Attack Economics and Attack Categories

Attack Economics

- Attack campaign on a predefined set of **targets**:
  - `Gain ≈ Takings - AttackCost`
- We want an estimate for:
  - **Human-operated** attacks vs **Automated** attacks
- **Very** simplified and intuitive treatment…yet very useful

Takings Estimate

- Assumption:
  - **Failed** attack on a target: **zero** taking
  - **Successful** attack on a target: always **the same** taking

- `Takings ≈ TakingPerTarget * #targets * ProbSuccess`

- Linear in `#targets`
- Slope `TakingPerTarget * ProbSuccess`

Attack Cost Estimate: Human-operated

- Assumption:
  - Initial cost **independent** from `#targets`
    - Reconnaissance + Resource Development
    - How you execute the attack and collect takings
  - **Additional** cost for each target
  - **Same** additional cost

- **`AttackCost ≈ FixedCost + CostPerTarget * #targets`**

- Linear in **`#targets`**
- Slope **`CostPerTarget`**

Gain Estimate: Human-operated

- **Takings** ≈ **TakingPerTarget** * ProbSuccess * **#targets**
- **AttackCost** ≈ **FixedCost** + **CostPerTarget** * **#targets**

- Attractive **only** when (≈ ≈):
  TakingPerTarget * ProbSuccess > > **CostPerTarget**

- "The **target** must be worth the effort"

Attack Cost Estimate: Automated (I)

- Assumption:
  - Initial cost **independent** from `#targets`
    - Reconnaissance + Resource Development
    - How you execute the attack and collect takings
  - ~~**Additional** cost for each target~~
  - ~~**Same** additional cost~~

- Counterintuitive fact:
  - For many automated attacks, **additional** costs are **negligible** (!)
  - Attacking 100 targets costs like attacking 10000 targets

Example: Phishing

- Assumption:
  - Initial cost **independent** from `#targets`
    - Reconnaissance + Resource Development
    - How you execute the attack and collect takings
  - At this point, sending 1000 or 10000 or 100000 emails has roughly the same cost

Example: Large-scale Injection

- Assumption:
  - Initial cost **independent** from `#targets`
    - Reconnaissance + Resource Development
    - How you execute the attack and collect takings
  - At this point, contacting 1000 or 10000 or 100000 IP addresses has roughly the same cost
    - Predominant cost is developing exploit

Attack Cost Estimate: Automated (II)

- Assumption:
  - Initial cost **independent** from `#targets`
    - Reconnaissance + Resource Development
    - How you execute the attack and collect takings
  - ~~**Additional** cost for each target~~
  - ~~**Same** additional cost~~
- **`AttackCost`** ≈ **`FixedCost`** ~~`+ CostPerTarget * #targets`~~
- **Independent** from **`#targets`**

Gain Estimate: Automated

- `Takings ≈ TakingPerTarget * ProbSuccess * #targets`
- **`AttackCost ≈ FixedCost`**

- Attractive when (≈ ≈):
  `TakingPerTarget` `* ProbSuccess *` **`#targets`** `> >` **`FixedCost`**

they may be **small**!
(because **`#targets`** may be very large)

Low-value targets (I)

- **Human-operated**:

`TakingPerTarget * ProbSuccess > > CostPerTarget`

Attacking a target of little value
is **not** rational

- **Automated**:

`TakingPerTarget * ProbSuccess * #targets > > FixedCost`

Attacking a target of little value
may be rational!

Low-value targets (II)

- **Human-operated**: Attacking a target of little value is **not** rational
- **Automated**: Attacking a target of little value **may be rational!**
- This considerations explains why:
  - Single-users are almost always affected by **automated** attacks
  - Phishing is still a huge problem

Automated: EXTREMELY FREQUENT

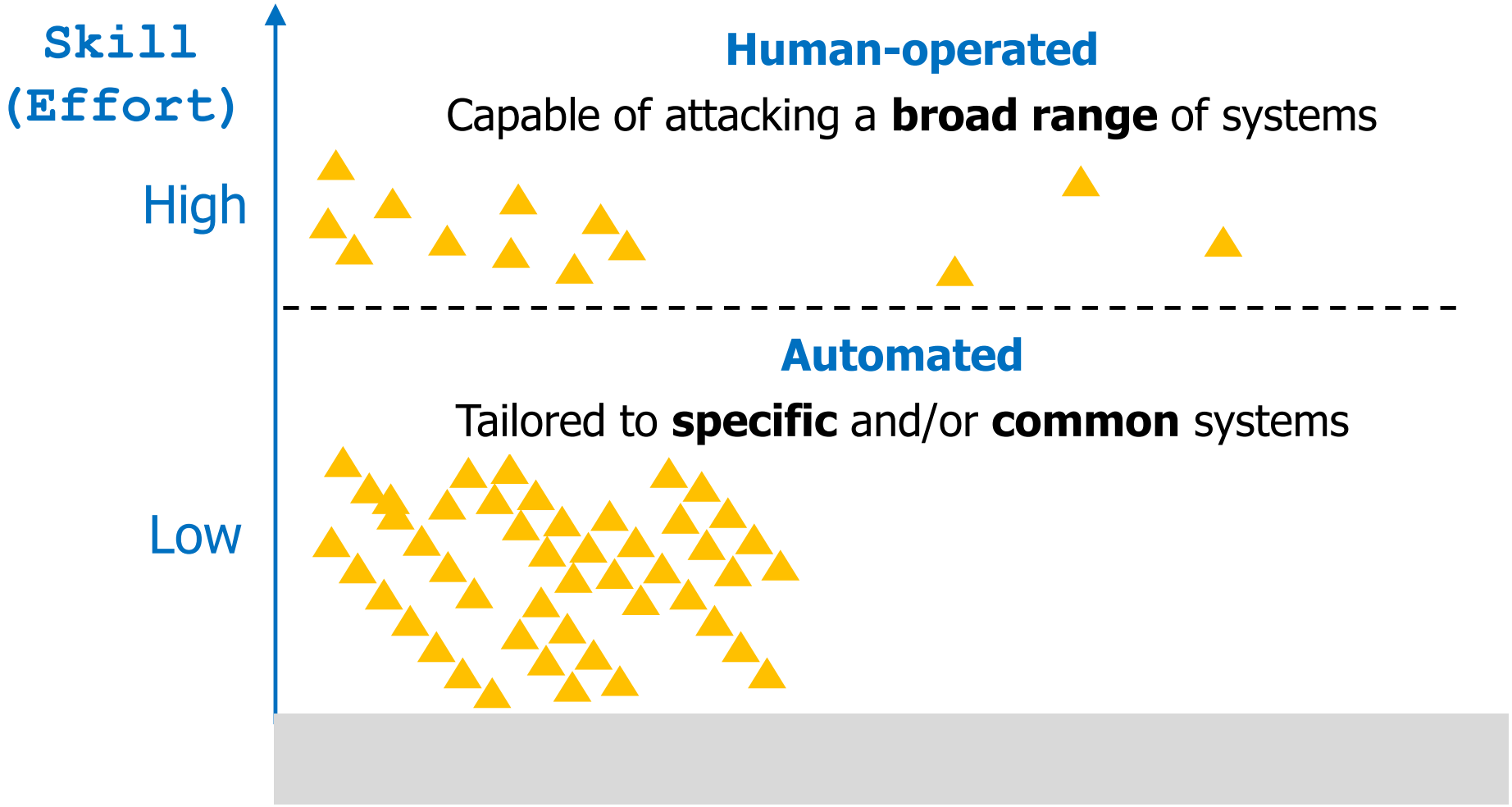
- `TakingPerTarget * ProbSuccess * #targets`
- `FixedCost`

- One **fixed** and **known** investment
- **A lot** of taking opportunities (**linear** in the number of **free attempts**)

- **Fantastic economic opportunity!**

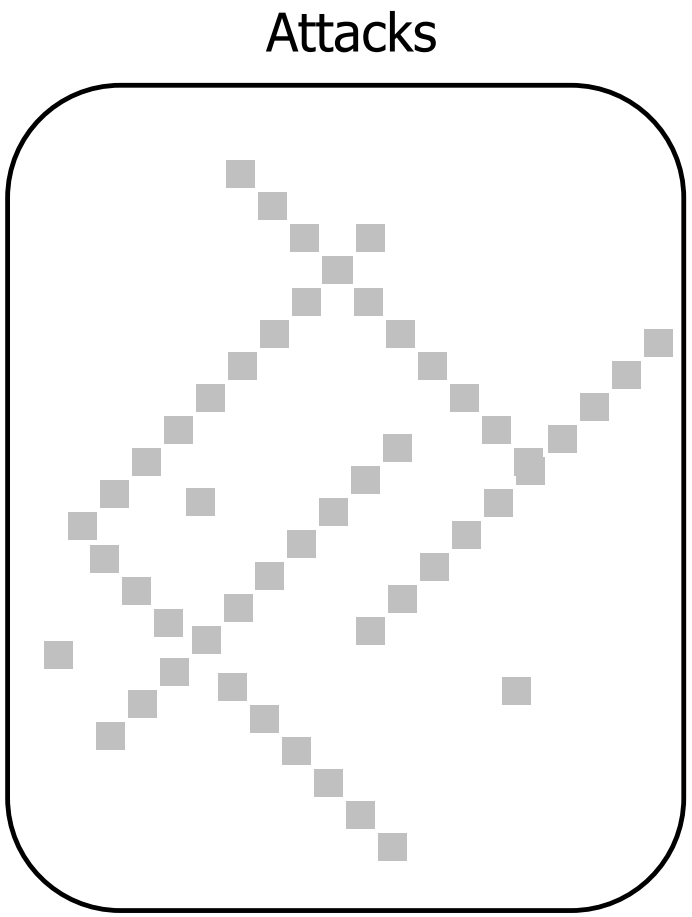
- One can make even a small bet
- **Extremely frequent**

Attack Categories: Skills (Effort)



Attack Categories

Attack Categories



- **Many** possible **categorizations**
- We will see a **very useful categorization** in 4 classes (Steve Bellovin)

- Then, we will reason about:
  - **How many** in each category?
  - Which category is **more relevant** for a **defender**?

Personal Consideration

- Seemingly trivial topic
- **HUGE** impact on my understanding of cybersecurity

Financially-motivated Attackers

Real Scenario: Attacker point of view

- **Plentiful** of targets
- **Many** of them have **bad** defenses
  (success requires moderate attack effort)

- While attacking **a certain target**, you do **not** know:
  - Whether you will **succeed** in your attack
  - What **investment** you will need for that target

Financially-motivated Attackers

- Interested **only** in **money**
- Clearly, a **very large** population of attackers

- Money is all that matters⇒
  - **Not** "fixated" on any specific target
  - **All** targets are **equivalent**

Keep in mind 1

- **Not** "fixated" on any specific target
- **All** targets are **equivalent**

- This is by far the **most common** attacker mindset

Key Question

- You are a financially-motivated attacker
- You are attacking a certain target
  - Your early attack steps are costly
  - Prevention and Detection appears "not bad"

- What is the **most rational** behavior?
  1. Invest more and more effort on this target
  2. Change target

Rational behavior

- What is the most rational behavior?
  1. Invest more and more effort on this target
  2. Change target

- Most rational behavior: **change target!**

- In a large population of attackers, the **prevalent** behavior is certainly the most rational one

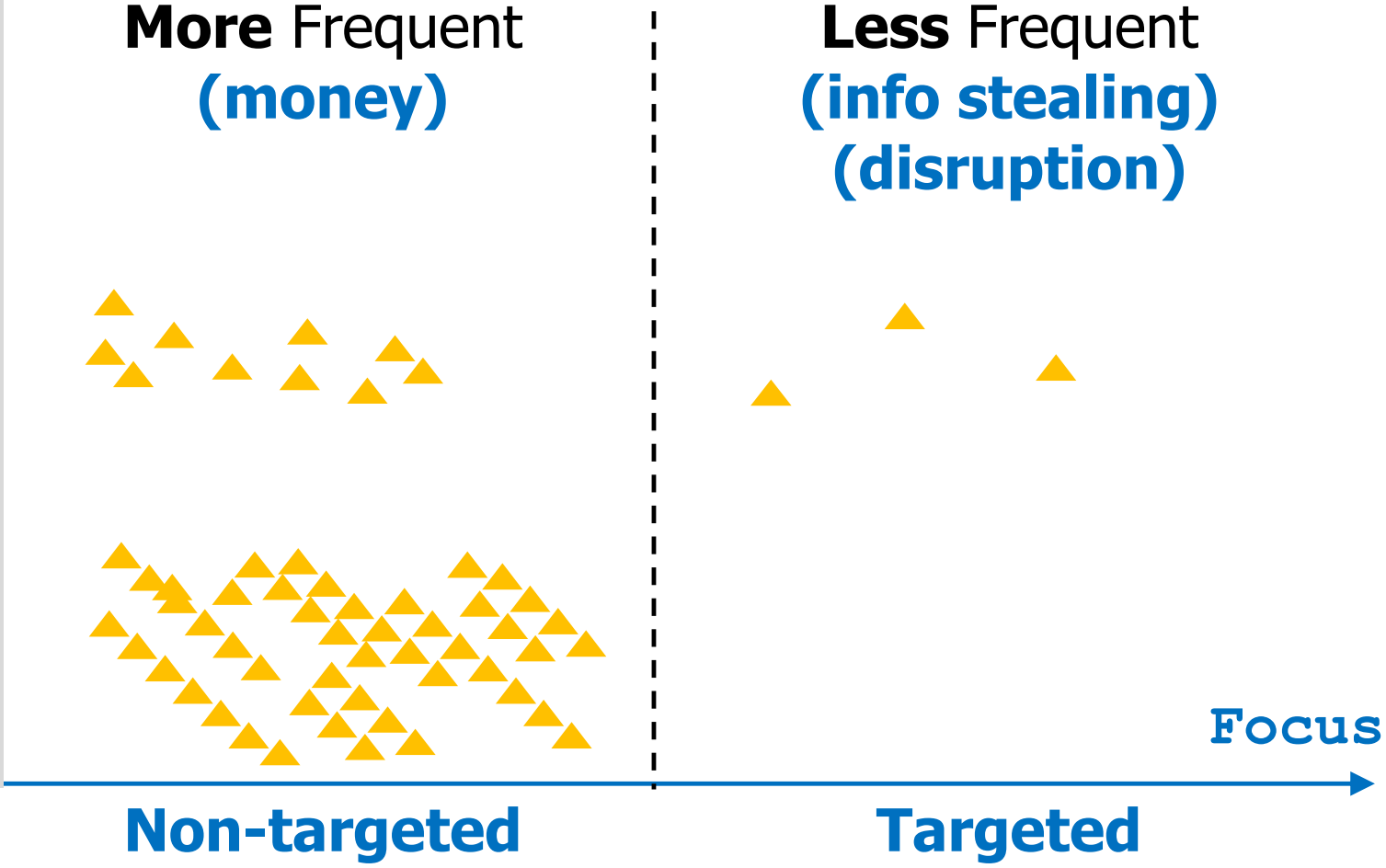
Keep in mind 2

- IF early attack steps on a particular target suggest that the target has a good defense
- THEN **change** the target

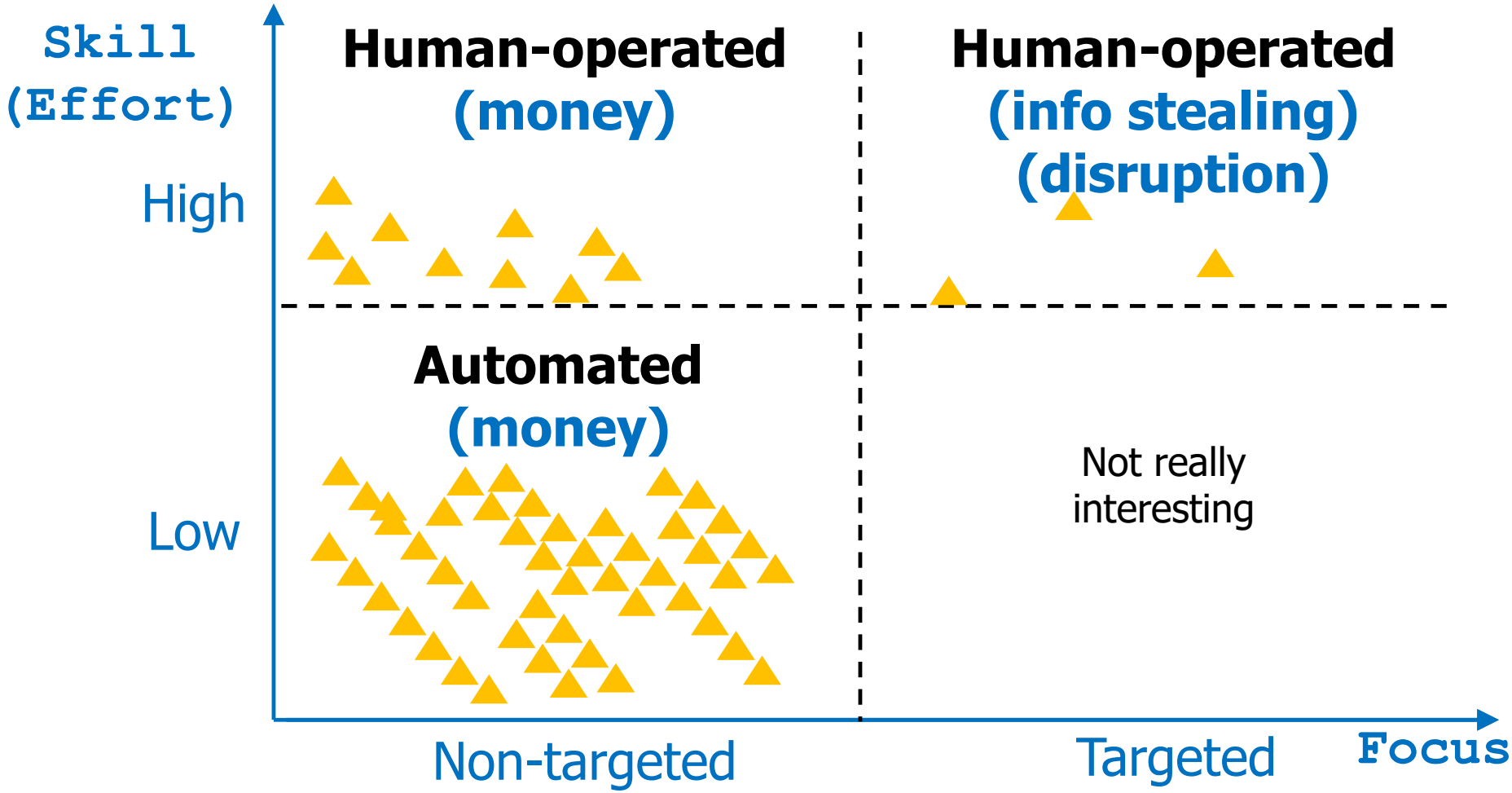
- This is by far the **most common** attacker mindset

Attack Categories

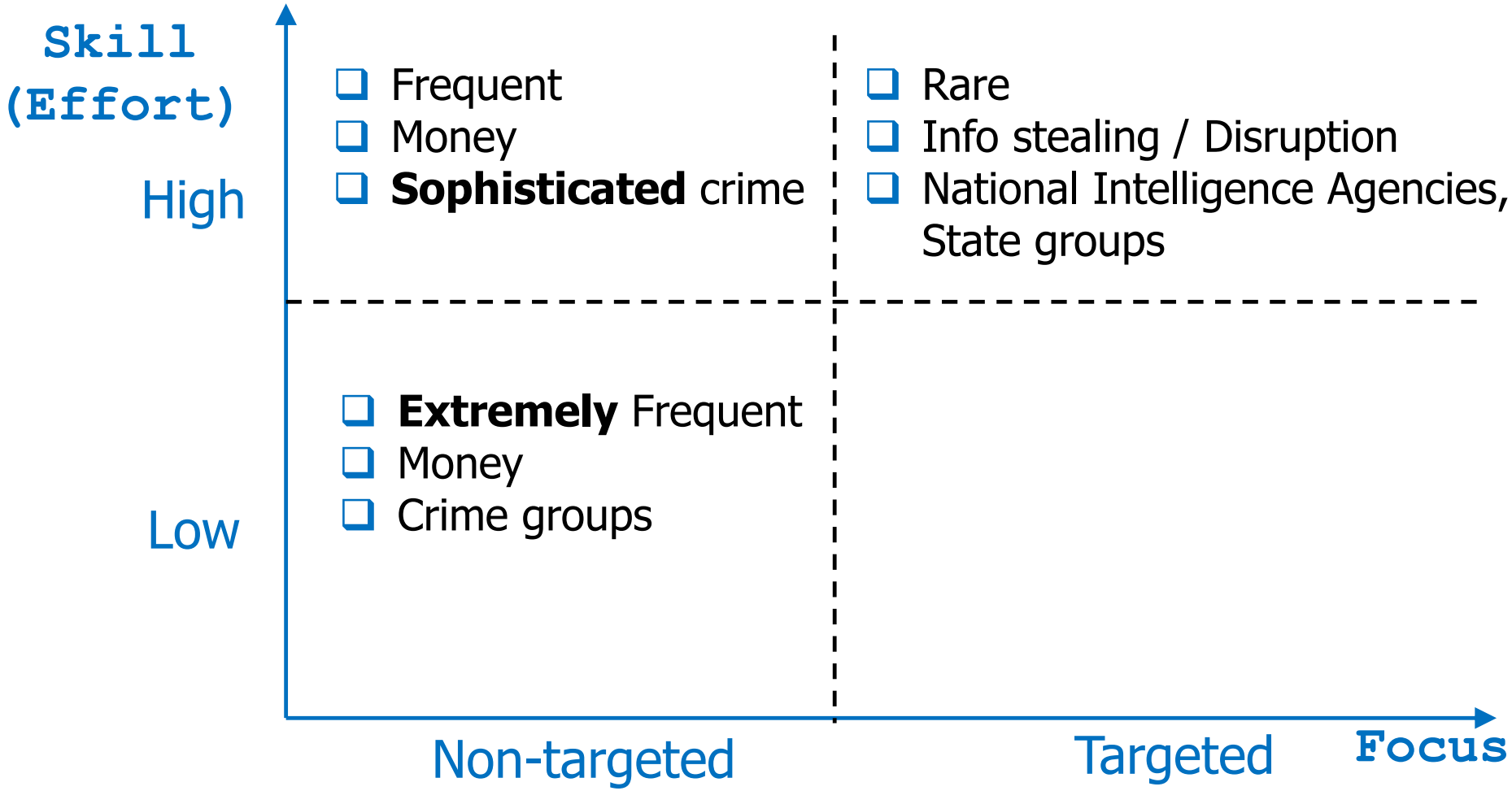
Attack Categories: Focus



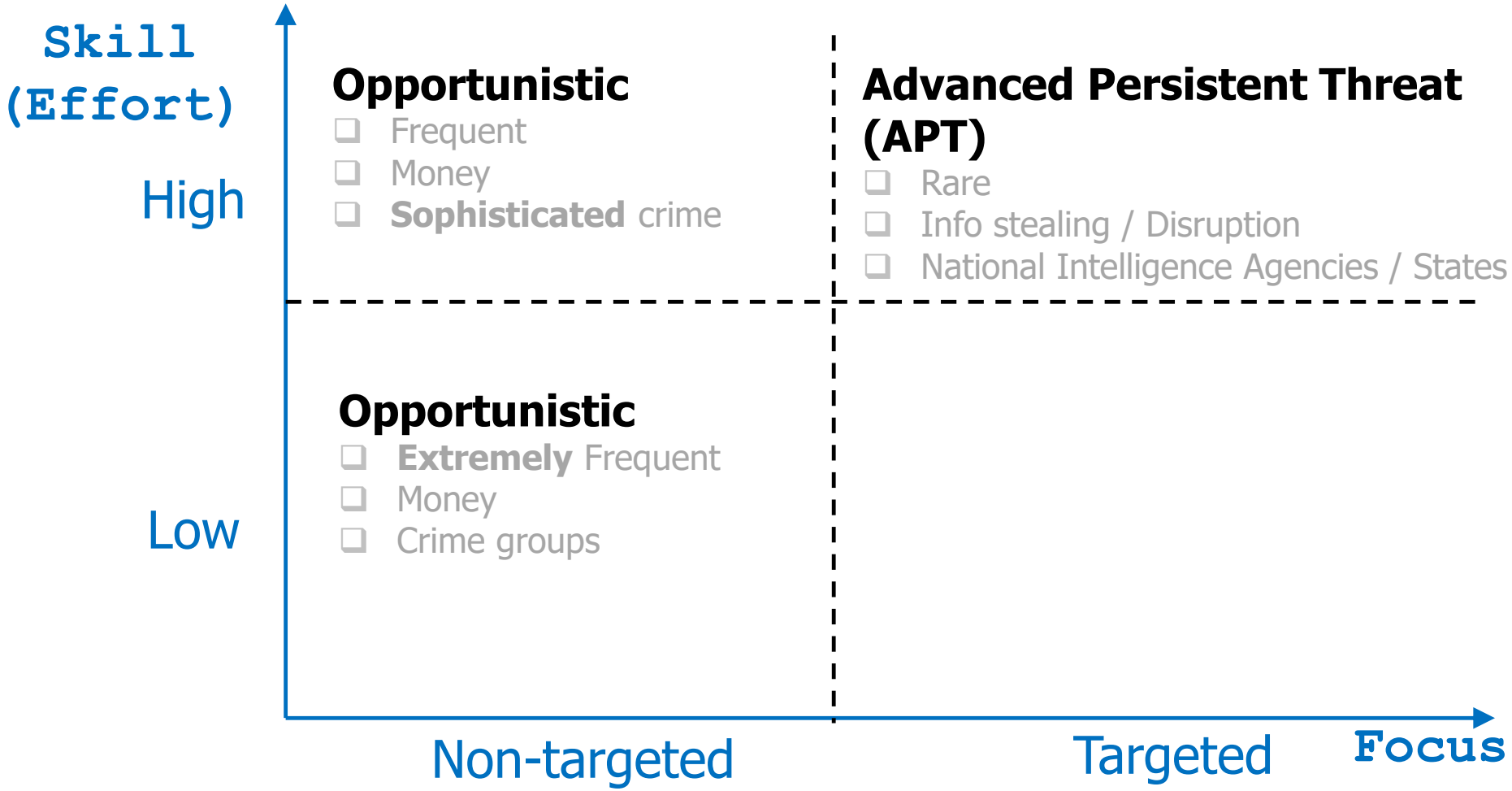
Attack Categories: Threat Matrix (I)



Attack Categories: Threat Matrix (II)

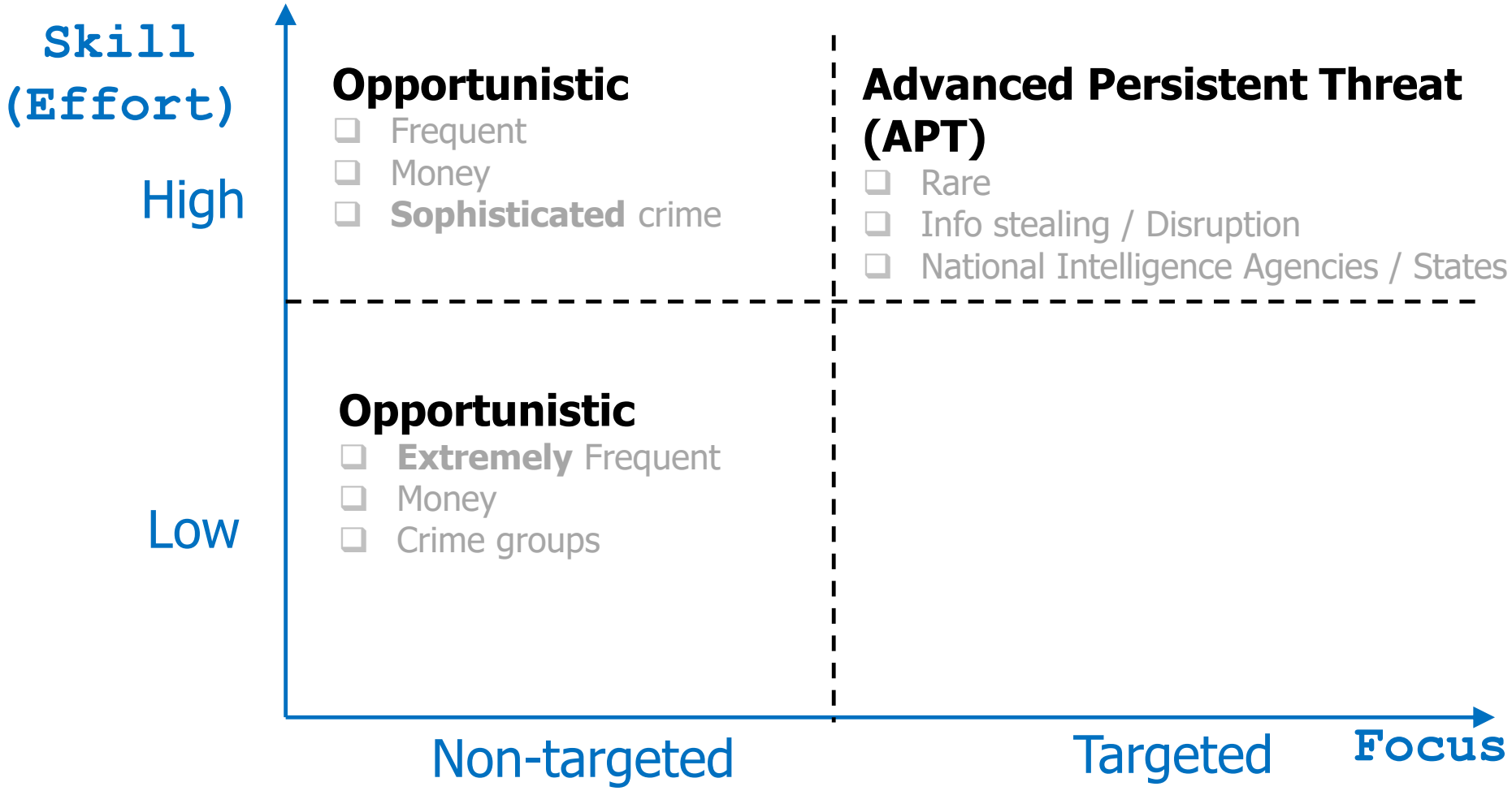


Attack Categories: Threat Matrix (III)

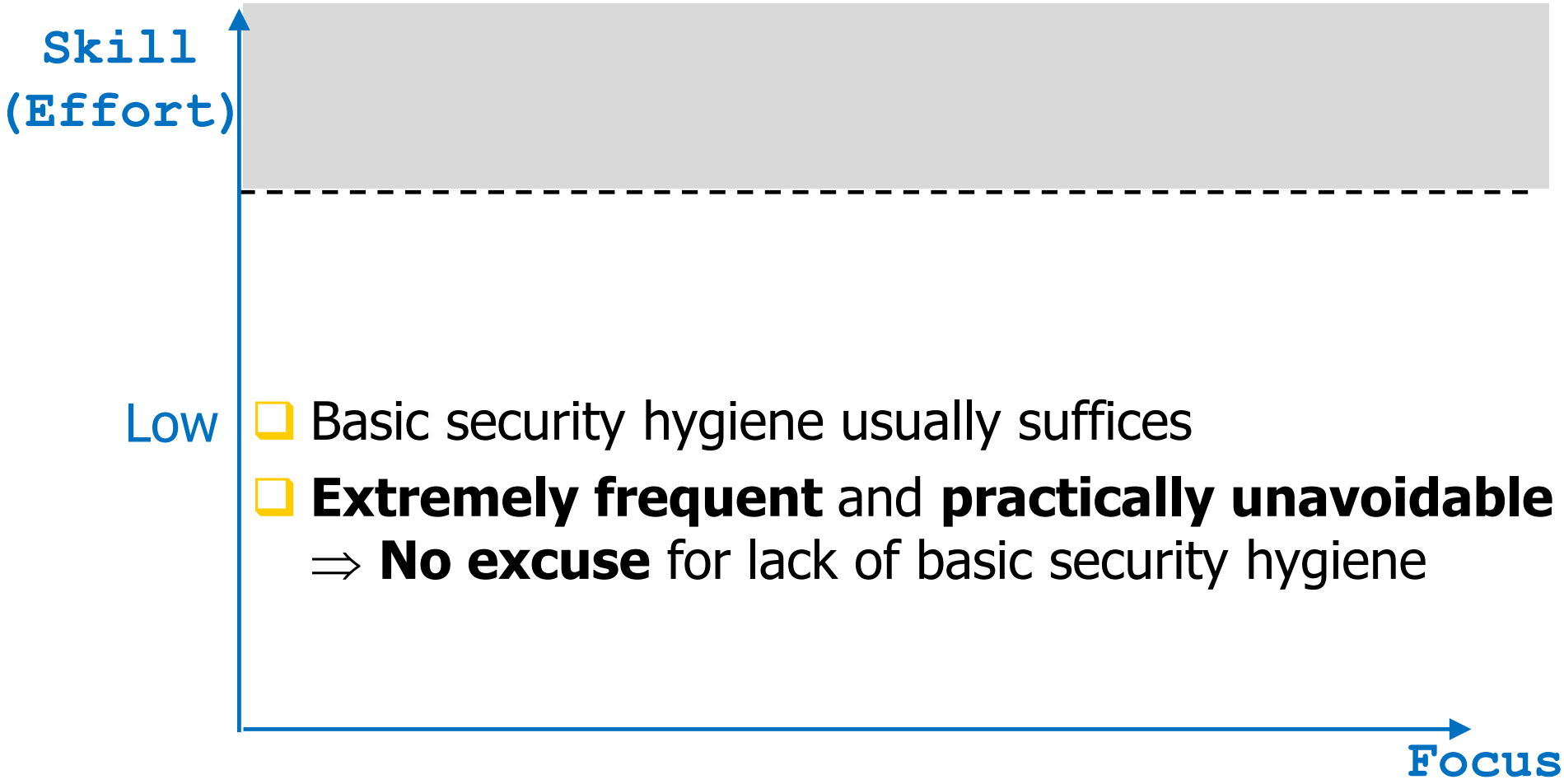


Strategic Framework: Defender Mindset

How to defend?

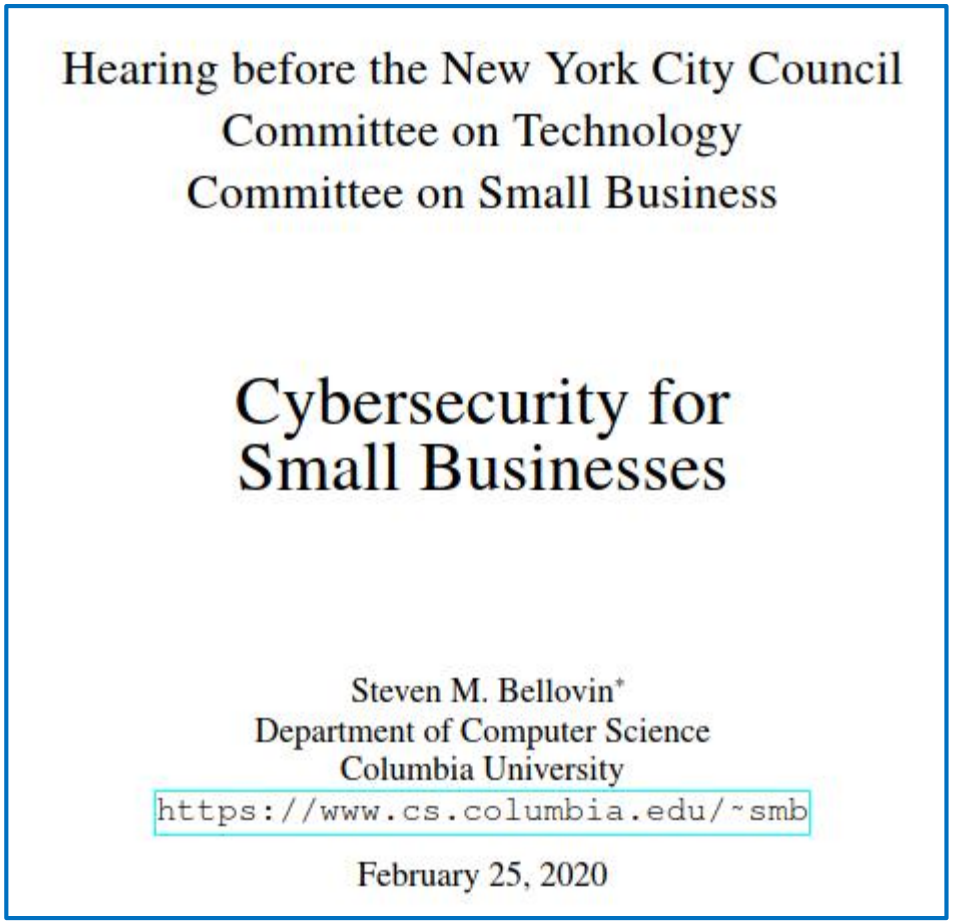


Low Effort Attacks



- Basic security hygiene usually suffices
- **Extremely frequent** and **practically unavoidable**
  ⇒ **No excuse** for lack of basic security hygiene

(Strongly) Suggested Reading



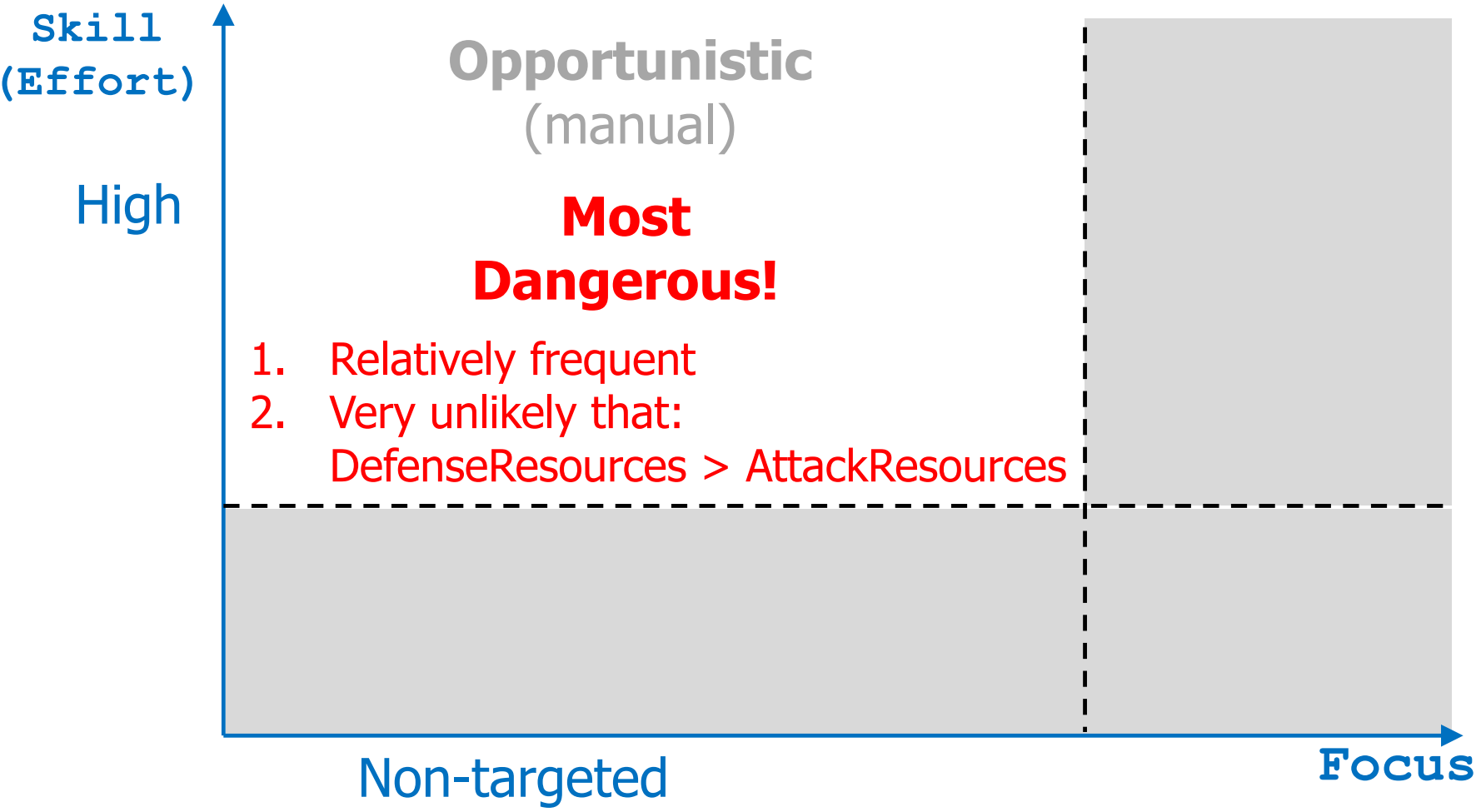
Hearing before the New York City Council
Committee on Technology
Committee on Small Business

Cybersecurity for Small Businesses

Steven M. Bellovin*
Department of Computer Science
Columbia University
https://www.cs.columbia.edu/~smb

February 25, 2020

High Effort Attacks: Opportunistic



DefenderResources vs AttackerResources

Very unlikely that:
DefenseResources > AttackResources

- Costs are **highly asymmetric**
  - Attacker: may **concentrate** resources on a **few points** in a **few moments**
  - Defender: must "dilute" resources **everywhere** and **always**

- With comparable resources, Attacker wins

Example: Initial Access

- Costs are **highly asymmetric**
  - Attacker: may **concentrate** resources on a **few points** in a **few moments**
  - Defender: must "dilute" resources **everywhere** and **always**
- Hundreds of PCs / Notebooks
- End-of-life web framework
- Network printer forgotten by everyone
- Webcams
- Heating / cooling systems
- ...

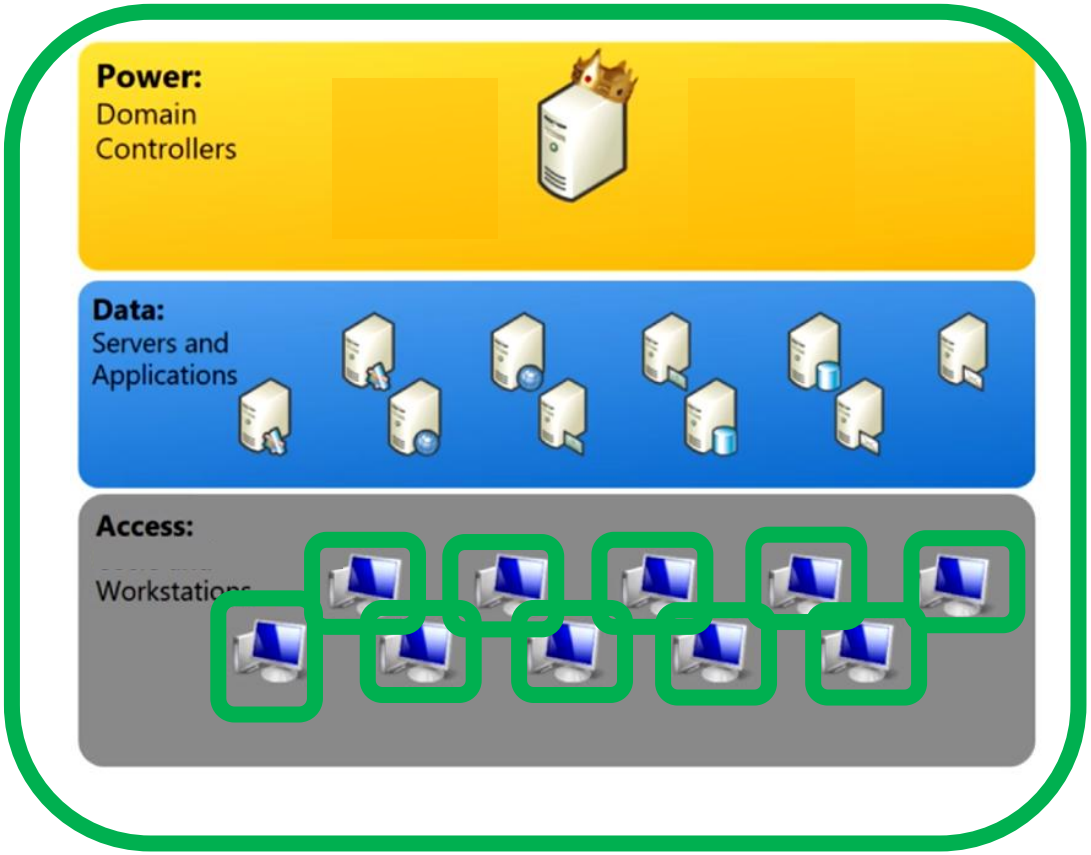
Opportunistic Attacks: Key Defender Strategy

1. Select target
2. (Possibly) Collect information
3. Execute attack
4. IF attack becomes too difficult THEN **change target**

- **Encourage attacker to change target**

- Defense must **appear** good
- Penetration / Lateral movement should be **expensive**
- Defense in depth (**multiple independent** layers)

Example: Tight Wks Firewalls

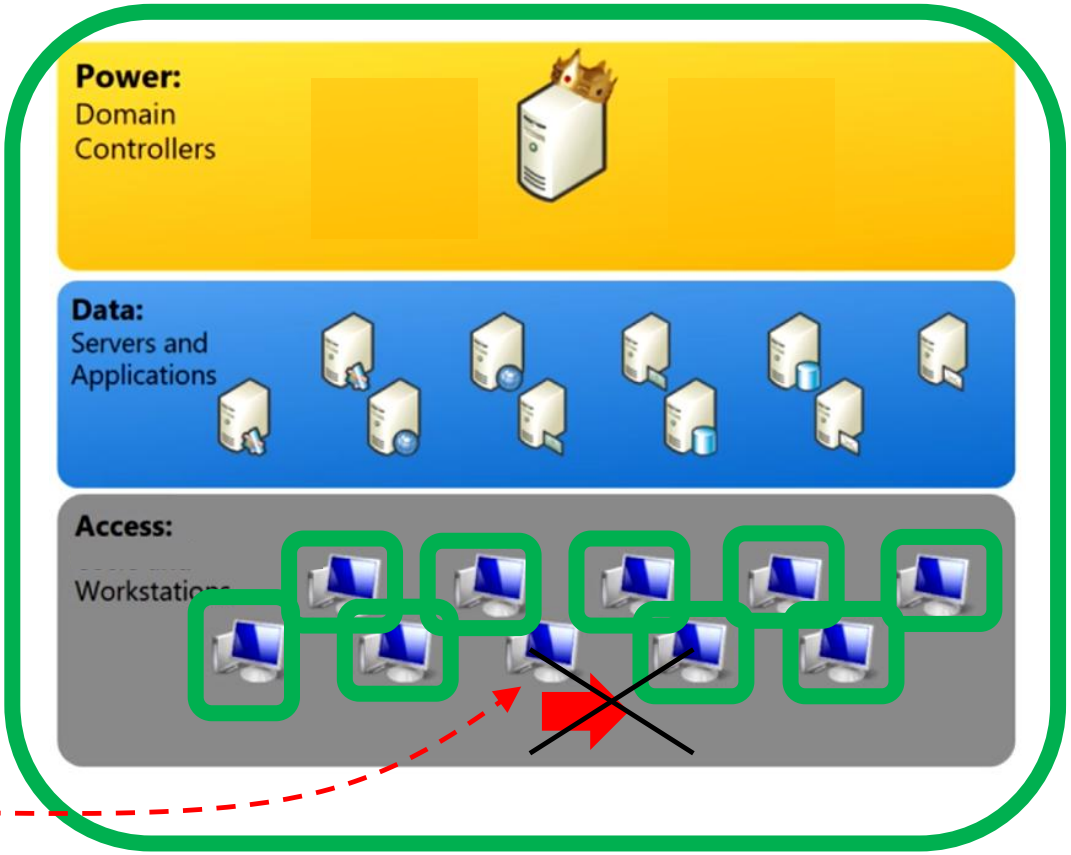


- ~~Default configuration: Accept **inbound** connections from **any** machine~~
- Stricter configuration: Do **not** accept **any** inbound connections
- Except from the **very few designated** remote maintenance wks

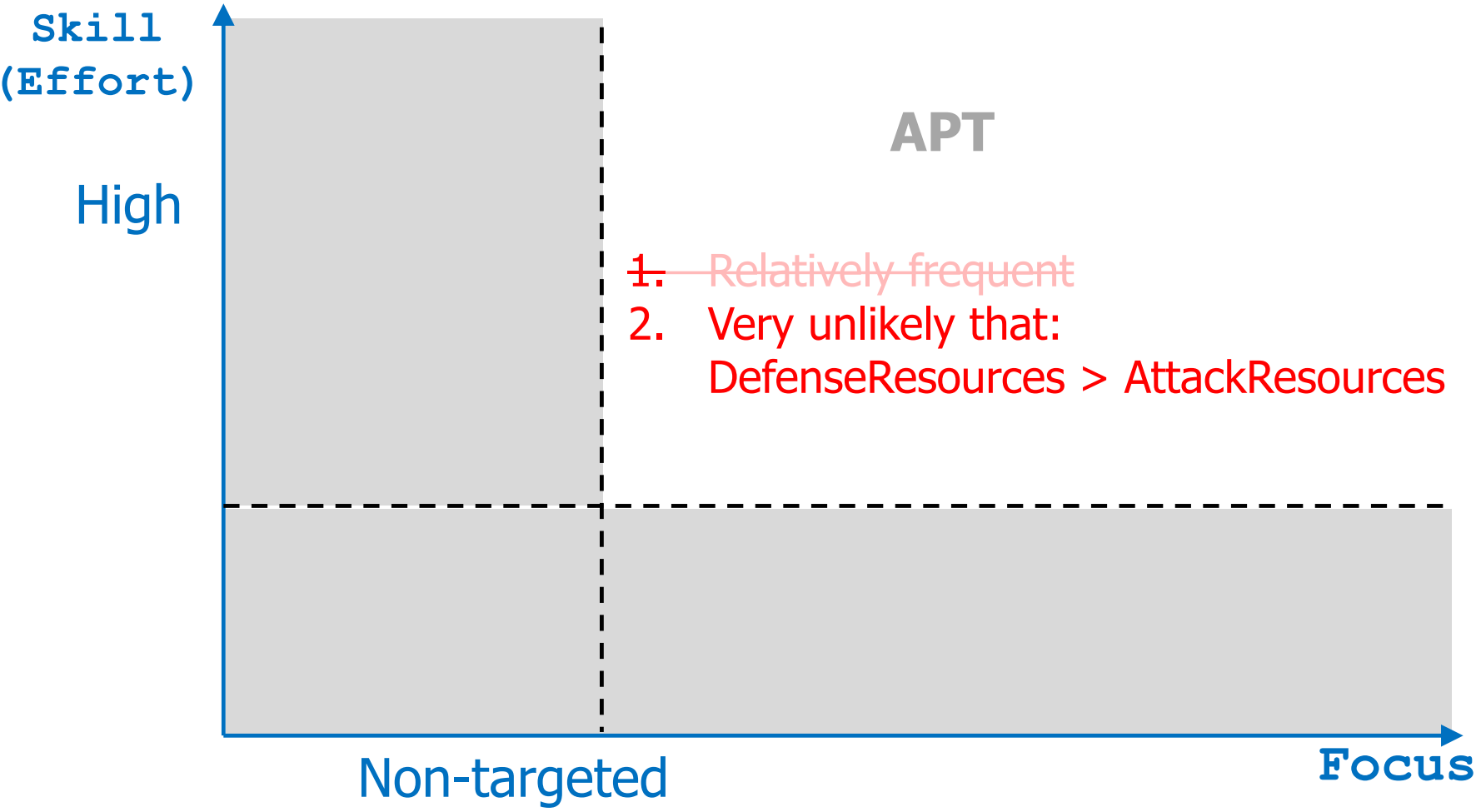
Lateral movement?

- I cannot connect anywhere!
- I need to find **how** to overcome this **additional** defense
- Will there be **further** defenses?

Better change target



High Skill/Effort Attacks: APT



APT Attacks: Key Defender Strategy

- **Cross your fingers!**
  - IF a **highly skilled** attacker is **firmly** interested in **you**
  - THEN it is **very unlikely** that you will be able to resist and it will not change target

- My suggestion: strong focus on **opportunistic** attackers

Understanding Cybersecurity

Every major incident…

- Recommended defensive actions:
  - Neither rocket science nor esoteric technology
  - **Always the same "boring" recommendations** (more or less)

Naive Questions

- Recommended defensive actions:
  - Neither rocket science nor esoteric technology
  - **Always the same "boring" recommendations** (more or less)

- Why it is always necessary to recommend them?
- Why they are not implemented???

Understanding Cybersecurity in the real world

- Do **not** look at **technical** issues
- Focus on the **incentive** structure of your environment

- **Warmly suggested** reading:
  "How CEOs think" - Robert Graham
  https://blog.erratasec.com/2020/07/how-ceos-think.html

Excerpt from "How CEO think"

- Unless you are a company like Google, whose cybersecurity is a competitive advantage, **you don't want to excel in cybersecurity**. You want to be average, or at most, slightly above average. **You want to do what your peers are doing**.
- It doesn't matter that this costs a lot of money due to data breaches. As long as the cost is no more than your competitors, then **you are still competitive in your markets**.

- (my opinion: one of the most important slides of this entire course)

Enter a tradeoff mindset

- Cybersecurity is **not** about **preventing** attacks
- It is about **tradeoffs**

- Distribute your defensive budget the best you can
  - Are 1000$ more effective for Prevention or for Remediation?
  - How should I distribute 1000$ for defending asset A and asset B?

Think in Economical Terms (REMIND)

- To understand cybersecurity **never** think only in **technical** terms
- **Always** think in **economical** terms

- What is the cost?
  - Attack, Defense, Incident
- Who pays?

- **Money is what drives the world**
  - It may sound cynical…but thinking in these terms is very helpful