Cyber Security and Vulnerability Assessments

THE EVOLVING LAW ON HACKING AND EXTORTION IN THE AGE OF BUG BOUNTIES

Presented by
Avi Gesser, Davis Polk Litigation Partner
Reuben Grinberg, Davis Polk Financial Institutions Group Associate
Matthew Kelly, Davis Polk Litigation Associate
Michael Scheinkman, Davis Polk Litigation Counsel

November 15, 2017

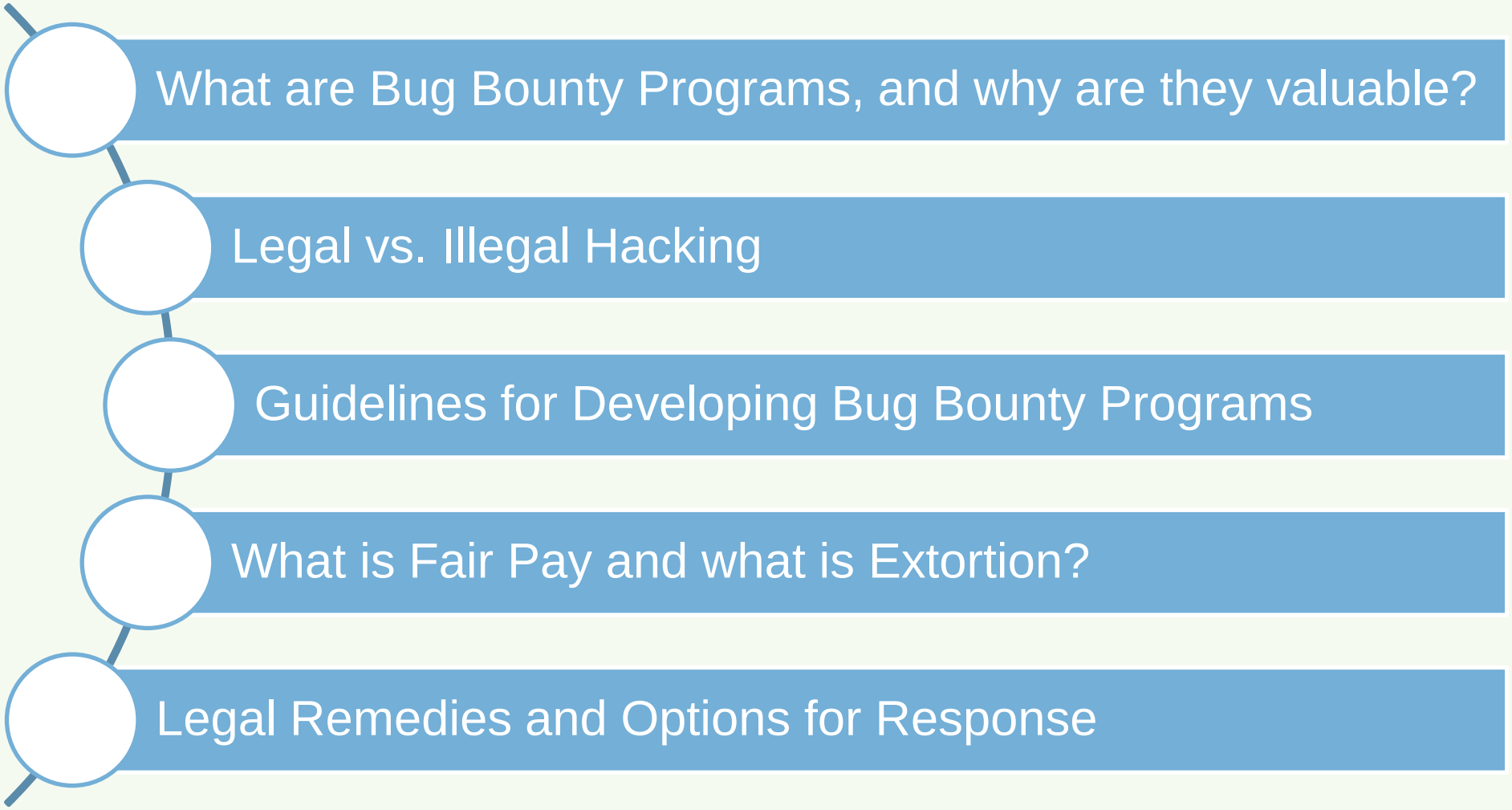
Davis Polk

Davis Polk & Wardwell LLP

CLE CREDIT AVAILABLE

WWW.CYBERBREACHCENTER.COM

Topics Overview



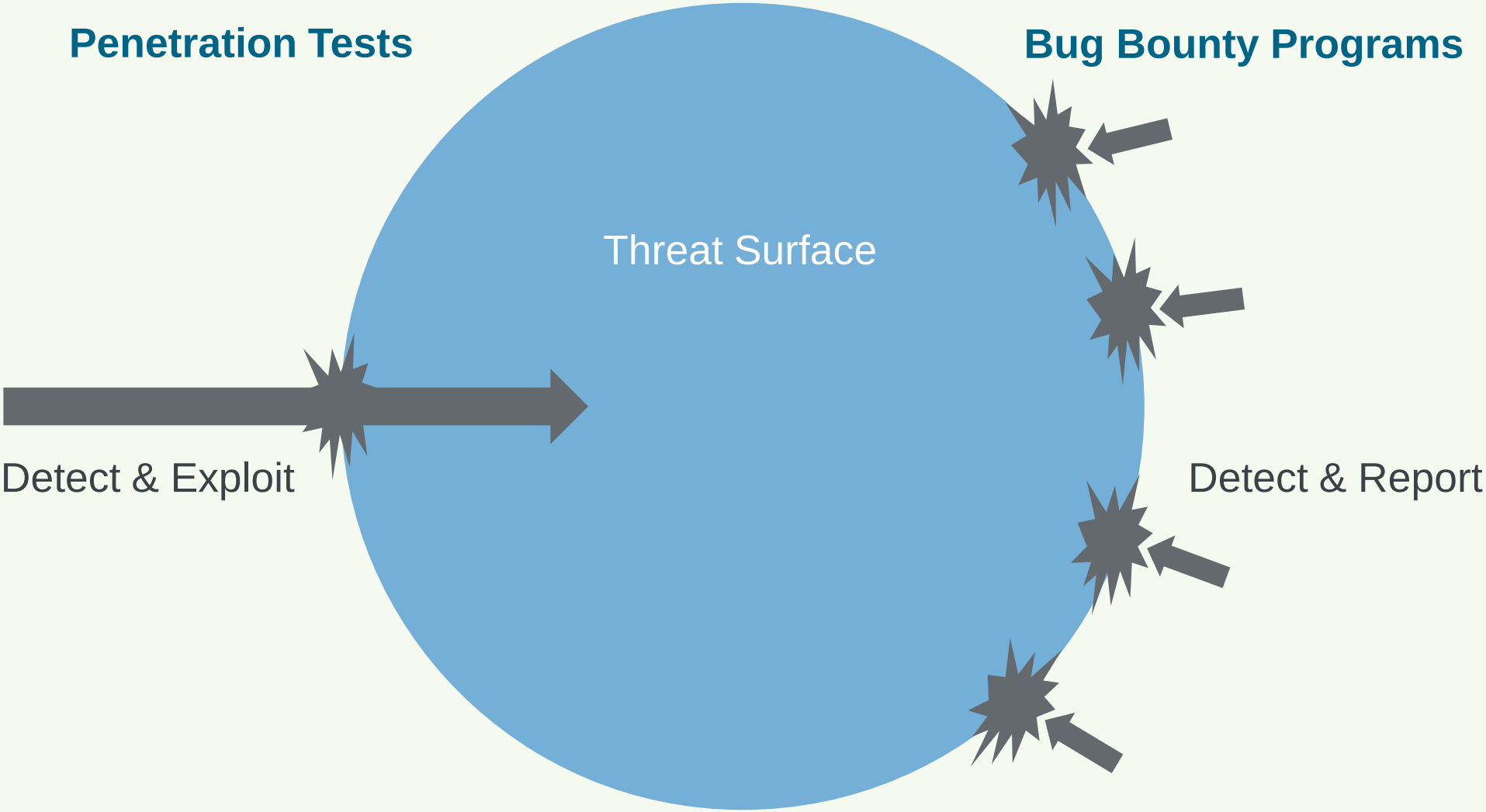
What are Vulnerability Assessments?

“Vulnerability” defined.

- “[A]n occurrence of a weakness (or multiple weaknesses) within software, in which the weakness can be used by a party to cause the software to modify or access unintended data, interrupt proper execution, or perform incorrect actions that were not specifically granted to the party who uses the weakness.”

Common Weakness Enumeration

What are Vulnerability Assessments?



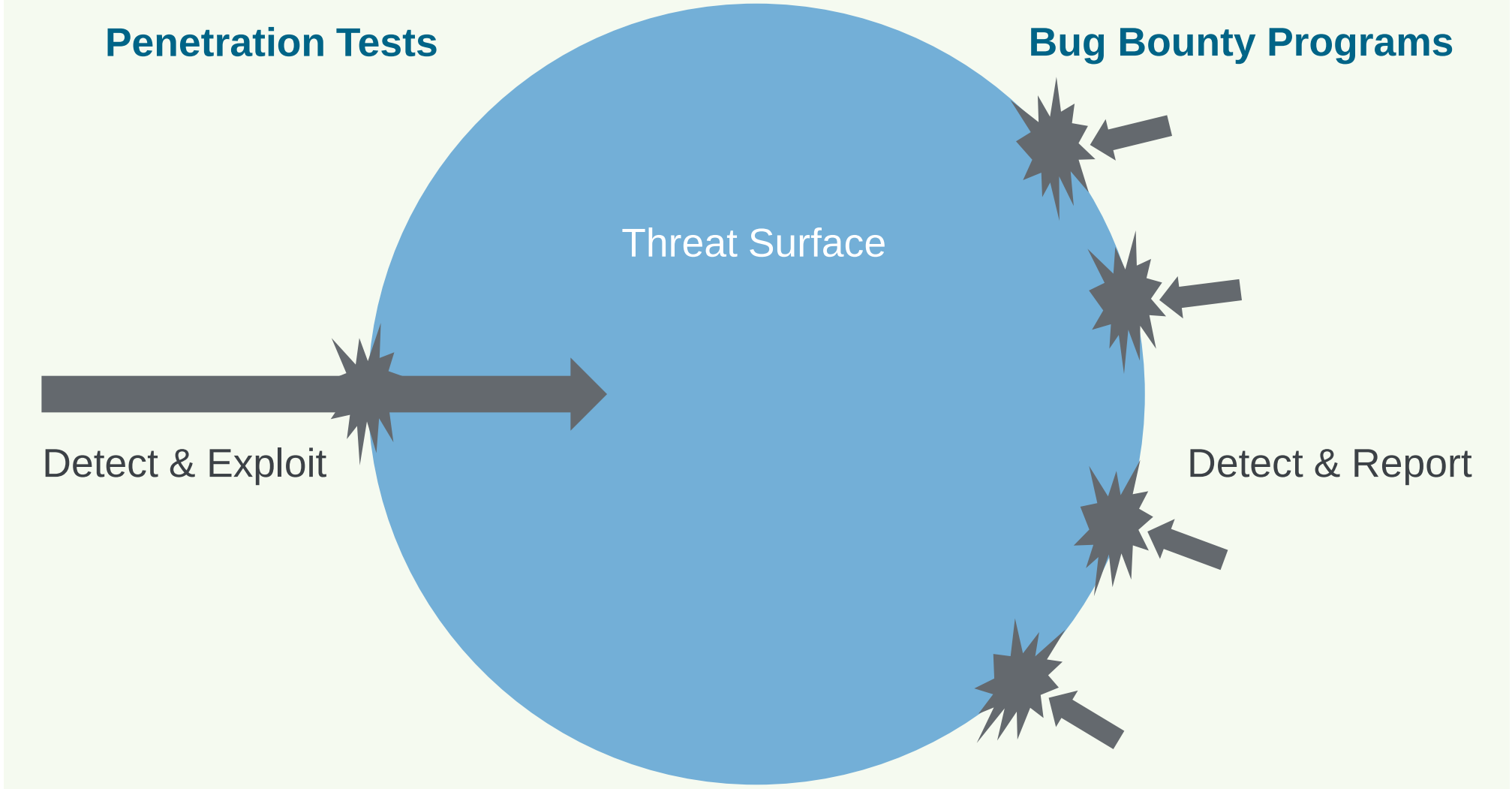
What is Illegal Hacking?

- **Computer Fraud and Abuse Act** ("CFAA"), 18 U.S.C. §1030(a)(2)
  - "*Whoever—*
    - *(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains*
      - *(c) information from any protected computer*

        shall be punished as provided in subsection (c) of this section."

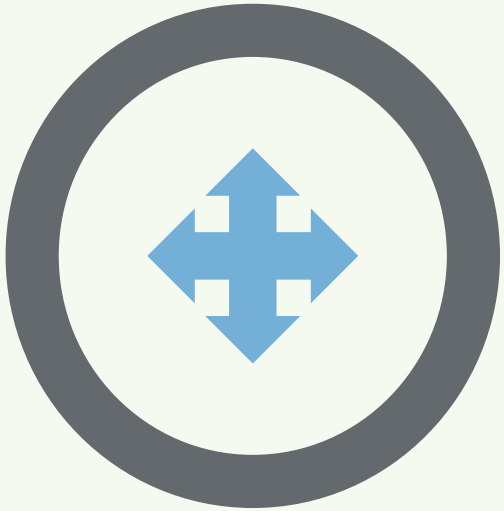
- **Digital Millennium Copyright Act** ("DMCA"), 17 U.S.C. §1201(a)(1)
  - "*(A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title.*"

Types of Vulnerability Assessments

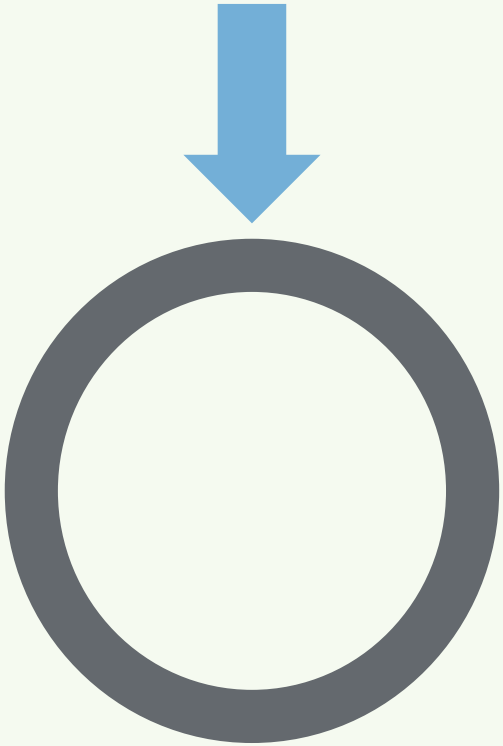


Types of Vulnerability Assessments (cont.)

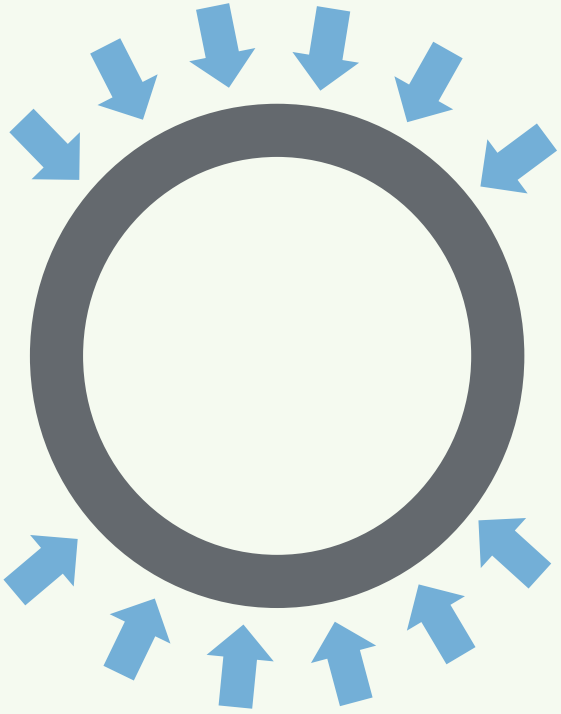
Employee Model



Third-Party Model



Bug Bounty Model



What are Bug Bounty programs?

Program Outlines typically include:

- Eligibility for Participation
- Conditions for Award of Bounty
- Payment Scale
  - Type of vulnerability
  - Severity of vulnerability
- Systems Included and Excluded
- Vulnerability Reporting Protocol
- Confidentiality Rules

Risks of Bug Bounty Programs

- Extortion
- Public Disclosure
- Black Market Sale
- Exploitation by Hacker

How to Minimize Risk in Bug Bounty Programs

- Manage everything through **contract**
  - Involve lawyers experienced in vulnerability assessment programs.
- Draw clear lines between **authorized** and **unauthorized** conduct
  - What vulnerabilities are you testing?
  - What techniques are off-limits?
    - Physical security challenges?
    - Social engineering?
  - What can hackers do with information acquired? When?
- Set clear **expectations**
  - Are hackers expected to fix the vulnerability?
  - Who is eligible? Who isn't?
- Limit possible **fallout**
  - Set up dummy environments.
  - Add safeguards for third-party data.

Compensation in Bug Bounty Programs

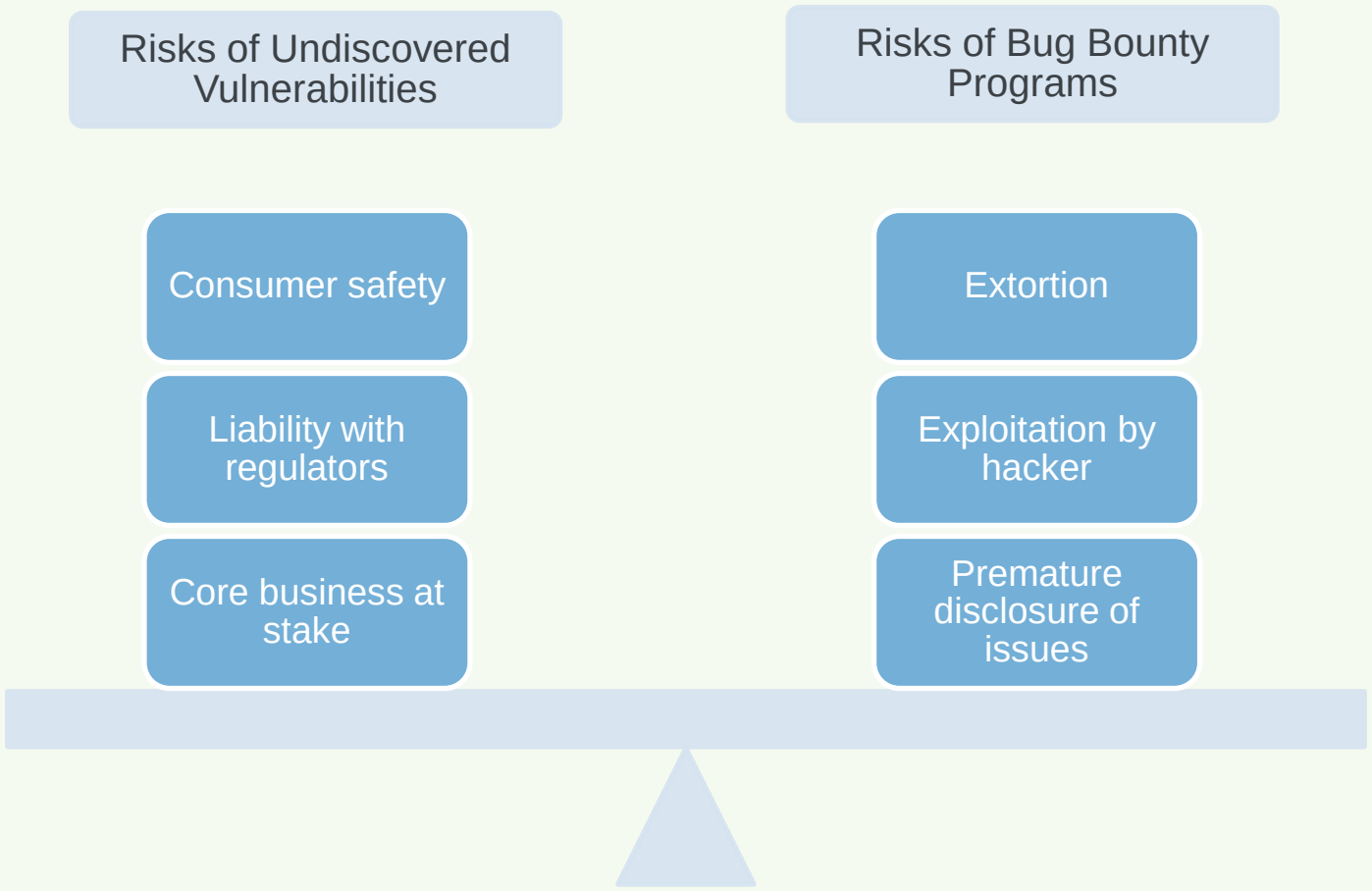
- **Compensation Factors**
  - Size and public profile of company
  - Complexity of threat surface
  - Risk profile and core business of company
  - Maturity of security systems
  - Type of vulnerability sought
  - Talent and experience of participants
- **Payment Structure**
  - Half on discovery; half on remediation without violative disclosure
  - Award to cybersecurity team if no vulnerabilities reported
- **Pricing Range**
  - Microsoft: Up to $250,000
  - Google: $500 to over $30,000
  - PayPal and Uber: Up to $10,000

Make Sure You Can Fix It!

Don’t initiate an assessment program without planning for remediation

- Designate resources for remediation
  - Money
  - Time
  - Personnel
- Remove or exclude things you can’t fix
  - Review and/or negotiate vendor contracts for repair obligations
  - Consider excluding third-party apps or software from scope
- Plan for program administration
  - Consider third-party brokers for eligibility, report verification, etc.

Why bother?


Risks of Undiscovered Vulnerabilities
Risks of Bug Bounty Programs
Consumer safety
Liability with regulators
Core business at stake
Extortion
Exploitation by hacker
Premature disclosure of issues

Responding to Extortion

Options for Response:

- Pay up
  - If the threat of damage is too great or the sum actually is reasonable in light of the vulnerability, payment may be easiest.
- Notify hacker of breach of contract
  - White hat hackers depend on their reputations – highlighting the implications of blacklisting may be enough.
  - Temporary Restraining Orders are possible, but may not prevent harm.
  - Threaten suit, if needed.
- File suit
  - A carefully drafted contract should provide adequate basis for an allegation of breach.

→ Demanding more money for a vulnerability is NOT blackmail, but it may be extortion.

Responding to Extortion (cont.)

Criminal Statutes

- 18 U.S.C. § 875(d)
  - *"Whoever, with intent to extort from any person, firm, association, or corporation, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, shall be fined under this title or imprisoned not more than two years, or both."*
- Hobbs Act: Interference with commerce by threats or violence, 18 U.S.C. § 1951
  - *"(a) Whoever in any way or degree obstructs, delays, or affects commerce or the movement of any article or commodity in commerce, by robbery or extortion or attempts or conspires so to do, or commits or threatens physical violence to any person or property in furtherance of a plan or purpose to do anything in violation of this section shall be fined under this title or imprisoned not more than twenty years, or both."*
    - *"(2) The term 'extortion' means the obtaining of property from another, with his consent, induced by wrongful use of actual or threatened force, violence, or fear, or under color of official right."*

Responding to Extortion (cont.)

Criminal Statutes (cont.)

- **Computer Fraud and Abuse Act** ("CFAA"), 18 U.S.C. § 1030(a)(7)
  - *"(a) Whoever—*
  - *(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—*
    - *(A) threat to cause damage to a protected computer;*
    - *(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or*
    - *(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;*
      - *shall be punished as provided in subsection (c) of this section."*

Outlook: Are Bug Bounty Programs Here to Stay?

It seems like it!

- Increased attention by regulators to both cyber vulnerabilities and what can or should be done to address them.
- Proliferation and increased sophistication and reliability of white hat hackers and brokers.
- Relatively high efficiency and ROI.
- Continued, dramatic increase in size and complexity of threat surfaces across all industries.

Questions?

Visit: www.cyberbreachcenter.com