black hat USA 2023

AUGUST 9-10, 2023

BRIEFINGS

Does Public Disclosure of Vulnerabilities Affect Hacker Participation in Bug Bounty Programs?

Speaker: Ali Ahmed, Ph.D. – University of Wisconsin Eau Claire

Contributors: Brian Lee – Penn State University, Amit Deokar – University of Massachusetts Lowell

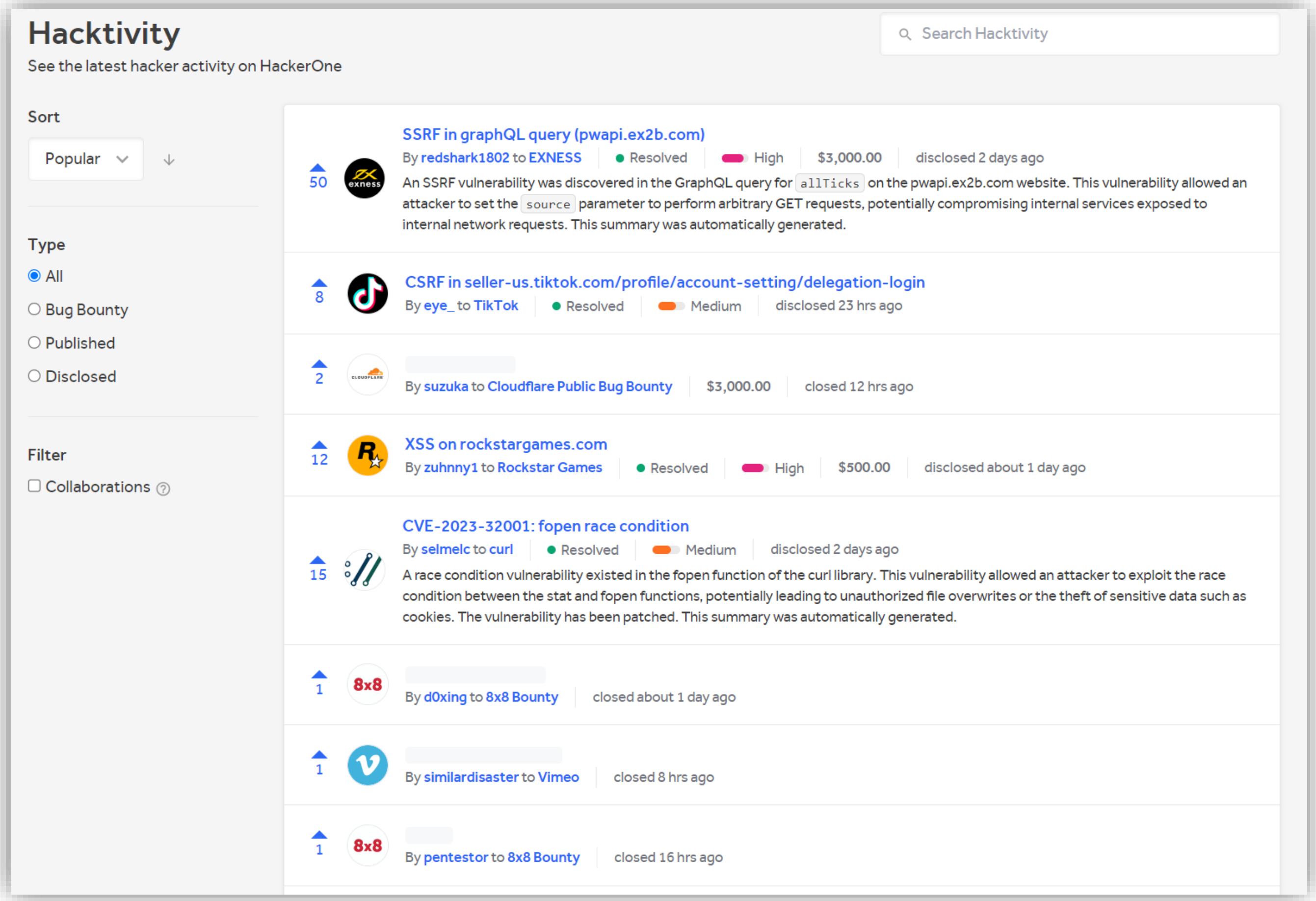
University of Wisconsin Eau Claire

Two Questions:

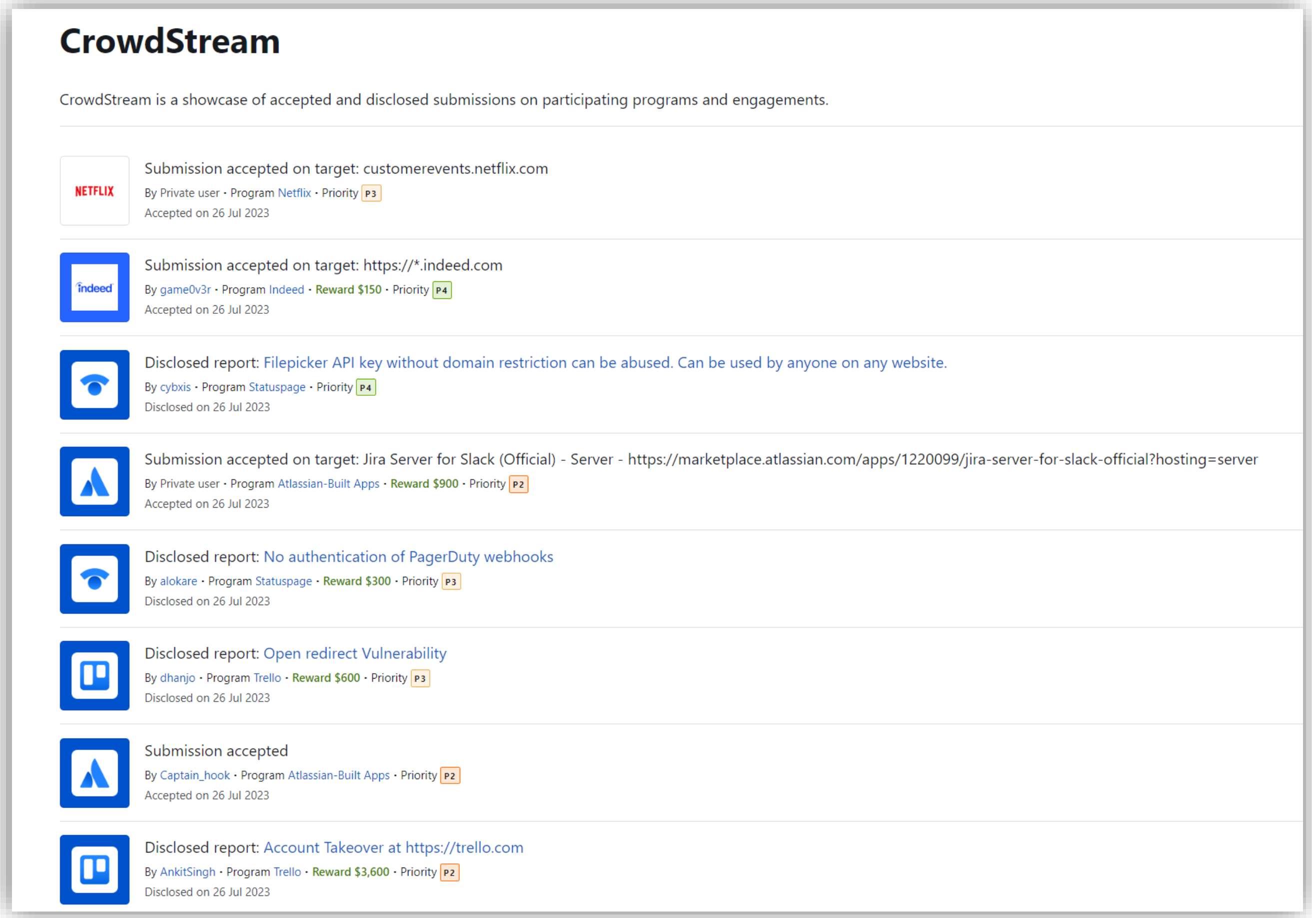
- As an organization, would you publicly disclose patched vulnerability reports?

- As a hacker, would the disclosed reports help you find more bugs?

Many Organizations on HackerOne and BugCrowd Publicly Disclose Reports



HackerOne's Hactivity



BugCrowd's CrowdStream

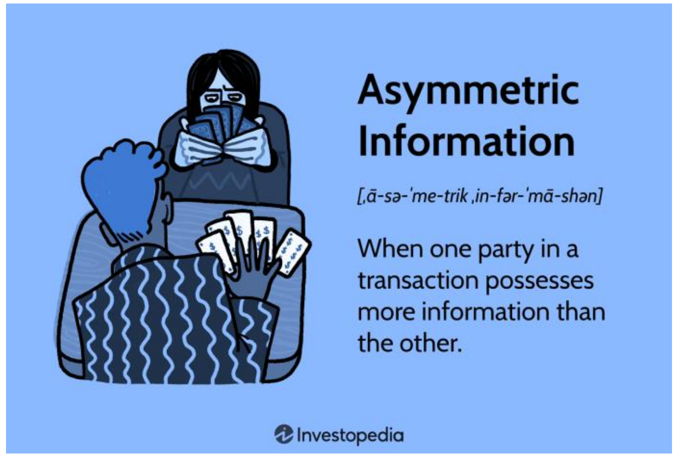
Research Questions

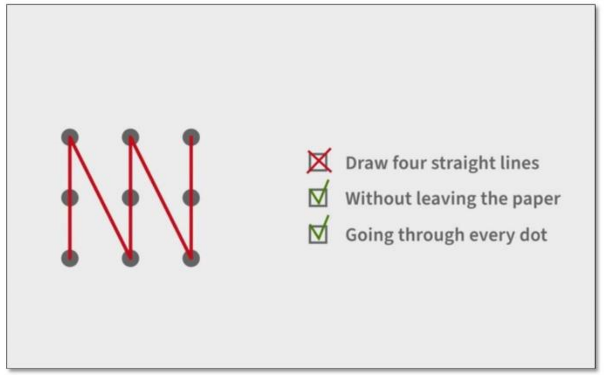
1. How does the public disclosure of patched vulnerabilities affect the discovery of new vulnerabilities in bug bounty programs?
2. Does the disclosed information help hackers in discovering new vulnerabilities?
3. Does the disclosure increase or decrease hackers' success?
4. If disclosure has an effect, what type of disclosures or hackers are most affected?

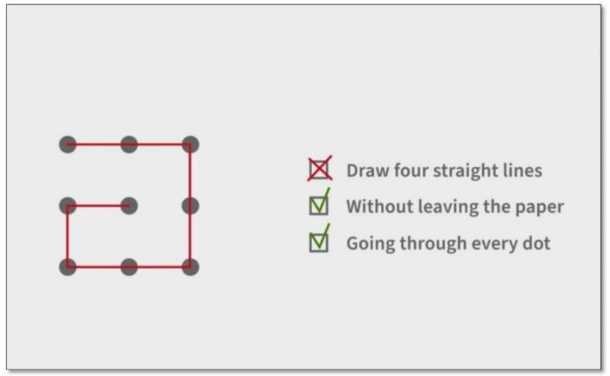
There could be two possibilities:

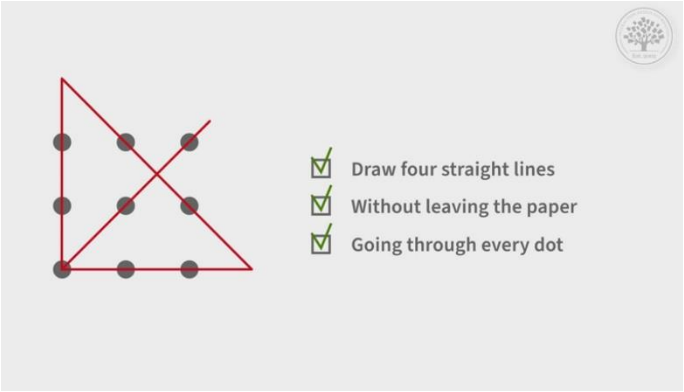
1. Disclosure can provide valuable information to hackers, which they can use to increase their success in finding new vulnerabilities in a system.

2. Disclosure can also obstruct hackers thinking and could negatively affect their cognitive capabilities. Disclosure can decrease their success in finding new vulnerabilities.









Theoretical Framework

Theoretical Framework

- Hacking is a highly creative process.
- Disclosure can cause cognitive fixation in hackers and can negatively impact their creativity.
- Fixation is the human tendency to approach a given problem in a set way that limits one's ability to shift to a new approach to that problem (Duncker 1945).
- **Prior examples** can reduce creativity, and people tend to fixate on the principles and features of prior examples.
- Disclosure of past discoveries can cause fixation in hackers' cognitive processes and obstruct their ability to find new ways to discover vulnerabilities.

Fixation:
"The mind's obstacle to seeing what is right in front of us."

There are types of fixation:

- Mental set
- The counterintuitive finding that prior experience or domain-specific knowledge can, under some circumstances, interfere with problem-solving performance.
- It is a cognitive trap arising from a desire to find familiar features in problems and reuse shortcuts to solve them.
- Prior experience can prime the mind and block creative problem-solving.
- Functional Fixedness
- It is a cognitive bias that limits a person to use an object only in the way it is traditionally used.
- The iceberg which drowned the Titanic could be used as a float.

Titanic Iceberg

We hypothesize:

- In bug bounty programs disclosing previous examples of discovered vulnerabilities may lead to cognitive fixation in hackers.
- Hackers are unable to generate new creative ideas to discover unknown vulnerabilities.
- Their search process may conform to the features related to the disclosed vulnerabilities, which is counterproductive in finding new vulnerabilities.
- Thus, disclosure leads to fewer discoveries and lower success for hackers.

Study Context, Dataset, and Methods

Dataset

- We collected publicly available data from a leading bug bounty platform.
- Our platform is similar to renowned bug bounty platforms like HackerOne and BugCrowd.
- Once the organization fixes the reported vulnerability, they mark it as resolved (patched) on the platform.
- After resolving, firms can publicly disclose the contents of the report.

Dataset

- Our dataset comprises of 368 firms that have launched public bug bounty programs.
- The total number of resolved reports from these firms is 83,473 vulnerability reports.
- Among them, 8,712 vulnerability reports were publicly disclosed by the firms (10.4% of the total).
- Using this report-level data, we created a firm and month-level (unbalanced) panel dataset consisting of 368 firms and 80 months.
- For each firm in each month, we calculated the number of reports resolved, the number of disclosed (and hidden) reports, the bounties awarded, and the number of hackers involved.

Dependent Variable: Resolutions

- Our dependent variable is the number of resolved reports for each month by a firm.
- We counted the number of reports resolved for each month by a firm and named it $Resolutions_{it}$, i.e., the number of resolved reports by firm *i* in month *t.*
- We also counted the number of unique successful hackers in each month and named it $SuccessfulHackers_{it}$

Independent Variable: Past Disclosures

- The main independent variables in our firm-month panel data are the cumulative resolutions and cumulative disclosures of reports by each firm in each month.
- We counted the number of resolved reports for each firm in a given month.
- We aggregated the count of resolved reports to capture the overall resolution level of a program.
- This variable is denoted as $CumlativeResolution_{it}$, representing the sum of resolved reports, $\sum_{t=1}^{n} ResolvedReports_{it}$, where *i* represents a firm and *t* represents a month.

Independent Variable: Past Disclosures (cont.)

$$CumulativeDisclosureFraction_{it} = \frac{CumulativeDisclosure_{it}}{CumulativeResolution_{it}}$$

- Since previously disclosed reports remain visible to hackers, we aggregated the counts of disclosed reports over time and call it $CumulativeDisclosure_{it}$.
- The $CumulativeDisclosureFraction_{it}$ serves as our main explanatory variable, capturing the effect of a firm's disclosure on the discovery and resolution of new vulnerabilities.
- It ranges between 0 and 1, and changes as new reports are disclosed or resolved. Additionally, disclosed reports are categorized as either "valid" or "invalid" by the firm.
- We computed the aggregated level of valid disclosures and divided it by the cumulative resolutions of the firm *i* until period *t* to obtain the proportion of disclosed reports that are valid.

Empirical Specifications

We used econometric specifications of multiple fixed-effects linear regression models to find the relationship between past disclosures and future resolutions.

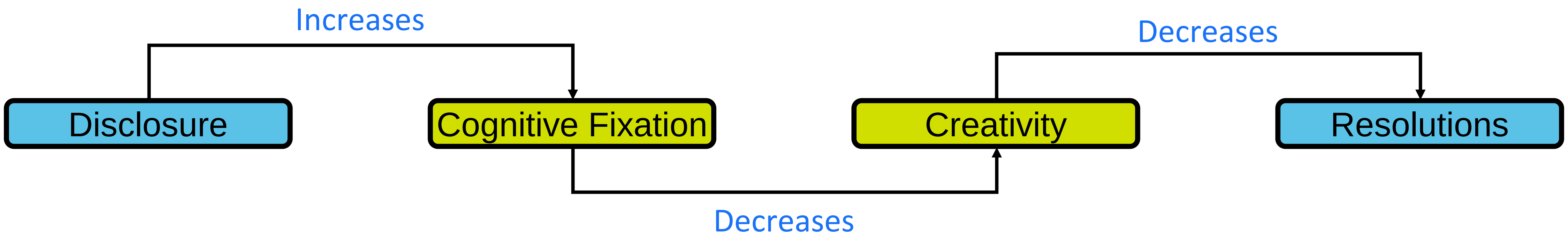
$$
\begin{aligned}
&LogResolutions_{it} \\
&\quad = \beta_1 CumulativeDisclosureFraction_{it-1} + \beta_2 LogCumulativeClosure_{it-1} \\
&\quad + \beta_3 LogCumulativeAverageBounty_{it-1} \\
&\quad + \beta_4 LogCumulativePlatformResolution_{it-1} \\
&\quad + \beta_5 LogCumulativePlatformDisclosureFraction_{it-1} + Firm_i + Month_t \\
&\quad + \varepsilon_{it} \qquad (1)
\end{aligned}
$$

where, *$Firm_i$ and $Month_t$* are fixed effects, capturing time-invariant firm and platform characteristics.

Results

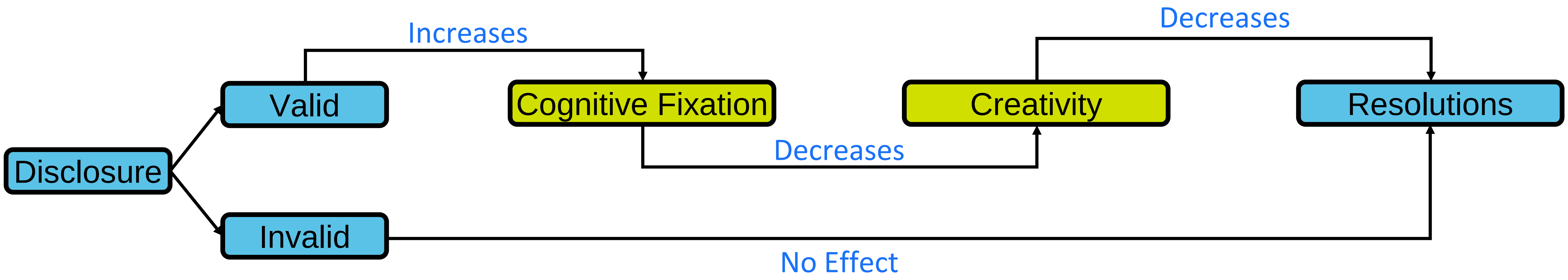
Main Findings

- Using multiple econometrics specifications, we found that past disclosures have a negative effect on the number of future resolutions.
- We also found that fewer hackers are likely to be successful if a firm increases its disclosure level.



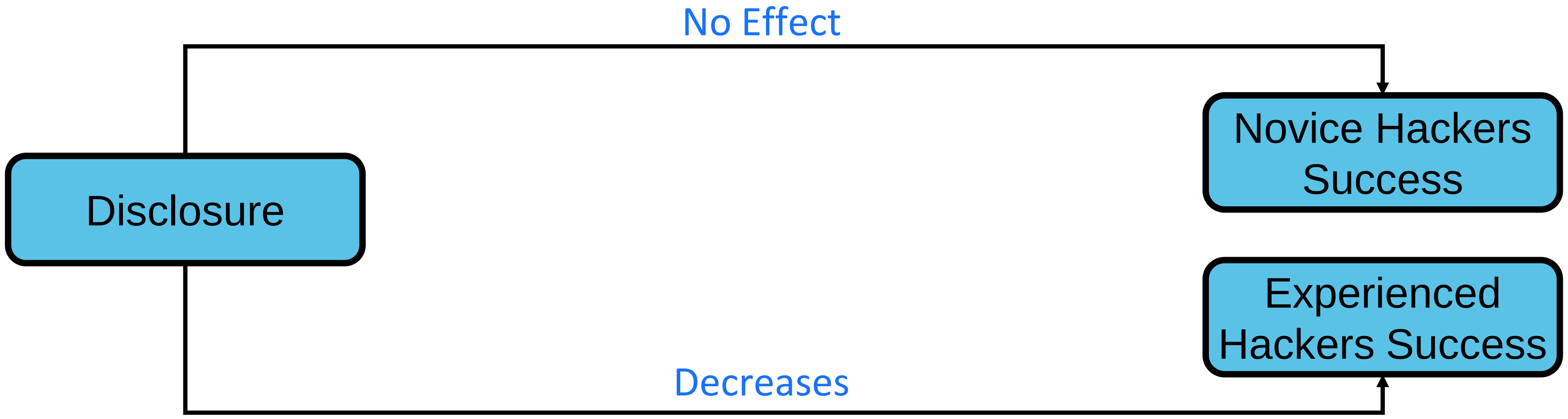
Different Types of Disclosure

- In our analysis, we have two types of Disclosures; Valid and Invalid Disclosures.
- The negative effects of disclosures mainly stem from valid disclosures, invalid disclosures have no effect.
- This suggests that hackers use valid disclosed information, which affects their ability.



Effect of Disclosure on Different Types of Hackers

- Fixation doesn't affect novice hackers.
- Disclosure has no effect on novice hackers
- Cognitive theories tell us that fixation affects experienced people more.
- Therefore, we found that experienced hackers are less likely to be successful due to disclosure.



Black Hat Sound Bytes

Key takeaways:

1. If organizations want hackers to find new vulnerabilities, they must limit their disclosures. If they want to disclose, invalid disclosures could be one possible way.
2. Hackers must use caution in accessing disclosed reports and must overcome cognitive fixation to discover new vulnerabilities.
3. One possible way to reduce fixation is by program switching. Continuously working on the same program could lead to more fixation.

- Ali Ahmed is an assistant professor in the Department of Information Systems of the College of Business at the University of Wisconsin – Eau Claire.
- He received his Ph.D. in Business Administration with a concentration in Management Information Systems from the University of Massachusetts Lowell.
- His research focuses on policy and the economics of information security.
- He has extensively studied bug bounty, vulnerability disclosure, and hackers' behavior on bug bounty platforms.
- Email: ahmeda@uwec.edu or ali_ahmed@student.uml.edu

Feel free to connect on LinkedIn