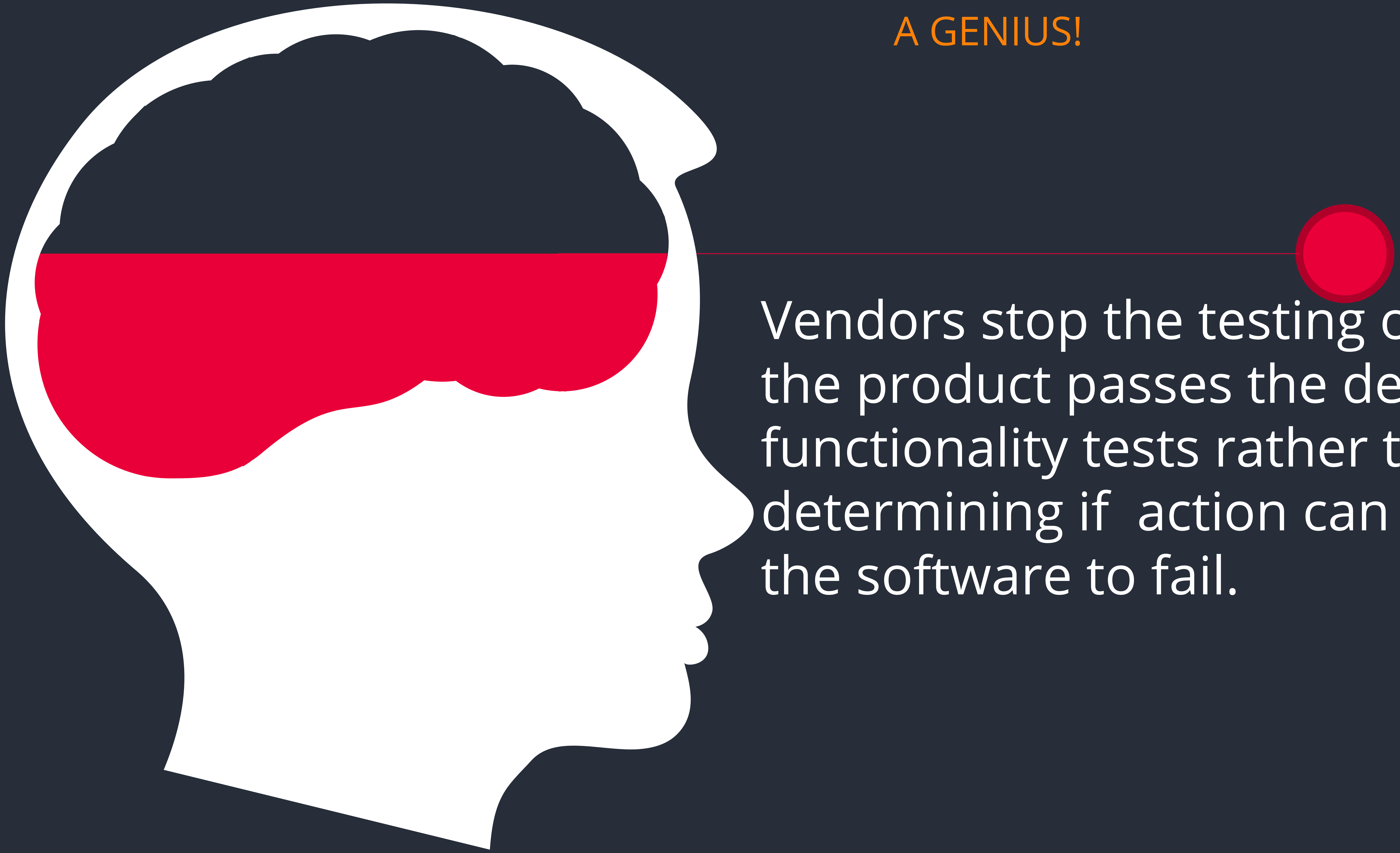
An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price

U

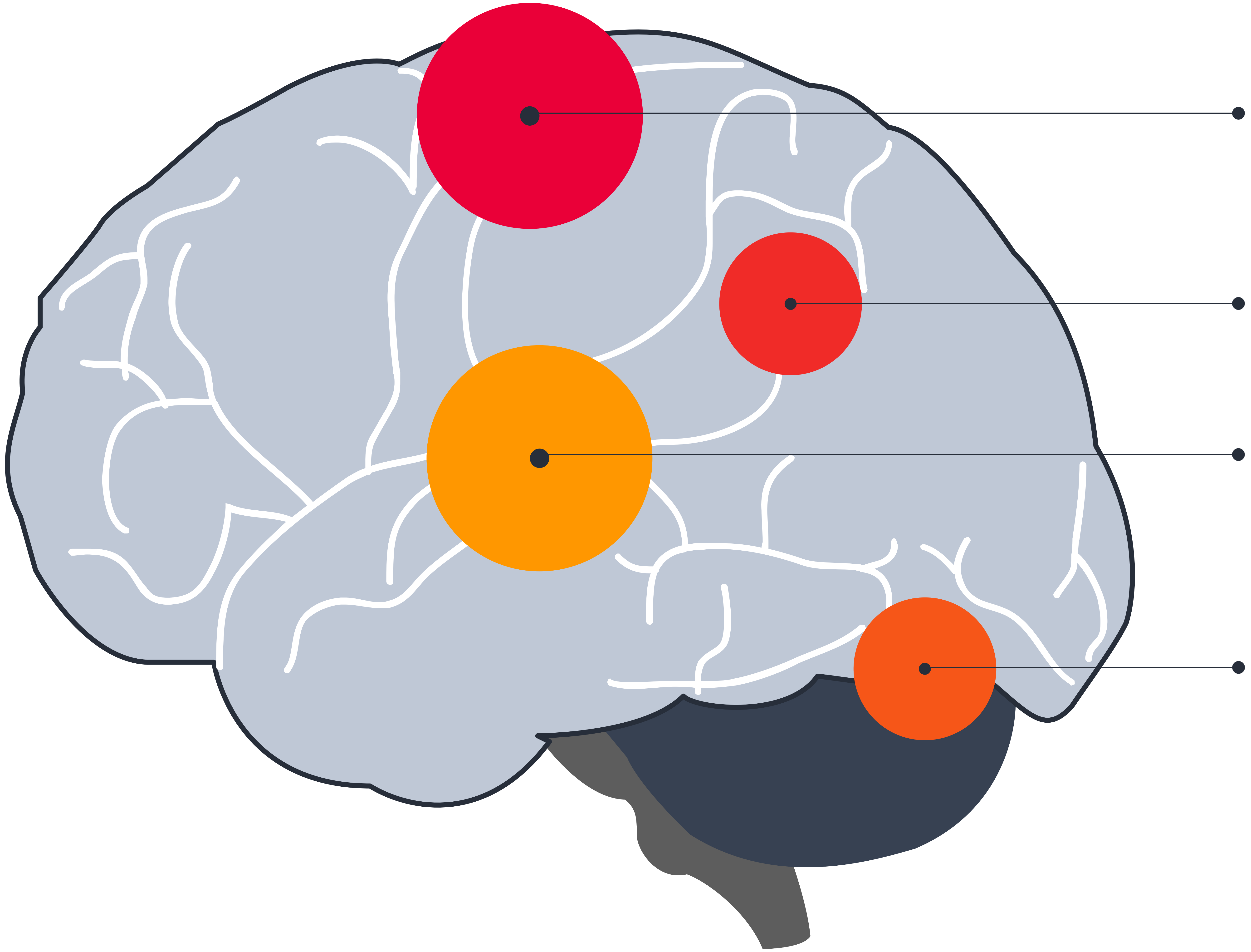
The people think that...

The market does not punish software vendors for defect into the software. There are no real consequences to the vendors for having bad security or low-quality software. Even worse, the marketplace often rewards low quality but additional features.

A GENIUS!



Vendors stop the testing once the product passes the desired functionality tests rather than determining if action can cause the software to fail.



BUREAUCRACY

LAWYERS

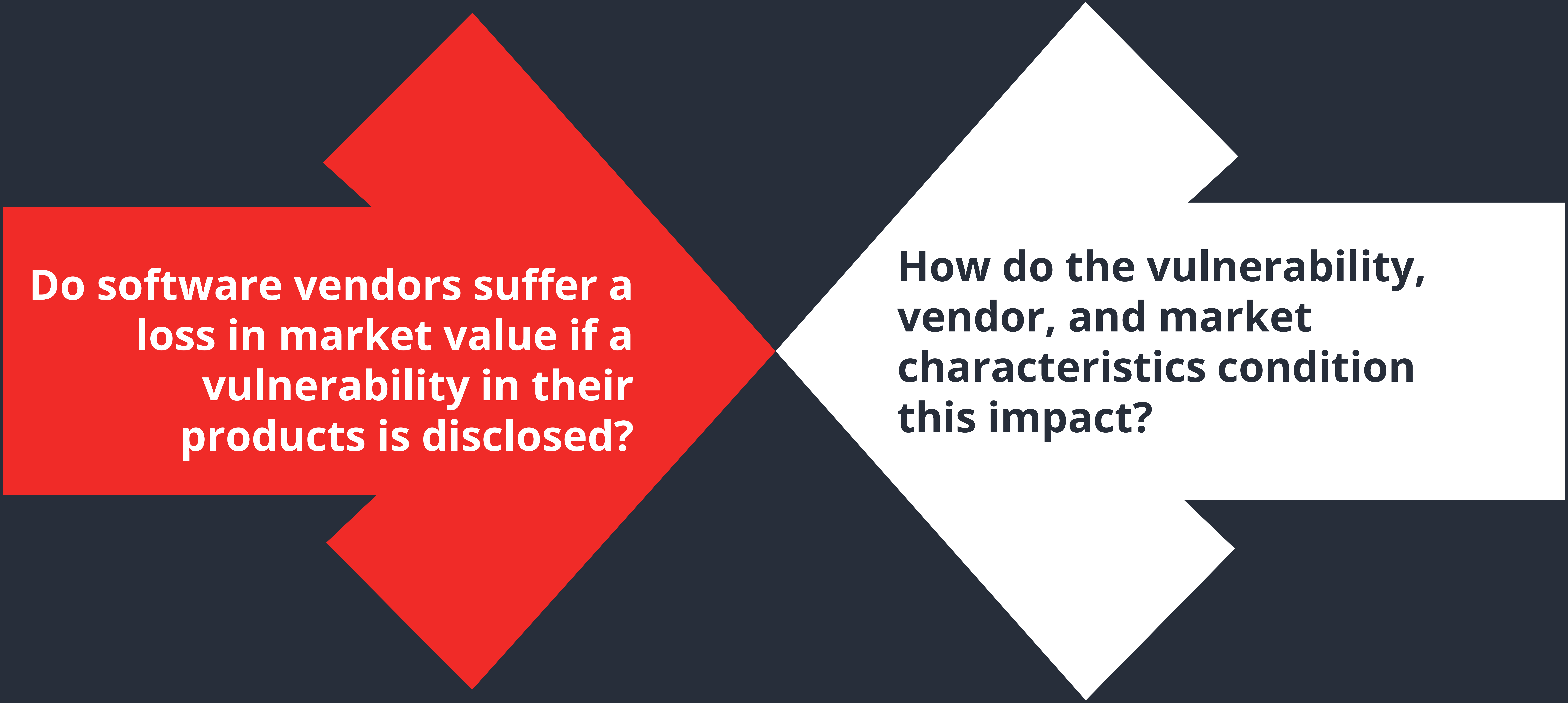
GHOST STATE

MONEY

THE LAW IS DIFFICULT!

Software products generally come with a click-wrap agreement which limits the vendors' responsability. For the law, the general philosophy is that software is a complex product that will probably have some defects

Questions



Do software vendors suffer a loss in market value if a vulnerability in their products is disclosed?

How do the vulnerability, vendor, and market characteristics condition this impact?

RESEARCH ANALYSIS

They collect data on 147 vulnerability disclosure announcements from industry over a period of more than five years.

Our results confirm that vulnerability disclosure

affects the stock performance of a software vendor.

They show that, on average, a software vendor loses around 0.63 percent of market value on the day of the vulnerability announcement.

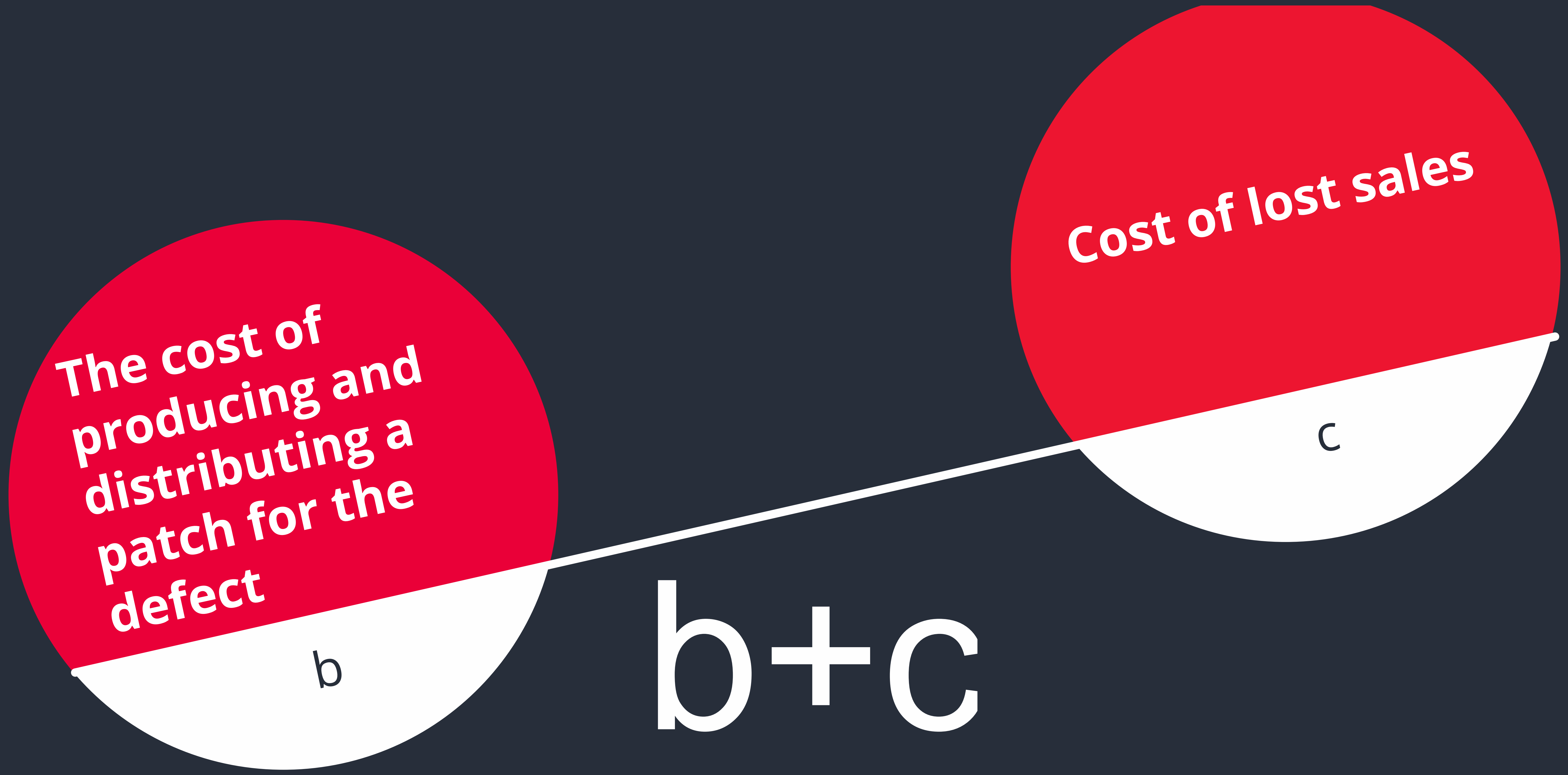
We also find that vulnerabilities disclosed without a patch have a more negative returns than those disclosed with a patch.

The cost of software defects to a vendor

two categories

b

The cost of fixing a system after release cost more than four to eight more times than normal fix. Microsoft spend a lot of money for security patch, but less compared to a firm’s market value



The cost of producing and distributing a patch for the defect

b

Cost of lost sales

c

b+c

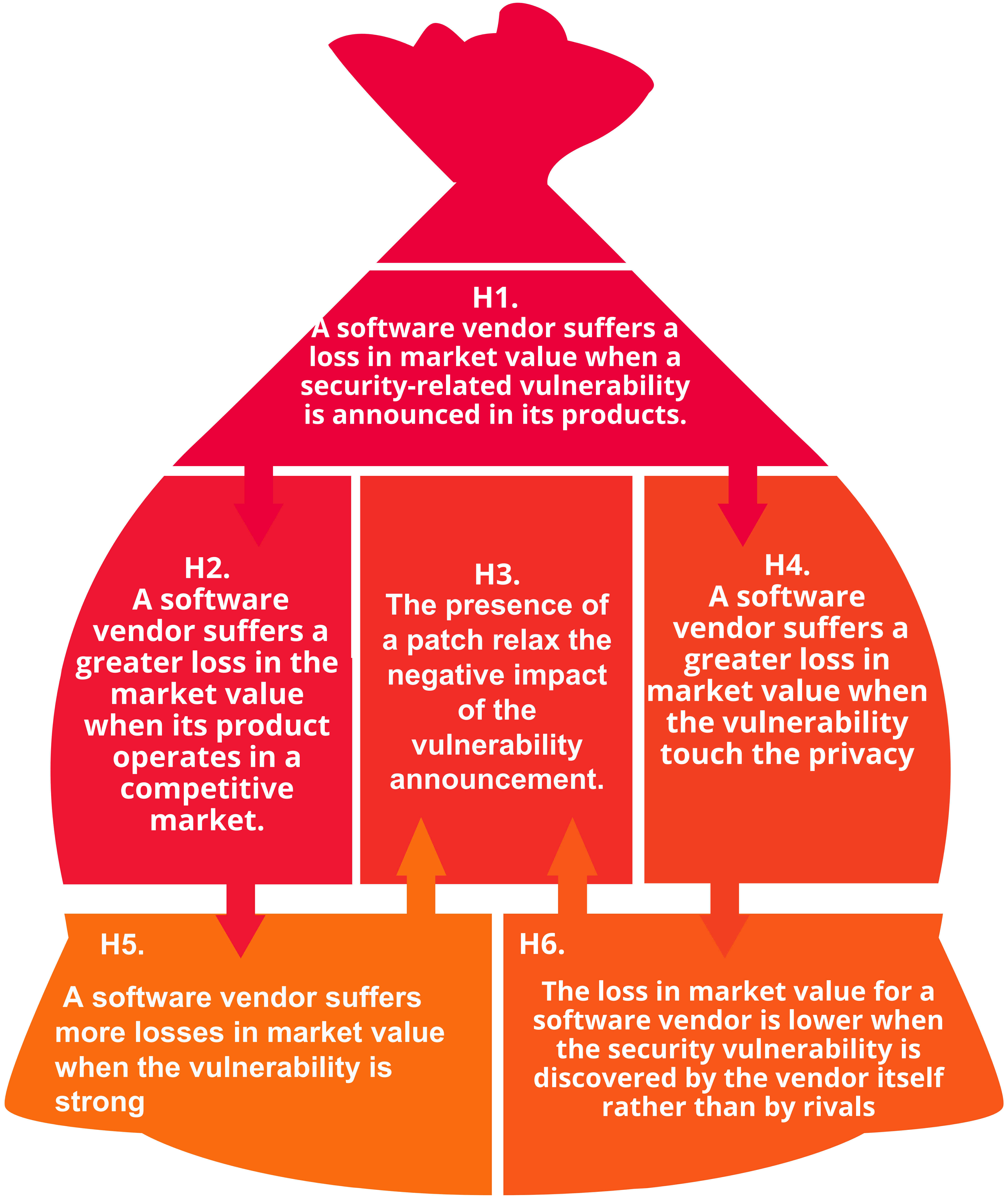
c

Cost of lost sales. Software vulnerabilities can lead to customer dissatisfaction, reputation loss, and, ultimately, to lost sales.

Hypothesis

H2. However, large firms are also diversified. Diversified firms have many product lines and the potential loss in revenues in one product may not impact the market value.

H4. DoS attacks are not associated with any significant loss in market value for a firm.



H1.
A software vendor suffers a loss in market value when a security-related vulnerability is announced in its products.

H2.
A software vendor suffers a greater loss in the market value when its product operates in a competitive market.

H3.
The presence of a patch relax the negative impact of the vulnerability announcement.

H4.
A software vendor suffers a greater loss in market value when the vulnerability touch the privacy

H5.

A software vendor suffers more losses in market value when the vulnerability is strong

H6.

The loss in market value for a software vendor is lower when the security vulnerability is discovered by the vendor itself rather than by rivals

DATA DESCRIPTION AND METHODOLOGY

The goal of this paper.

This article analyzes if software vulnerability impacts stock returns.

What is the stock?

The stock is the capital raised by a company or corporation through the issue and subscription of share.

This study focuses on 147 vulnerability announcements for 18 companies between January 1999 and May 2004. These announcements come from the popular press and CERT consulting departments.

The main media from which the sources were taken are: "the Wall Street Journal, the New York Times, the Washington Post and the Los Angeles Times".

The study does not focus on announcements related to companies that are not listed on the stock exchange and announcements that indicate protocol defects.

For example

For example, a flaw in the FTP protocol affects multiple vendors. The reason behind dropping this category is that the flaw exists in the software only because it follows a flawed protocol and not due to the vendor.

Methodology

For this analysis it was used the standard event-study methodology.
The event in our case is the announcement of the discovery vulnerability.

Event window

The period of interest for which we observe the event is known as the event window. In this study the event window is one day.

For two reasons:

1) A shorter event period permits a better estimation of the effects of information on stock prices since it reduces the possibility of other confounding factors not related to the announcement.

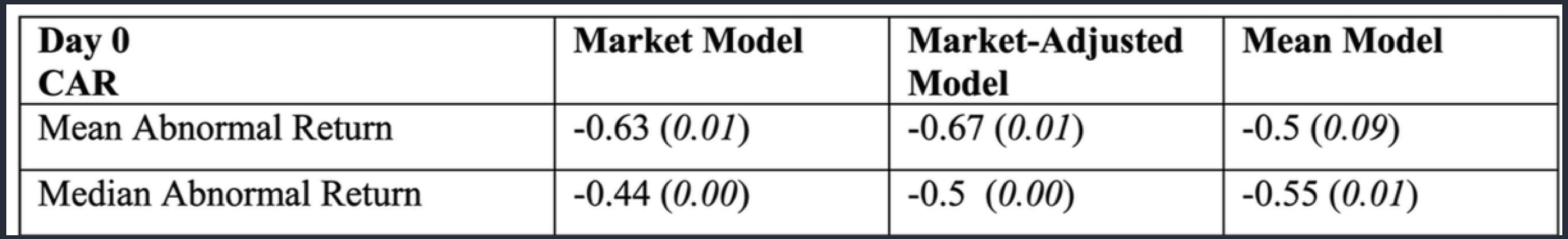
2) It also increases the power of the statistical tests.

Abnormal returns

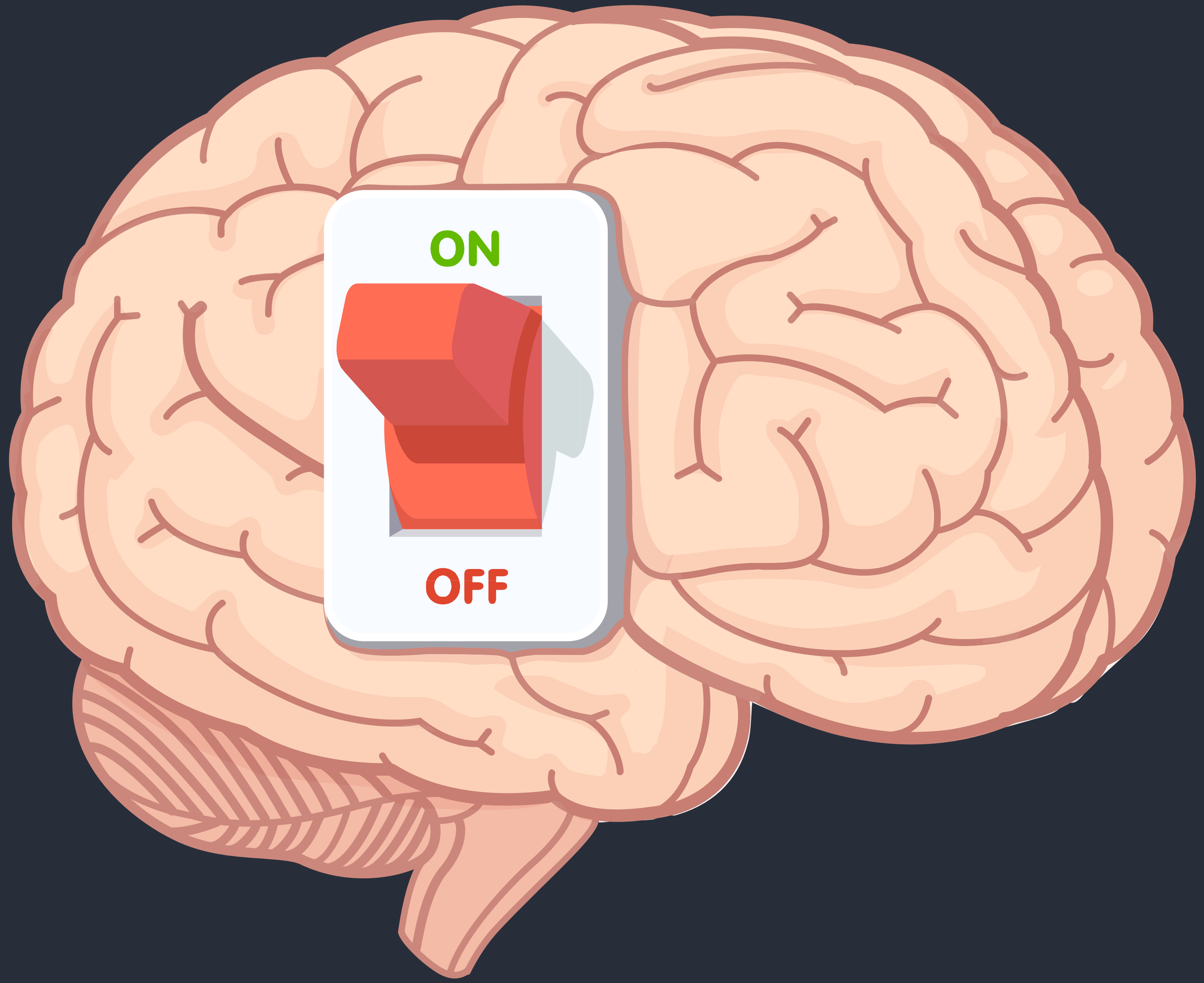
To satisfy the goal of this study they have to calculate the abnormal returns. Abnormal returns are defined as the difference between the actual return of the stock over the event window minus the expected return of the stock over the event window.

The expected return on the stock is calculated in several ways, in this analysis, it was used the market model, and verify this results using other methods, such as the market-adjusted method and the mean-adjusted method.

THE RESULT OF THE ABNORMAL RETURNS FOR THIS METHOD



Day 0 CAR	**Market Model**	**Market-Adjusted Model**	**Mean Model**
Mean Abnormal Return	-0.63 (*0.01*)	-0.67 (*0.01*)	-0.5 (*0.09*)
Median Abnormal Return	-0.44 (*0.00*)	-0.5 (*0.00*)	-0.55 (*0.01*)



At the end

Overall, the results suggest that software vendors lose market value when a vulnerability is announced in their product. This result is robust across various models and across various statistical tests.

REGRESSION ANALYSIS

Regression Analysis

$$AR_{it} = \beta X_i + \gamma Z_i + \varepsilon_i,$$

Regression Analysis

$$AR_{it} = \beta X_i + \gamma Z_i + \varepsilon_i,$$

- $i = 1 \ldots\ldots N\ is\ the\ total\ number\ of\ events$

Regression Analysis

$$AR_{it} = \beta X_i + \gamma Z_i + \varepsilon_i,$$

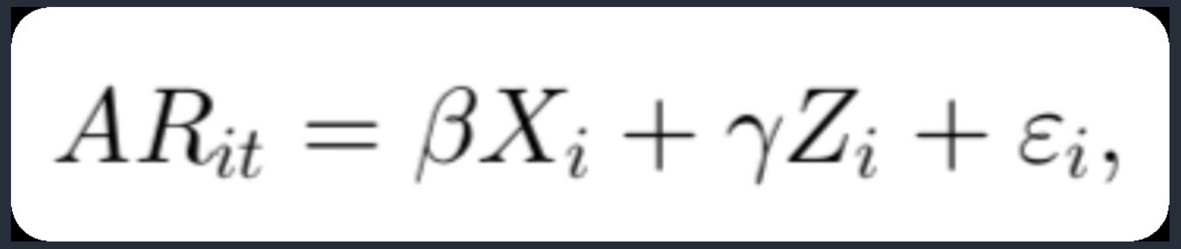
- $i = 1 \ldots\ldots N$ *is the total number of events*
- AR_{it} is the abnormal return for an event i

Regression Analysis

$$AR_{it} = \beta X_i + \gamma Z_i + \varepsilon_i,$$

- $i = 1 \ldots\ldots N\ is\ the\ total\ number\ of\ events$
- AR_{it} is the abnormal return for an event i
- ε is the prercentage of error

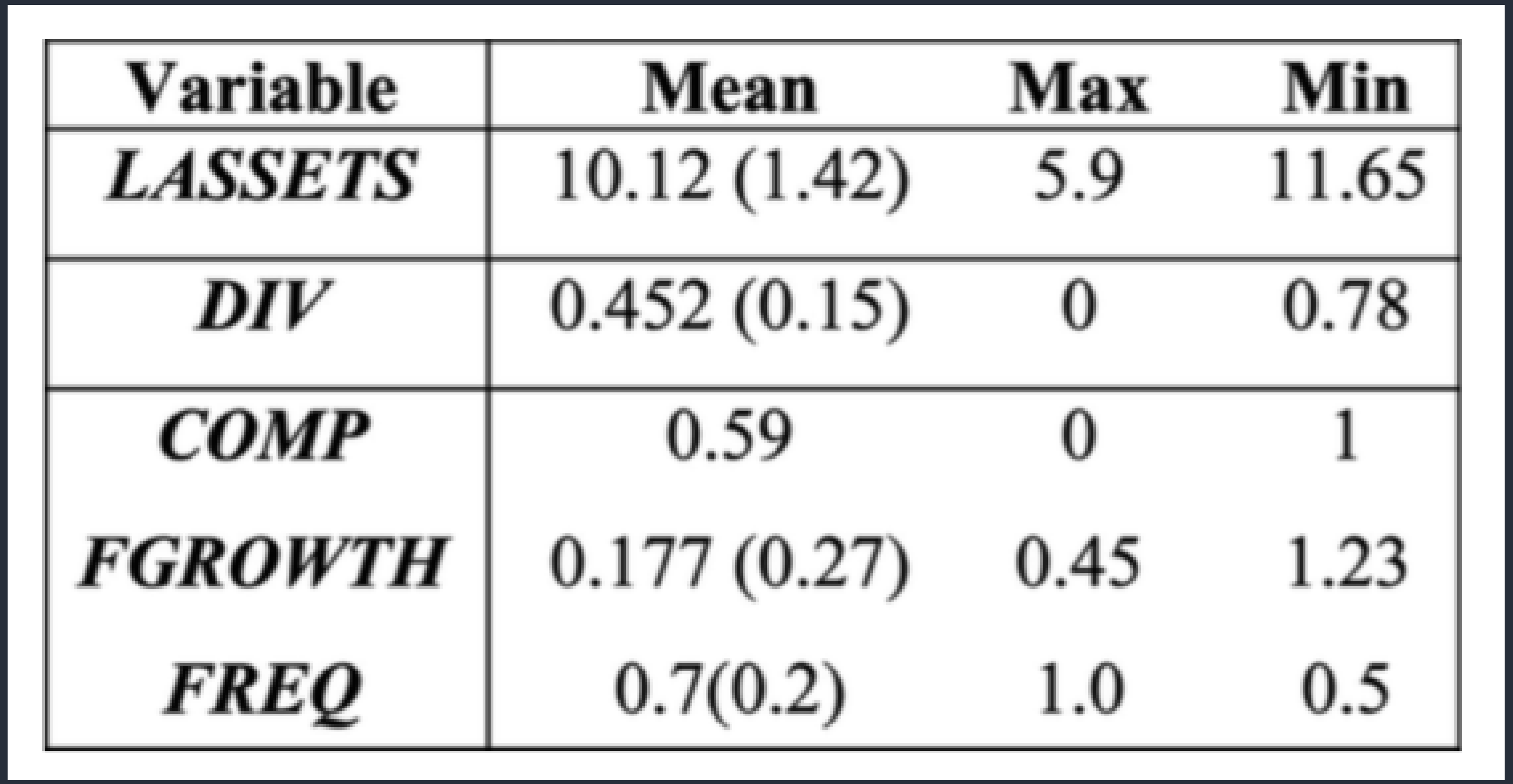
Regression Analysis



$$AR_{it} = \beta X_i + \gamma Z_i + \varepsilon_i,$$

- $i = 1 \ldots\ldots N\ is\ the\ total\ number\ of\ events$
- AR_{it} is the abnormal return for an event i
- ε is the prercentage of error
- X_j and Z_j are the indipendent variables that captures firm-specific and vulnerability specific for the event j

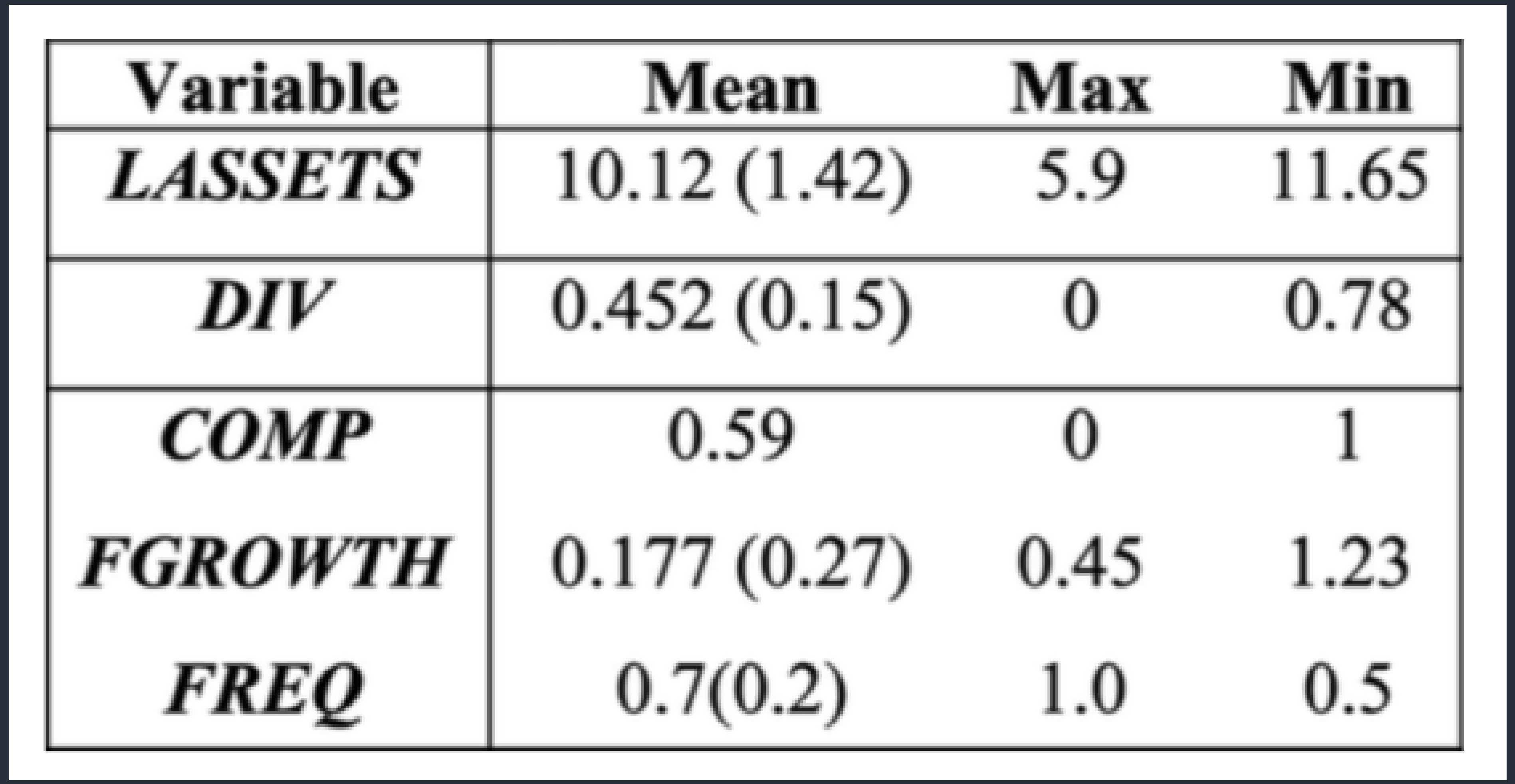
Firm-Specific Characteristics (X_j)



Variable	Mean	Max	Min
LASSETS	10.12 (1.42)	5.9	11.65
DIV	0.452 (0.15)	0	0.78
COMP	0.59	0	1
FGROWTH	0.177 (0.27)	0.45	1.23
FREQ	0.7(0.2)	1.0	0.5

- **LASSETS is the size of the firm (calculated with log k)**
  k= patrimony of the firm (in million of dollars)

Firm-Specific Characteristics (X_j)

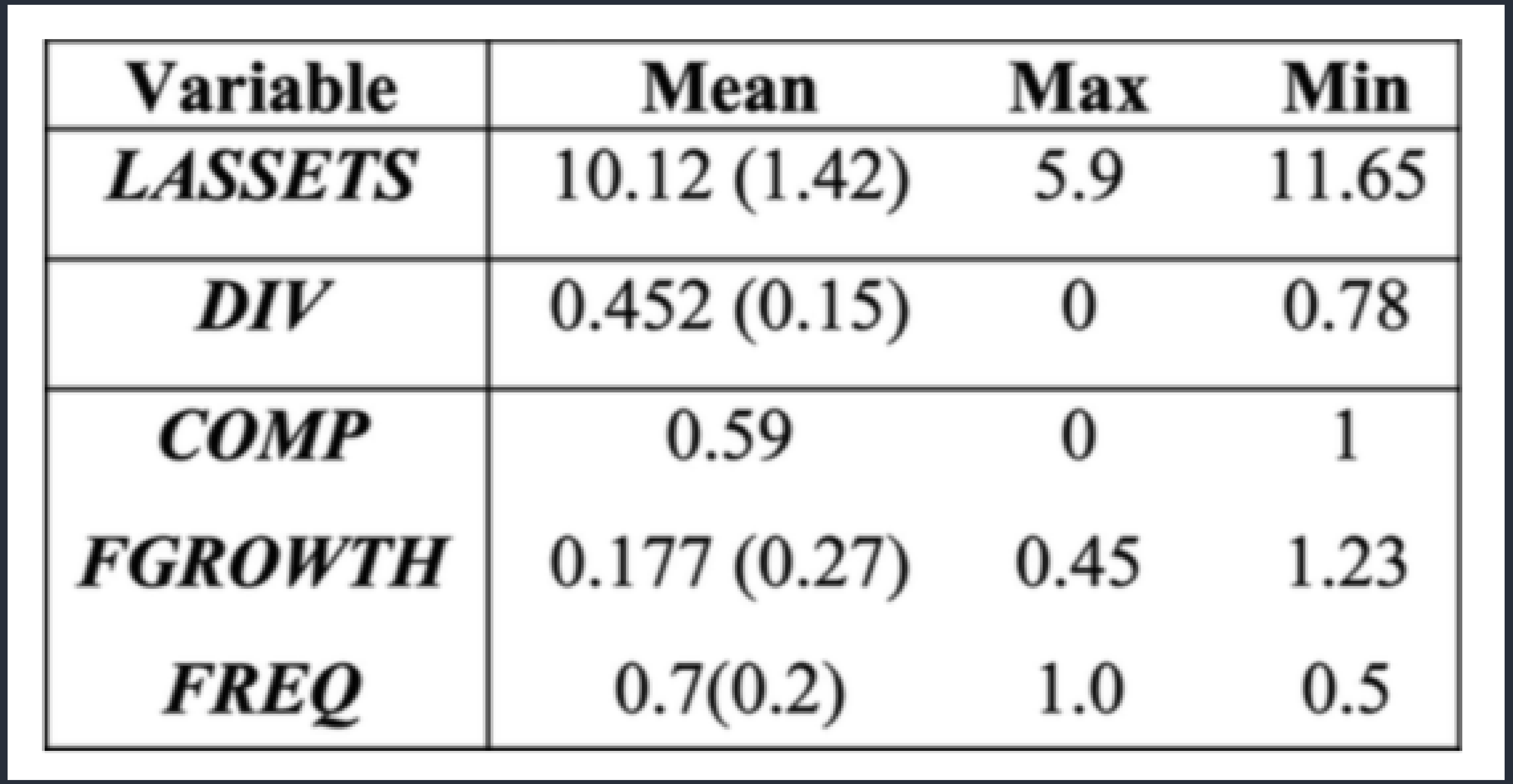


Variable	Mean	Max	Min
LASSETS	10.12 (1.42)	5.9	11.65
DIV	0.452 (0.15)	0	0.78
COMP	0.59	0	1
FGROWTH	0.177 (0.27)	0.45	1.23
FREQ	0.7(0.2)	1.0	0.5

- **LASSETS is the size of the firm (calculated with log k)**

  k= patrimony of the firm (in million of dollars)
- **DIV is the diversification, measured with the Herfindahl index**

Firm-Specific Characteristics (X_j)

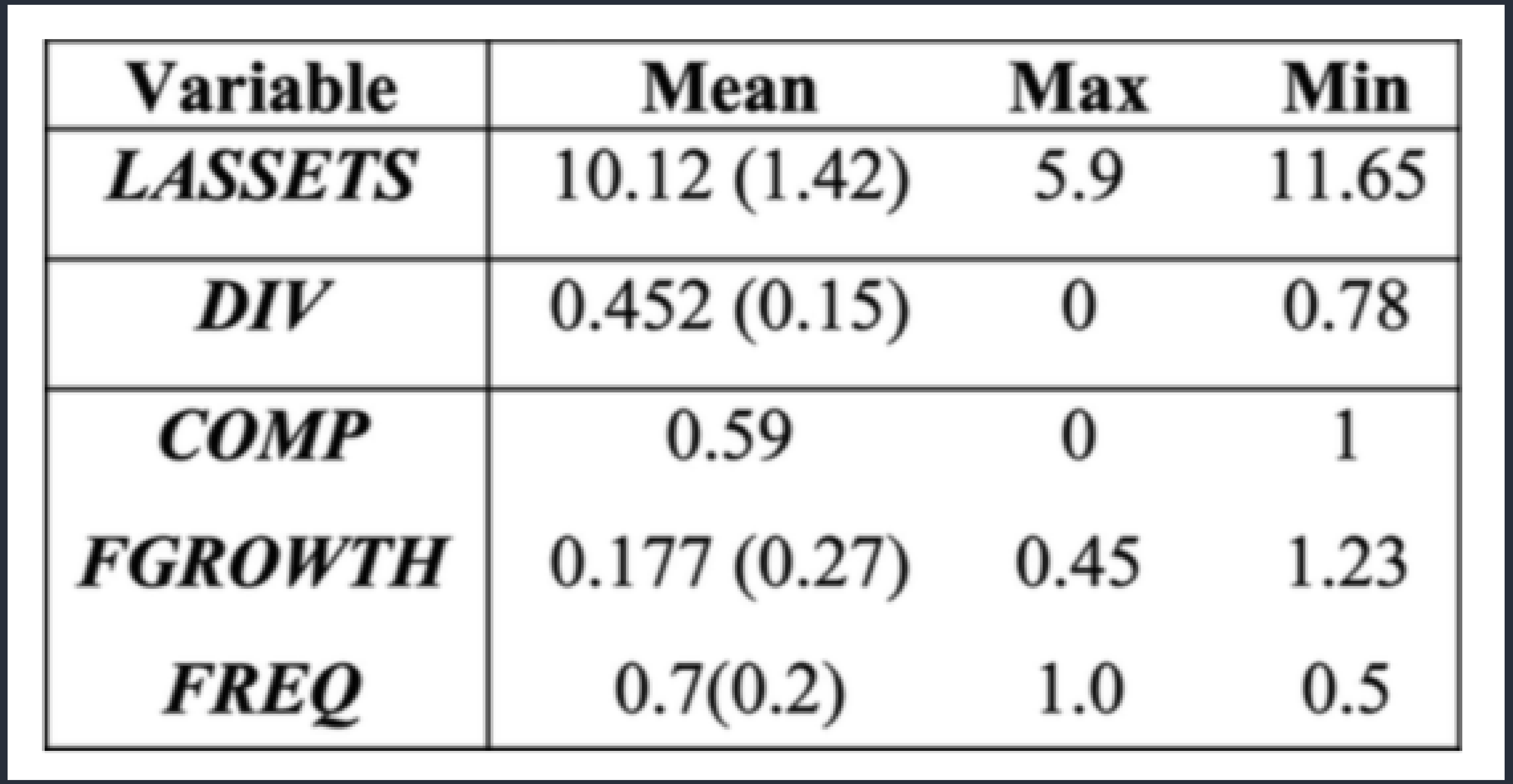


Variable	Mean	Max	Min
LASSETS	10.12 (1.42)	5.9	11.65
DIV	0.452 (0.15)	0	0.78
COMP	0.59	0	1
FGROWTH	0.177 (0.27)	0.45	1.23
FREQ	0.7(0.2)	1.0	0.5

- LASSETS is the size of the firm (calculated with log k)
  k= patrimony of the firm (in million of dollars)
- DIV is the diversification, measured with the Herfindahl index

$$H = \sum_{i=1}^{N} s_i^2$$

Firm-Specific Characteristics (X_j)

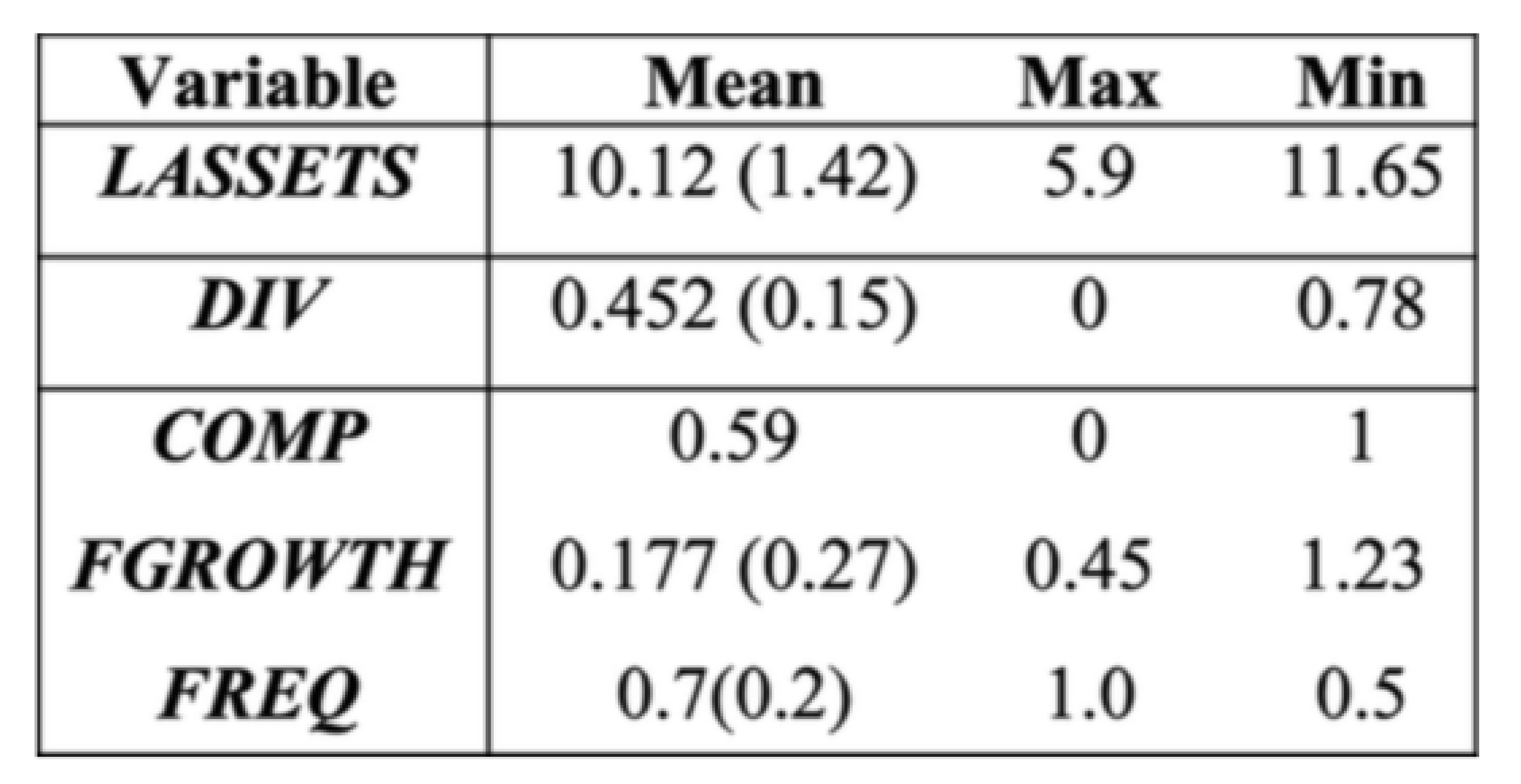


Variable	Mean	Max	Min
LASSETS	10.12 (1.42)	5.9	11.65
DIV	0.452 (0.15)	0	0.78
COMP	0.59	0	1
FGROWTH	0.177 (0.27)	0.45	1.23
FREQ	0.7(0.2)	1.0	0.5

- **LASSETS is the size of the firm (calculated with log k)**

  k= patrimony of the firm (in million of dollars)
- **DIV is the diversification, measured with the Herfindahl index**
- **COMP measures the market competition (binary)**

Firm-Specific Characteristics (X_j)



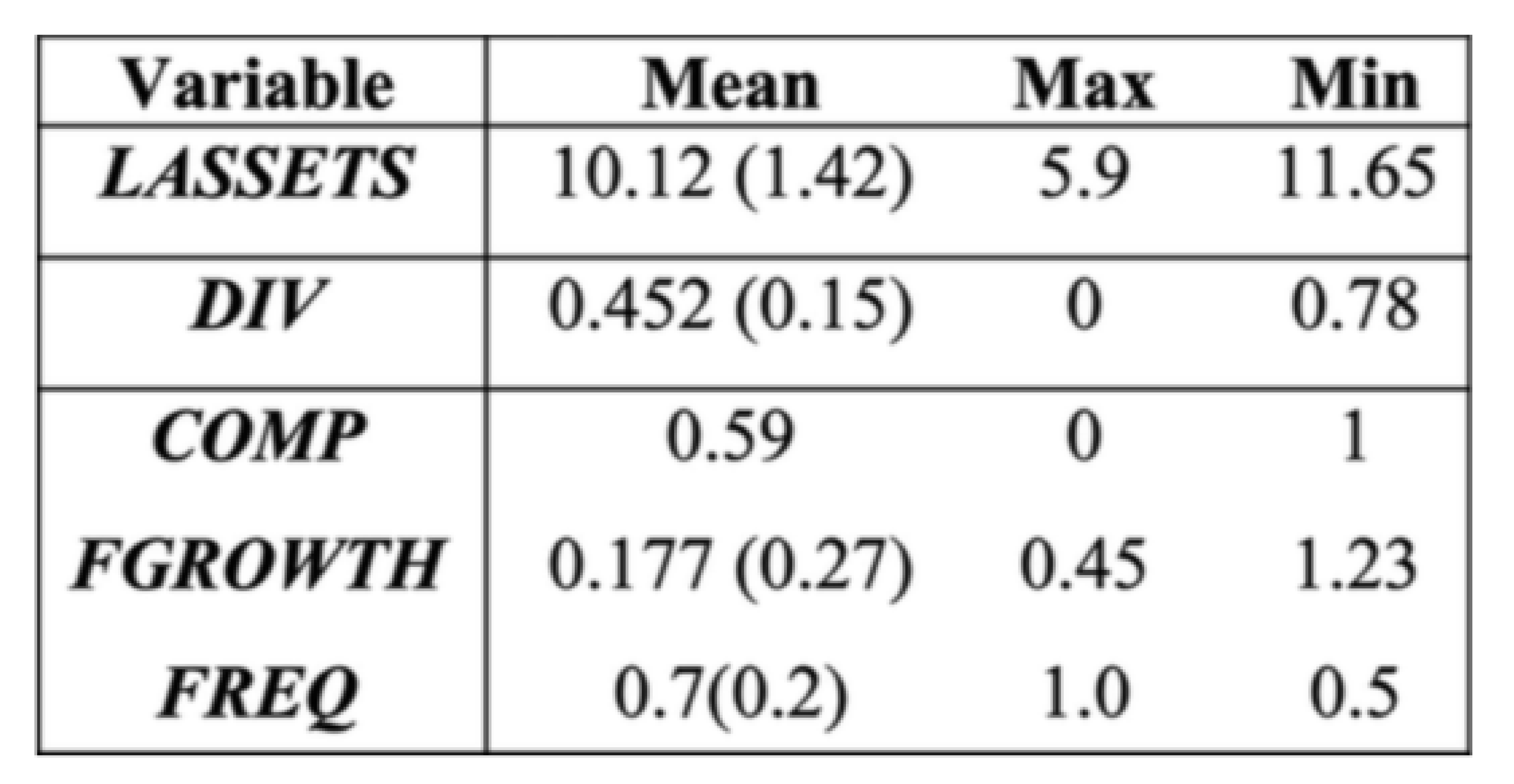
Variable	Mean	Max	Min
LASSETS	10.12 (1.42)	5.9	11.65
DIV	0.452 (0.15)	0	0.78
COMP	0.59	0	1
FGROWTH	0.177 (0.27)	0.45	1.23
FREQ	0.7(0.2)	1.0	0.5

- LASSETS is the size of the firm (calculated with log k)
  k= patrimony of the firm (in million of dollars)
- DIV is the diversification, measured with the Herfindahl index
- COMP measures the market competition (binary)

1 = COMPETITORS

0 = MONOPOLY

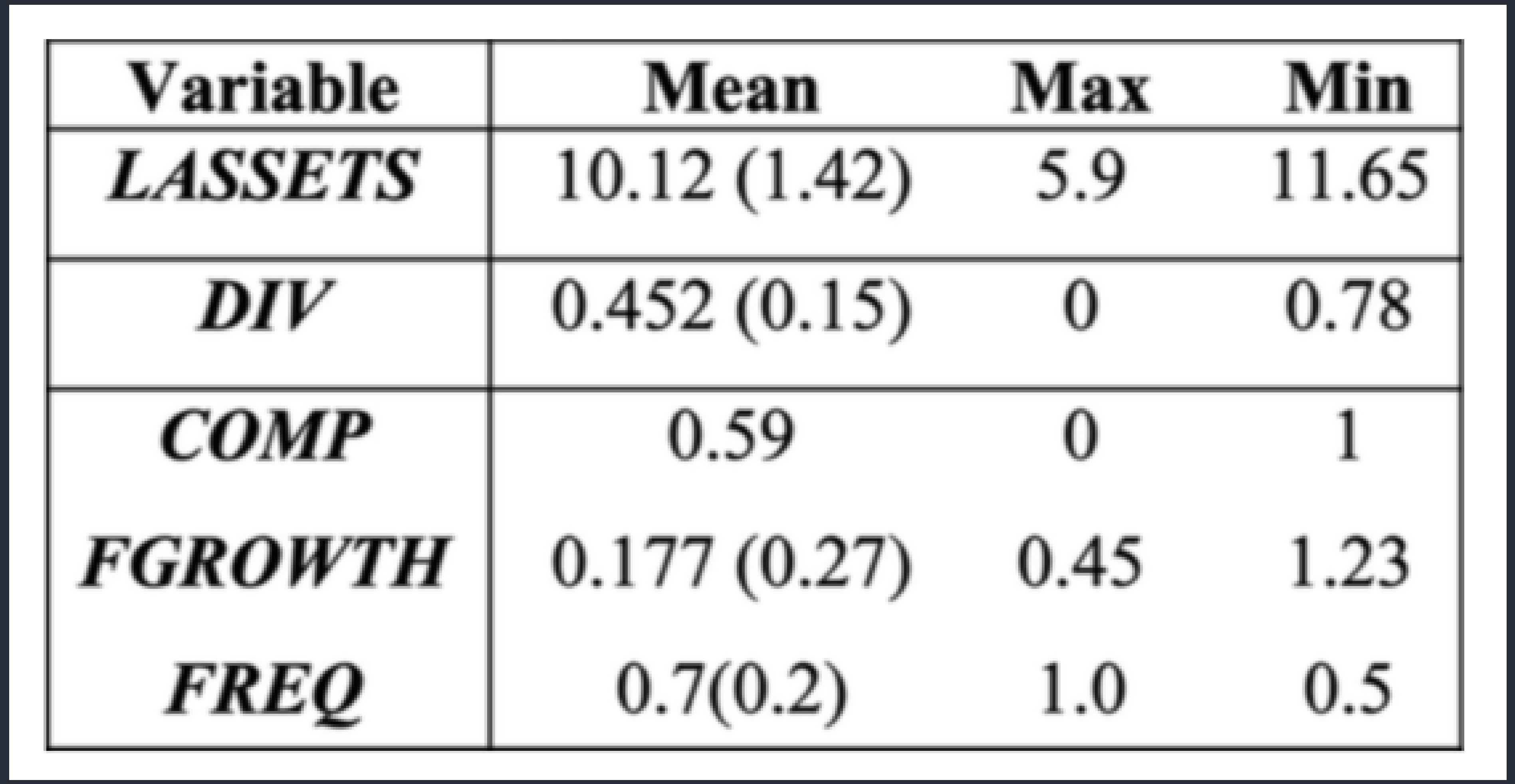
Firm-Specific Characteristics (X_j)



Variable	Mean	Max	Min
LASSETS	10.12 (1.42)	5.9	11.65
DIV	0.452 (0.15)	0	0.78
COMP	0.59	0	1
FGROWTH	0.177 (0.27)	0.45	1.23
FREQ	0.7(0.2)	1.0	0.5

- **LASSETS is the size of the firm (calculated with log k)**
  k= patrimony of the firm (in million of dollars)
- **DIV is the diversification, measured with the Herfindahl index**
- **COMP measures the market competition (binary)**
- **FGROWTH rate is measured as a percentage of the alteration of the firm revenues compared to the prevous year**

Firm-Specific Characteristics (X_j)



Variable	Mean	Max	Min
LASSETS	10.12 (1.42)	5.9	11.65
DIV	0.452 (0.15)	0	0.78
COMP	0.59	0	1
FGROWTH	0.177 (0.27)	0.45	1.23
FREQ	0.7(0.2)	1.0	0.5

- **LASSETS is the size of the firm (calculated with log k)**
  k= patrimony of the firm (in million of dollars)
- **DIV is the diversification, measured with the Herfindahl index**
- **COMP measures the market competition (binary)**
- **FGROWTH rate is measured as a percentage of the alteration of the firm revenues compared to the prevous year**
- **FREQ is the number of report about the vulnerability in the previous 12 month (FREQ= $1/(1+e^n)$)**

Vulnerability-Specific Characteristics (Z_j)

- PATCH is 1 if the patch is available (annuncement date)

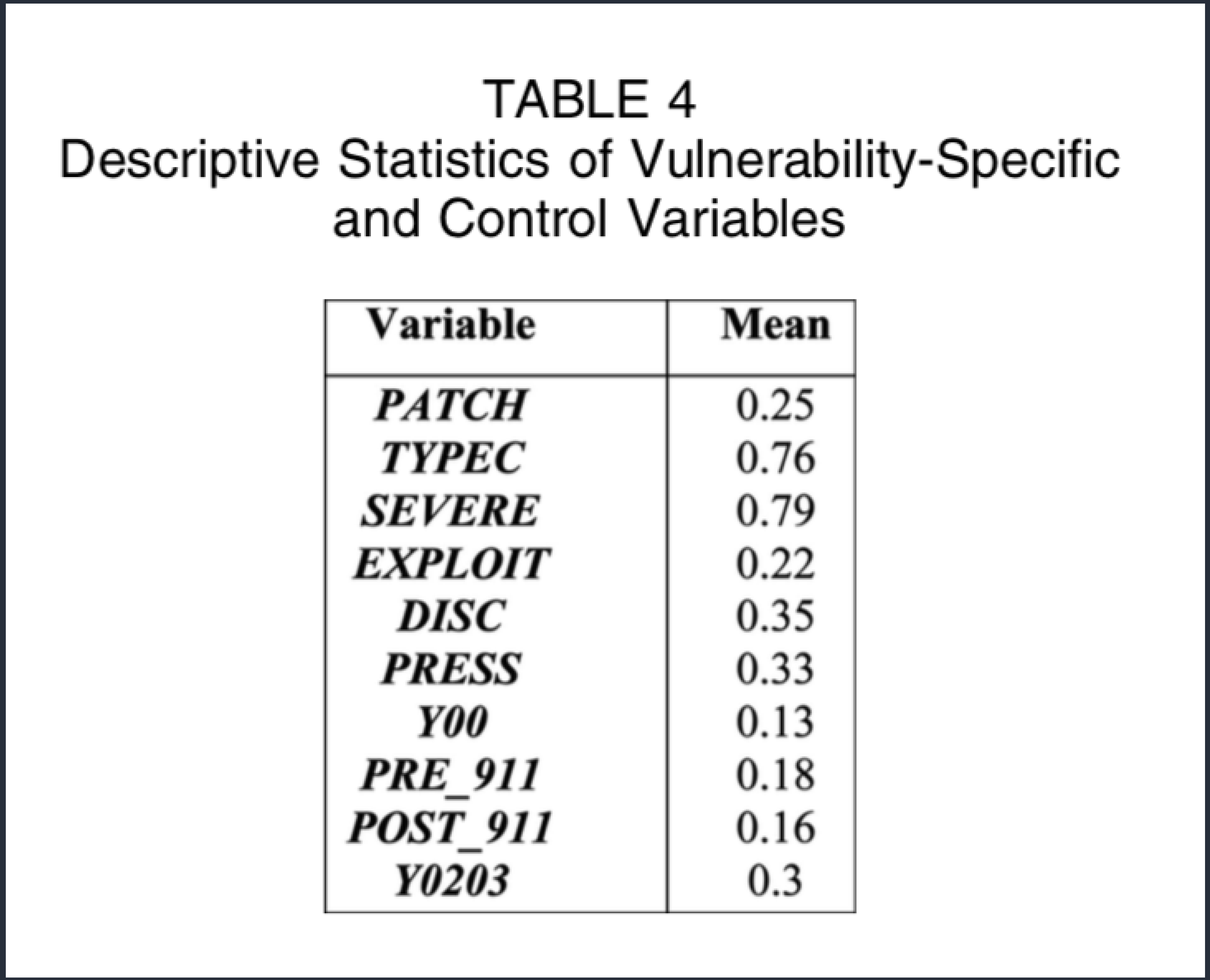


TABLE 4
Descriptive Statistics of Vulnerability-Specific and Control Variables

Variable	Mean
PATCH	0.25
TYPEC	0.76
SEVERE	0.79
EXPLOIT	0.22
DISC	0.35
PRESS	0.33
Y00	0.13
PRE_911	0.18
POST_911	0.16
Y0203	0.3

Vulnerability-Specific Characteristics (Z_j)

- PATCH is 1 if the patch is available (annuncement date)
- TYPEC is 1 if the vulnerability can allow potential intruders to steal private information

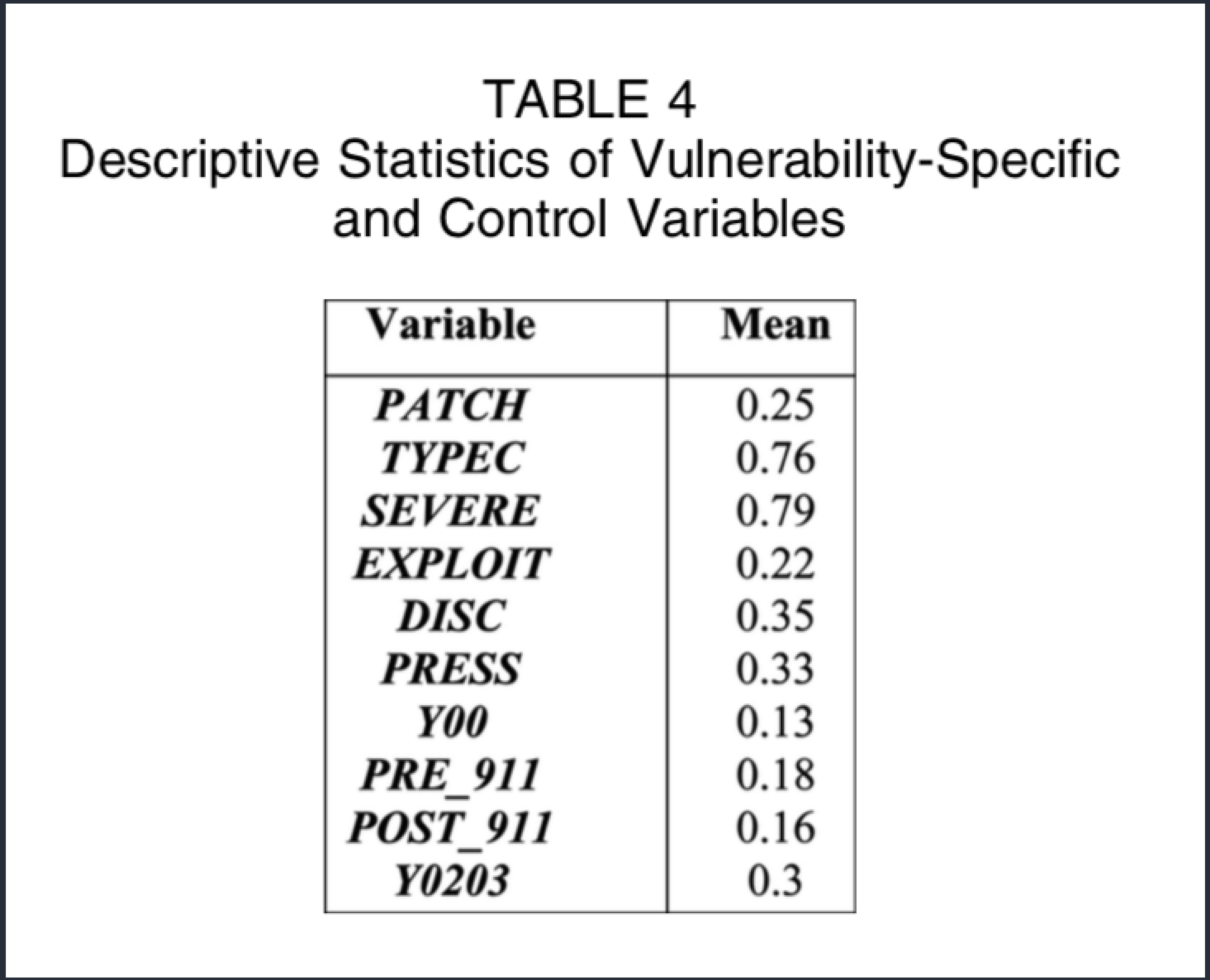


TABLE 4
Descriptive Statistics of Vulnerability-Specific and Control Variables

Variable	Mean
PATCH	0.25
TYPEC	0.76
SEVERE	0.79
EXPLOIT	0.22
DISC	0.35
PRESS	0.33
Y00	0.13
PRE_911	0.18
POST_911	0.16
Y0203	0.3

Vulnerability-Specific Characteristics (Z_j)

- PATCH is 1 if the patch is available (annuncement date)
- TYPEC is 1 if the vulnerability can allow potential intruders to steal private information
- SEVERE is 1 if the severity of the vulnerability is categorized as serious

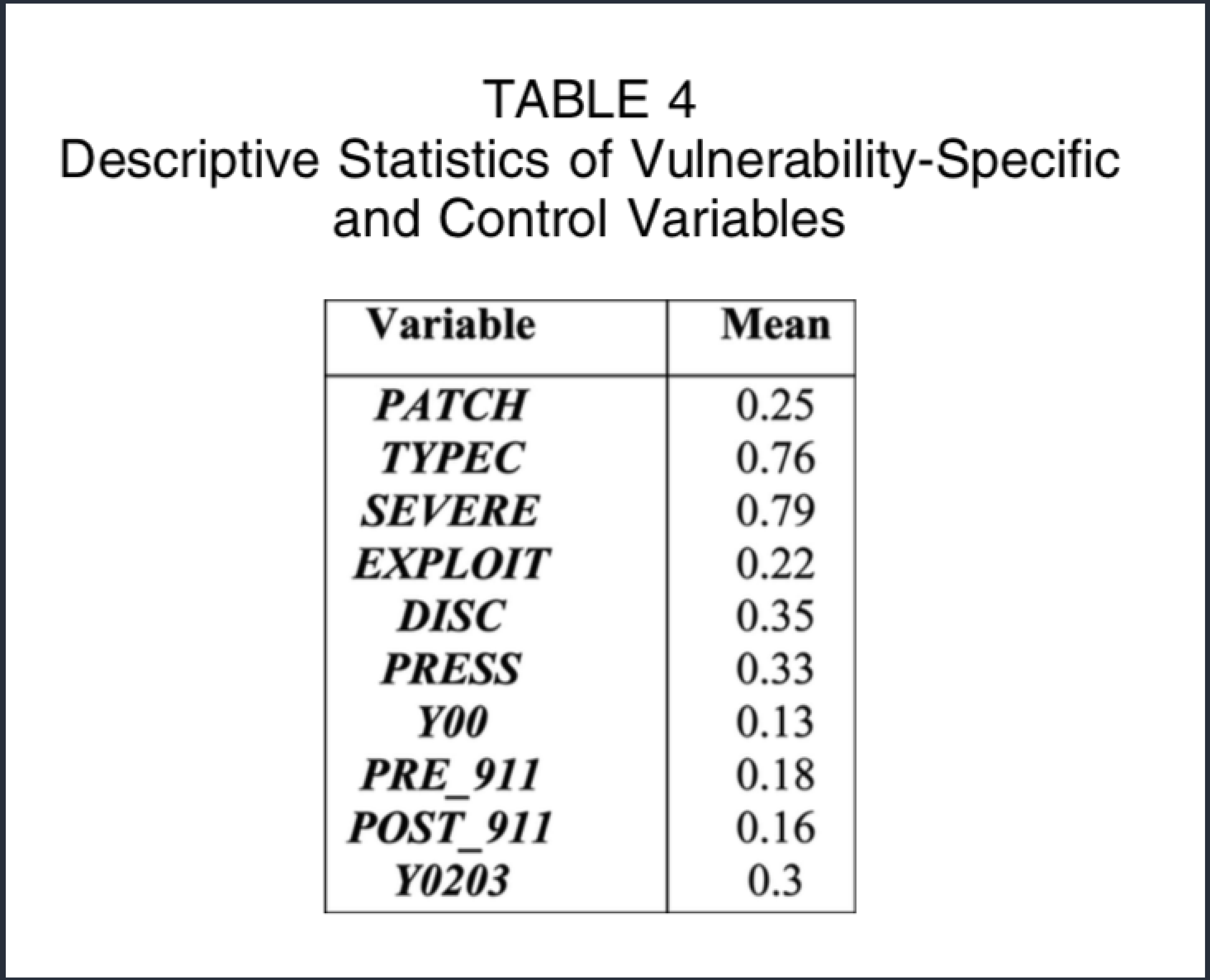


TABLE 4
Descriptive Statistics of Vulnerability-Specific and Control Variables

Variable	Mean
PATCH	0.25
TYPEC	0.76
SEVERE	0.79
EXPLOIT	0.22
DISC	0.35
PRESS	0.33
Y00	0.13
PRE_911	0.18
POST_911	0.16
Y0203	0.3

Vulnerability-Specific Characteristics (Z_j)

- PATCH is 1 if the patch is available (annuncement date)
- TYPEC is 1 if the vulnerability can allow potential intruders to steal private information
- SEVERE is 1 if the severity of the vulnerability is categorized as serious
- EXPLOIT is 1 if an exploit is circulating

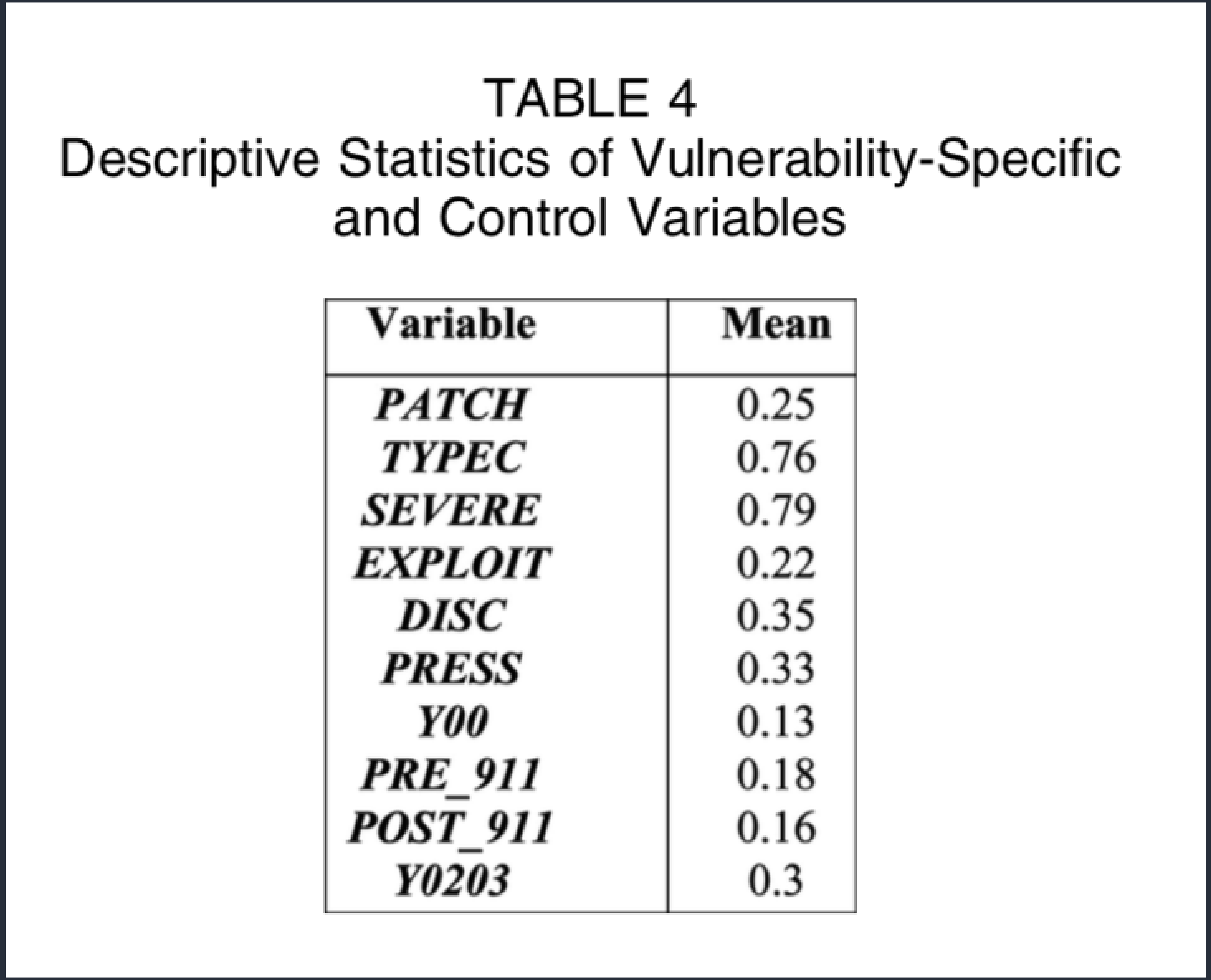


TABLE 4
Descriptive Statistics of Vulnerability-Specific and Control Variables

Variable	Mean
PATCH	0.25
TYPEC	0.76
SEVERE	0.79
EXPLOIT	0.22
DISC	0.35
PRESS	0.33
Y00	0.13
PRE_911	0.18
POST_911	0.16
Y0203	0.3

Vulnerability-Specific Characteristics (Z_j)

- PATCH is 1 if the patch is available (annuncement date)
- TYPEC is 1 if the vulnerability can allow potential intruders to steal private information
- SEVERE is 1 if the severity of the vulnerability is categorized as serious
- EXPLOIT is 1 if an exploit is circulating
- DISC is 1 if the firm discovered the vulnerability or 0 if the vulnerability has been discovered by someone else

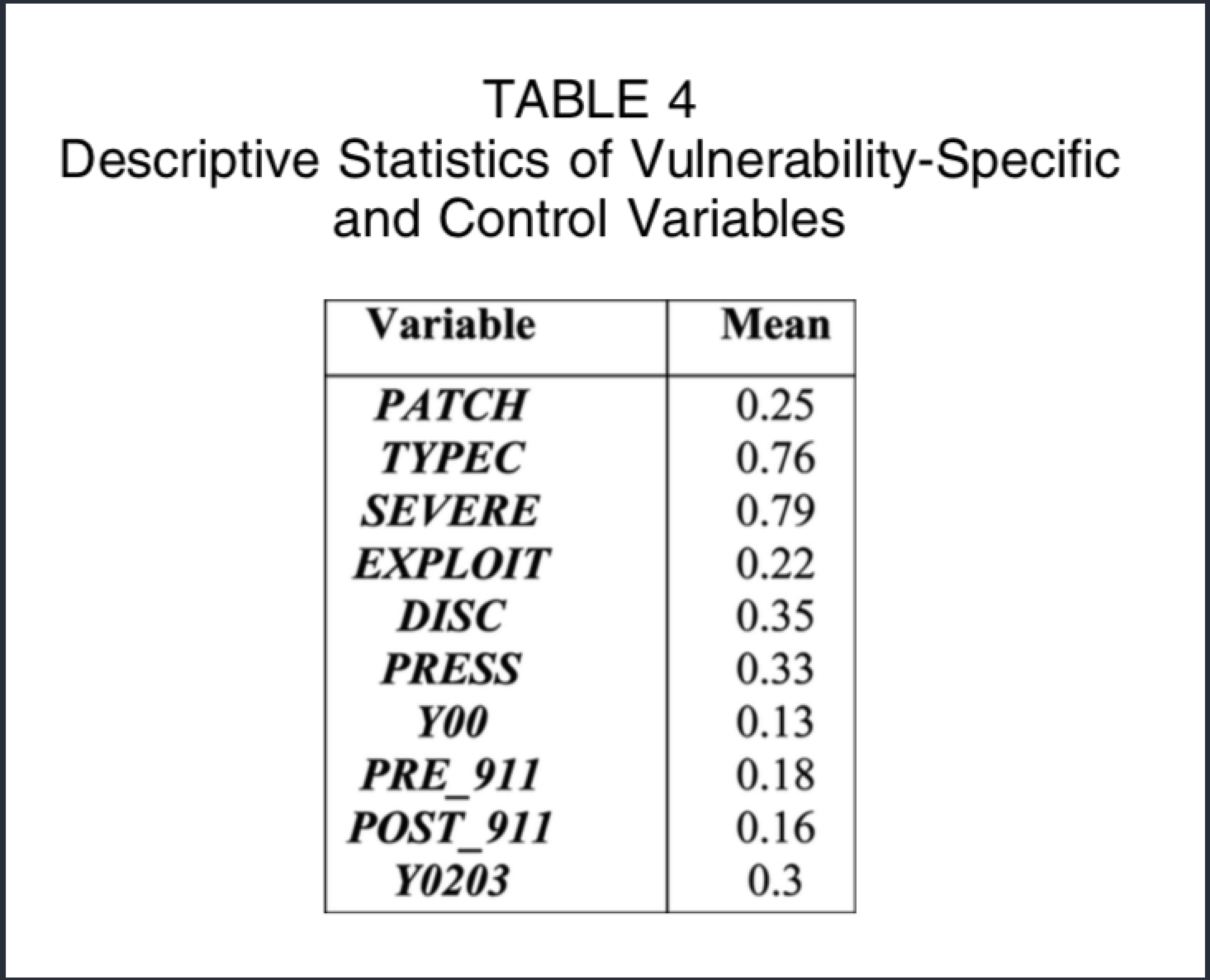


TABLE 4
Descriptive Statistics of Vulnerability-Specific and Control Variables

Variable	**Mean**
PATCH	0.25
TYPEC	0.76
SEVERE	0.79
EXPLOIT	0.22
DISC	0.35
PRESS	0.33
Y00	0.13
PRE_911	0.18
POST_911	0.16
Y0203	0.3

Control Variables (Z_j)

- PRESS is 1 if the vulnerability was annunced by the public press, or 0 if was annunced by industry sources

- DATE VARIABLES:

  - PRE AND POST 9/11
  - STRONG MARKET CRASH OF THE 2000 AND 2003

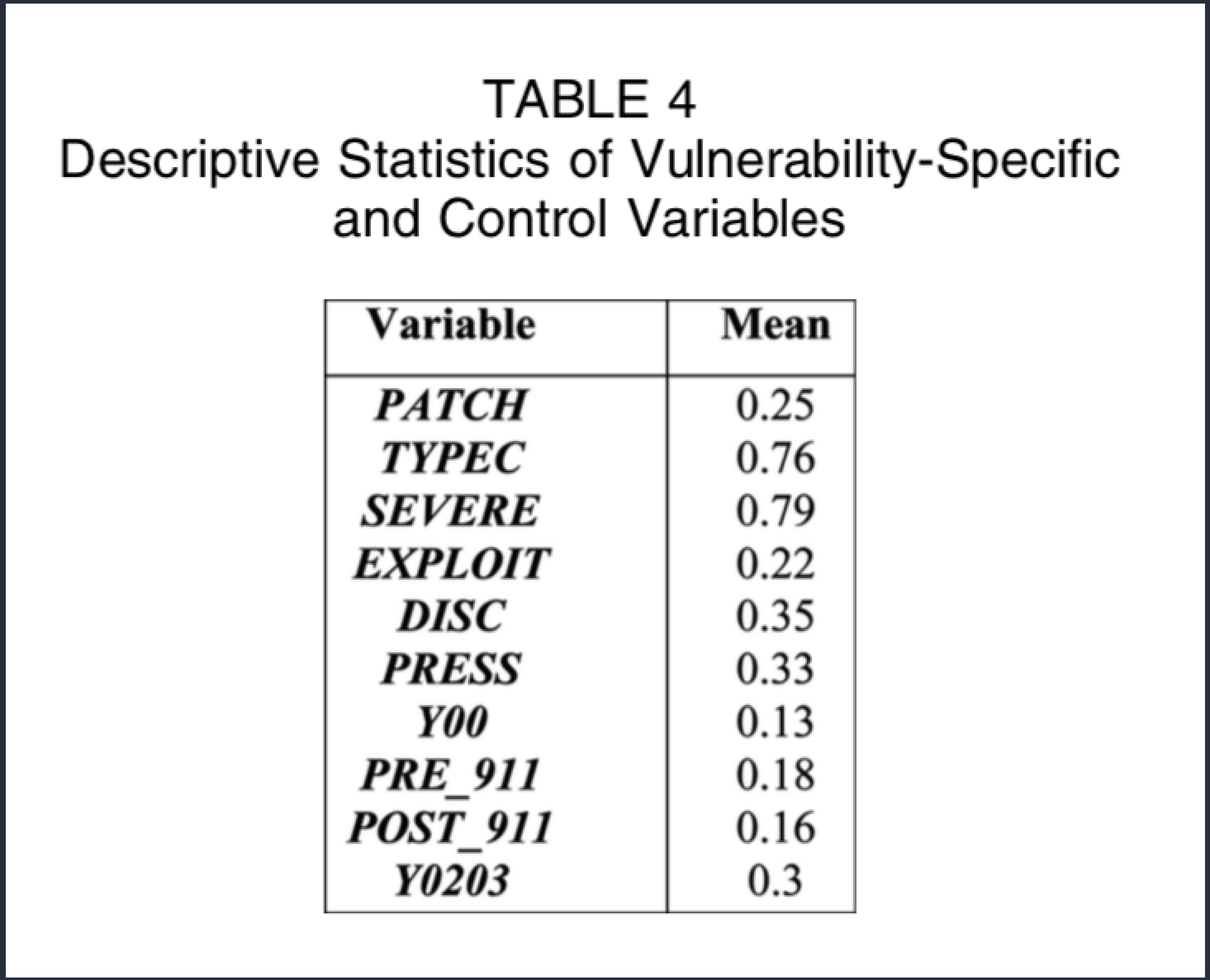
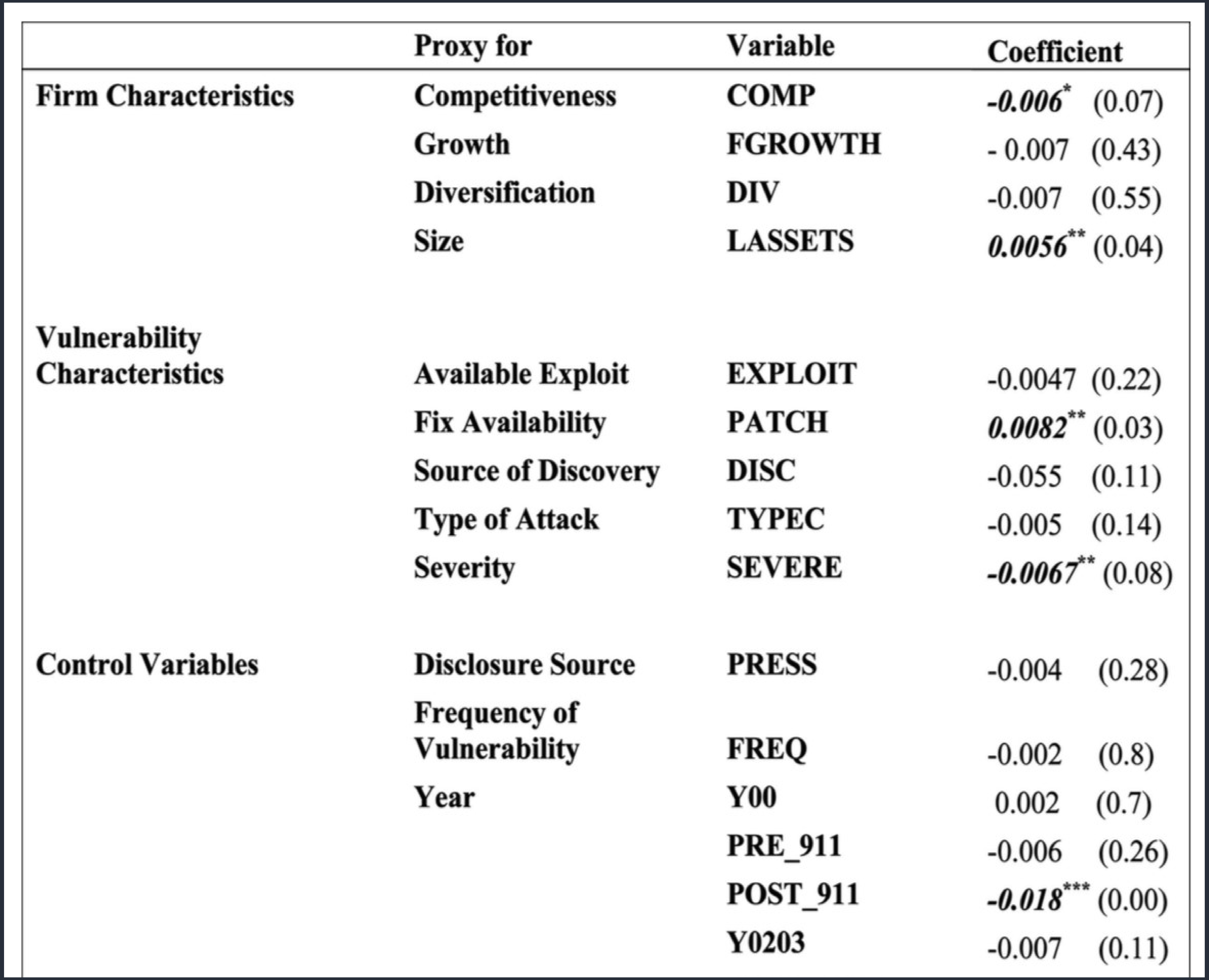


TABLE 4
Descriptive Statistics of Vulnerability-Specific and Control Variables

Variable	Mean
PATCH	0.25
TYPEC	0.76
SEVERE	0.79
EXPLOIT	0.22
DISC	0.35
PRESS	0.33
Y00	0.13
PRE_911	0.18
POST_911	0.16
Y0203	0.3

Results

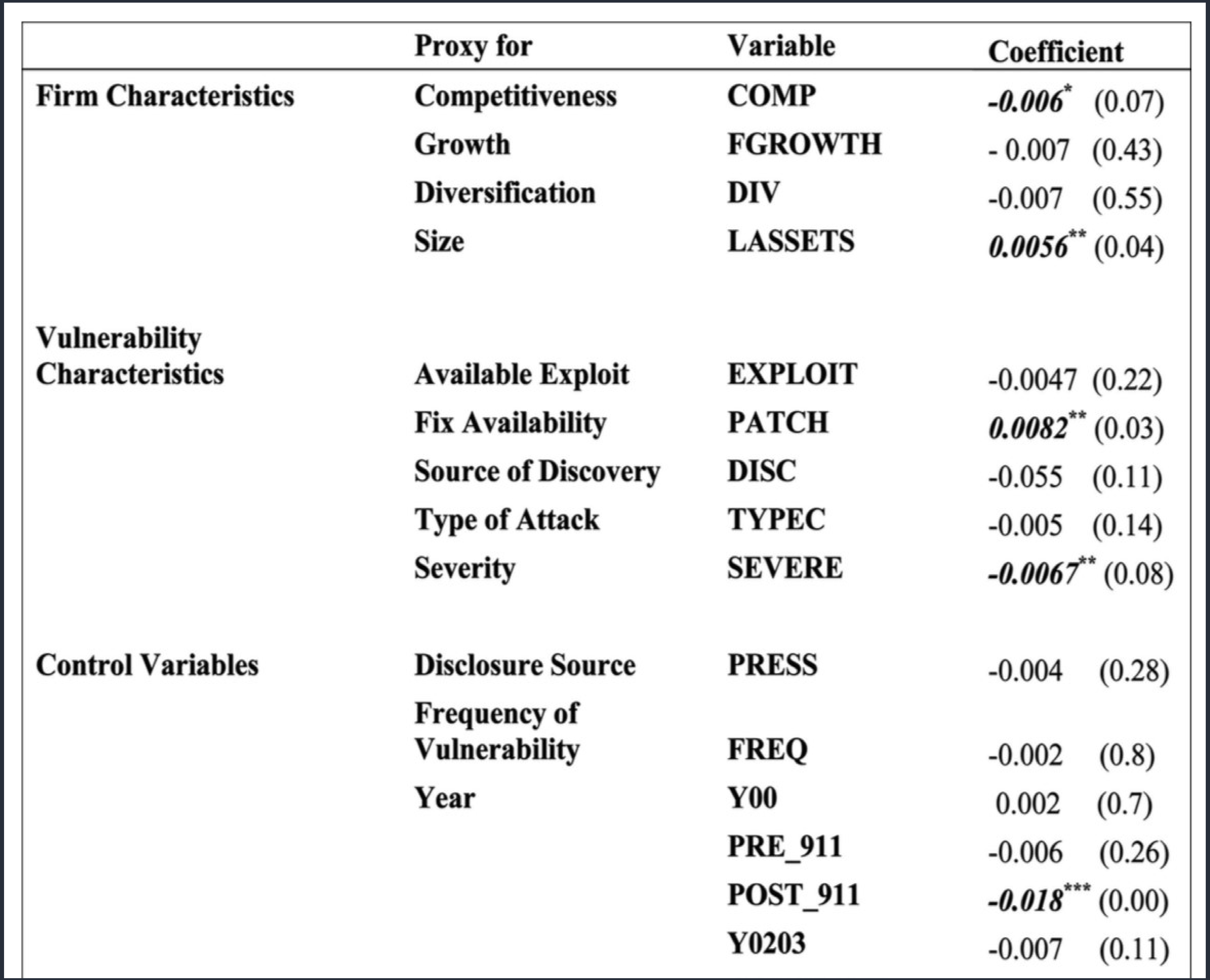
- COMP
  In a competitive market the vendors lose 0.6% more market value than in a monopoly market.



	Proxy for	Variable	Coefficient
Firm Characteristics	Competitiveness	COMP	***-0.006**** (0.07)
	Growth	FGROWTH	- 0.007 (0.43)
	Diversification	DIV	-0.007 (0.55)
	Size	LASSETS	***0.0056***** (0.04)
Vulnerability Characteristics	Available Exploit	EXPLOIT	-0.0047 (0.22)
	Fix Availability	PATCH	***0.0082***** (0.03)
	Source of Discovery	DISC	-0.055 (0.11)
	Type of Attack	TYPEC	-0.005 (0.14)
	Severity	SEVERE	***-0.0067***** (0.08)
Control Variables	Disclosure Source	PRESS	-0.004 (0.28)
	Frequency of Vulnerability	FREQ	-0.002 (0.8)
	Year	Y00	0.002 (0.7)
		PRE_911	-0.006 (0.26)
		POST_911	***-0.018****** (0.00)
		Y0203	-0.007 (0.11)

Results

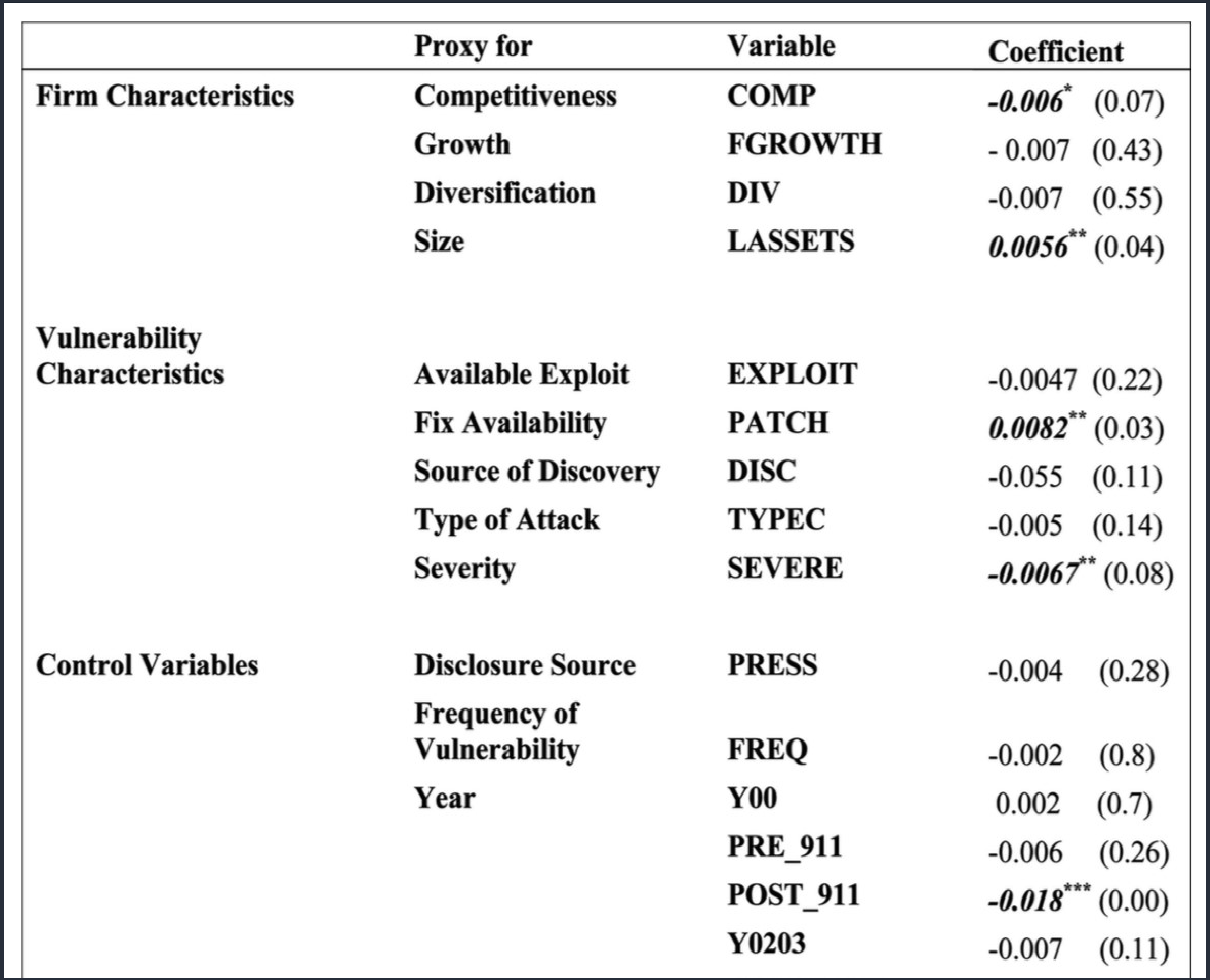
- LASSETS
  Bigger firms lose less market value than smaller firms.



	Proxy for	Variable	Coefficient
Firm Characteristics	Competitiveness	COMP	***-0.006**** (0.07)
	Growth	FGROWTH	- 0.007 (0.43)
	Diversification	DIV	-0.007 (0.55)
	Size	LASSETS	***0.0056***** (0.04)
Vulnerability Characteristics	Available Exploit	EXPLOIT	-0.0047 (0.22)
	Fix Availability	PATCH	***0.0082***** (0.03)
	Source of Discovery	DISC	-0.055 (0.11)
	Type of Attack	TYPEC	-0.005 (0.14)
	Severity	SEVERE	***-0.0067***** (0.08)
Control Variables	Disclosure Source	PRESS	-0.004 (0.28)
	Frequency of Vulnerability	FREQ	-0.002 (0.8)
	Year	Y00	0.002 (0.7)
		PRE_911	-0.006 (0.26)
		POST_911	***-0.018****** (0.00)
		Y0203	-0.007 (0.11)

Results

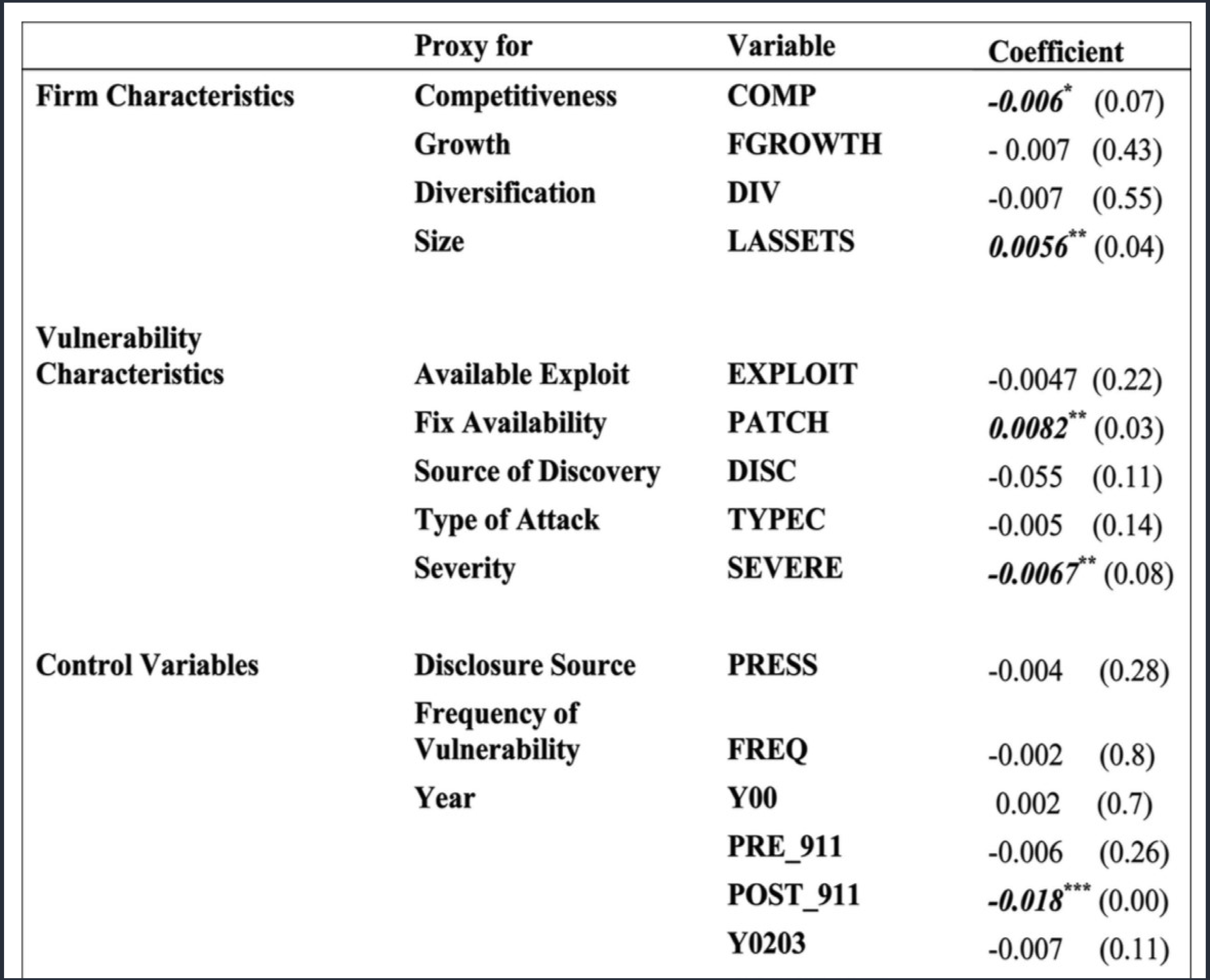
- SEVERE
  Serious vulnerabilities have a larger impact on the market
  -0.67%



	Proxy for	Variable	Coefficient
Firm Characteristics	Competitiveness	COMP	***-0.006**** (0.07)
	Growth	FGROWTH	- 0.007 (0.43)
	Diversification	DIV	-0.007 (0.55)
	Size	LASSETS	***0.0056***** (0.04)
Vulnerability Characteristics	Available Exploit	EXPLOIT	-0.0047 (0.22)
	Fix Availability	PATCH	***0.0082***** (0.03)
	Source of Discovery	DISC	-0.055 (0.11)
	Type of Attack	TYPEC	-0.005 (0.14)
	Severity	SEVERE	***-0.0067***** (0.08)
Control Variables	Disclosure Source	PRESS	-0.004 (0.28)
	Frequency of Vulnerability	FREQ	-0.002 (0.8)
	Year	Y00	0.002 (0.7)
		PRE_911	-0.006 (0.26)
		POST_911	***-0.018****** (0.00)
		Y0203	-0.007 (0.11)

Results

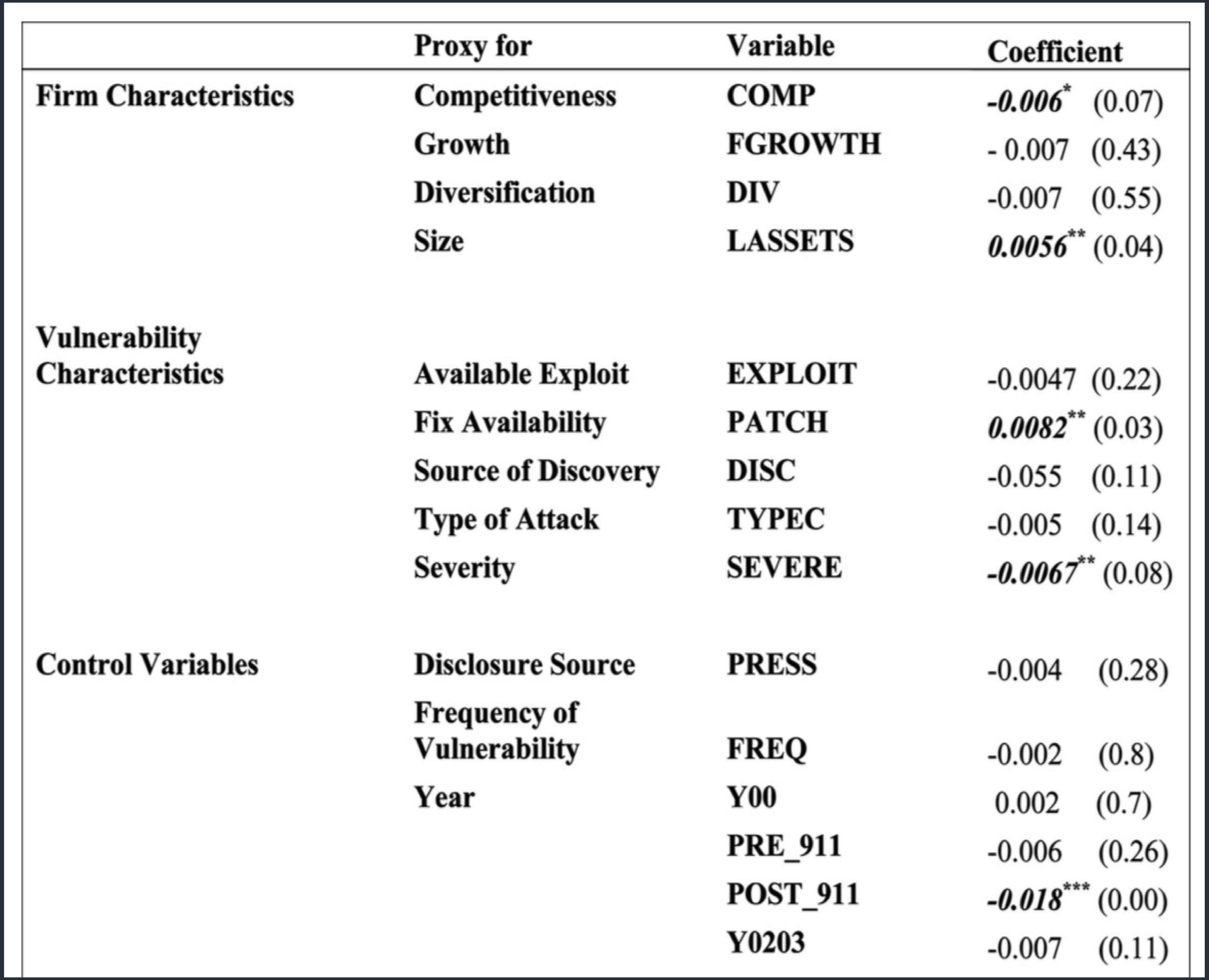
- **PATCH**
  If the patch of the vulnerability is not published by the vendor it will lose 0.82% more than firms that provide a patch.



	Proxy for	Variable	Coefficient
Firm Characteristics	Competitiveness	COMP	***-0.006**** (0.07)
	Growth	FGROWTH	- 0.007 (0.43)
	Diversification	DIV	-0.007 (0.55)
	Size	LASSETS	***0.0056***** (0.04)
Vulnerability Characteristics	Available Exploit	EXPLOIT	-0.0047 (0.22)
	Fix Availability	PATCH	***0.0082***** (0.03)
	Source of Discovery	DISC	-0.055 (0.11)
	Type of Attack	TYPEC	-0.005 (0.14)
	Severity	SEVERE	***-0.0067***** (0.08)
Control Variables	Disclosure Source	PRESS	-0.004 (0.28)
	Frequency of Vulnerability	FREQ	-0.002 (0.8)
	Year	Y00	0.002 (0.7)
		PRE_911	-0.006 (0.26)
		POST_911	***-0.018****** (0.00)
		Y0203	-0.007 (0.11)

Results

- **POST_911**
  If the vendor has discovered a vulnerability in the period after the the twin towers attack, it lost -1.8%.



	Proxy for	Variable	Coefficient
Firm Characteristics	Competitiveness	COMP	-0.006^{*} (0.07)
	Growth	FGROWTH	- 0.007 (0.43)
	Diversification	DIV	-0.007 (0.55)
	Size	LASSETS	0.0056^{**} (0.04)
Vulnerability Characteristics	Available Exploit	EXPLOIT	-0.0047 (0.22)
	Fix Availability	PATCH	0.0082^{**} (0.03)
	Source of Discovery	DISC	-0.055 (0.11)
	Type of Attack	TYPEC	-0.005 (0.14)
	Severity	SEVERE	-0.0067^{**} (0.08)
Control Variables	Disclosure Source	PRESS	-0.004 (0.28)
	Frequency of Vulnerability	FREQ	-0.002 (0.8)
	Year	Y00	0.002 (0.7)
		PRE_911	-0.006 (0.26)
		POST_911	-0.018^{***} (0.00)
		Y0203	-0.007 (0.11)

Conclusions

This research addresses an interesting and contemporary issue of whether software vendors are adversely affected by security-related vulnerability announcements in their products.

Prior studies in other industries mostly suggest vendors suffer a loss in market value when defects are announced in their products.

In this study, 147 different security vulnerabilities related to 18 vendors were considered.

Conclusions

How do stock markets react?

They obviously react badly and, in particular, the vendors lose about 0.63 percent in market value on the day the vulnerability is announced.

0.63 %

But anyway…

Firms lose and gain market value over the normal course and the bigger they are the less they suffer vulnerability disclosures.

How do vendors avoid the problem?

This study points to the fact that product defects hurt software vendors and that the managers need to pay attention to associated bad press as well as stock price slide. Of course a more secure product can generate positive value for a firm.

How do vendors avoid the problem?

Vendors would like to launch software products as soon as possible, they need to focus testing in areas that can potentially contain a greater number of security vulnerabilities.

Vulnerability news is bad news for vendors and they are probably better off keeping quiet and integrating their fixes as either service packs or newer versions and announce the patch only if someone else has disclosed it.

They practically hide it!

How do vendors avoid the problem?

Thank you for listening!