operational network and systems.
- Analysts recognize how a cyber attack could impact the organization's ability to operate and communicate to stakeholders and institute appropriate contingencies to eliminate this impact when an attack occurs in the future.
- Knowledge of the impact cyber attacks can have on an organization's operations enables analysts to determine the financial costs to recover and repair damage done by the threats that the analysts' prioritization efforts deem most likely to harm the organization.
- Analysts ensure that threat prioritization isn't based off personal biases or those of decision makers, stakeholders, service providers, or the media.
- Analysts correlate logs of IPs accessing the parts of their organization's website containing data on strategic planning and intellectual property with known bad IPs to predict where threats will be concentrated now and in the future.
- Analysts understand the financial cost associated with a geopolitical event in a country threatening their organization's Internet presence in that market.
- Analysts recognize that if peers in their industry and the organization's economic interests are being attacked, the likelihood of being targeted increases and they take preventative measures to ensure that doesn't happen.

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.



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.