Through a Lens Darkly Keynote: Handout

SYNERCOMM IT Summit – September 2025

Actors have differing goals, targets & TTPs. Who you’re up against will shape your risk & priorities.

Dimension	Hacktivists	Cybercriminals	Nation-State Actors
Primary Motivation	Ideological, political & social causes	Financial gain	Geopolitical advantage, espionage, sabotage
Target Selection	Symbolic (gov’s, firms, industries)	Opportunistic	Strategically valuable
Sophistication	Low-to-moderate; free hacker tools	Varies but moderate to high	High to untraceable
Common TTPs	Defacements, DDoS, leaks, doxxing	Phish, ransomware, cred theft, BEC	0-days, moles, LolBins, supply-chain
Resourcing	Un-/Self-funded	Profit-supported	State-backed, agency level funding
Organization	Volunteers, amateur collectives	Structured, professional businesses	Hierarchical, government-sponsored
Consequences	Embarrassment, reputational harm	Financial/operational loss, fines	NatSec risk, IP theft, kinetic conflict
Fear Factor	Aggravation, Embarrassment, $	Reputation loss, ops disruption, $$	Existential threat to firms, industries $$$
Examples	Anonymous, OpWallSt	Colonial Pipeline, Equifax, Target	SolarWinds, Stuxnet

A framework for how to look at your public estate from both points of view

The Question I Ask	What It Tells Me (Assuming the role of Attacker)	Why I Care (As the defender assessing risk)
Who am "I" in this scenario?	My goals, motivations, and therefore likely targets	Can inform my view of adversary sophistication, likely TTPs, Initial Access vectors and point to likely at-risk systems & data
What kind of asset is it?	Does the tech match either my targets of interest and/or my skills, toolset and knowledge, aka "Should/can I hit this?"	Everyone has finite resources, and work must be prioritized; my potential attacker may bias toward certain systems; use that intel & stack rank risk remediation work
Where do I think it's located?	Geography, ISP, physical owner etc. may influence my interest level, e.g. familiarity with security controls, insider access, DAB offers, likelihood of prosecution etc.	Security maturity almost always varies by location (by cloud, by data center, by country, facility or office) etc. Risk ranking drives intelligent prioritization
How important might it be?	Whatever says "more important" – naming conventions, login access, payment-related or core to customer journeys – says "worth more to ransom, hurts more if I break it."	Prioritizing importance to the business is obvious; What's not is whether *your* view of the importance aligns to what the attacker can observe and the likely conclusions THEY draw
How valuable is the stuff inside?	This is not quite the same as above; Importance to the victim is one axis of importance; market/sale value of data is another, and is distinct	Once again, attacker profile is key here; ATPs and hacktivists may be content to break things; criminals want to monetize; NOT the same priorities
What observable controls protect it?	The more layers of defense I can observe, the faster I will pivot to lower LOE options	My most valuable assets may be well-layered and protected; less hardened targets may be down my list, but high on the attackers; this leads to misaligned prioritization