December 2001

Assessing the Risk in E-Commerce

Michael Ettredge
University of Kansas

Vernon Richardson
University of Kansas

ASSESSING THE RISK IN E-COMMERCE

Michael Ettredge
University of Kansas

Vernon J. Richardson
University of Kansas

Abstract

This study identifies the risks to e-commerce using a diverse sample of Internet and other firms by assessing the stock market reaction to hacker attacks. The research issue is, do expert business risk assessors perceive that Internet activity and e- commerce risks per se *generate incremental risk of financial distress?*

Keywords: Event study, e-commerce risk, hacker attacks, stock market reaction.

INTRODUCTION

A major stream of recent research has investigated the economic consequences of resources devoted to information technology (IT) in business settings. Economic consequences have been captured using a variety of variables, such as abnormal stock returns and return on assets. Resources devoted to IT also have been measured in various ways, such as press announcements of significant IT investments, and announcements of newly created chief information officer positions. Almost without exception, such studies have sought evidence of the benefits of resources devoted to IT. This orientation is reflected in the titles of papers that review this literature: "The Impact of Information Technology Investments on Firm Performance: A Review of the Literature" (Sircar et al. 1998) and "Returns to Information Systems Investments: A Review of the Literature" (Dehning and Richardson 2001). Early studies that failed to document benefits of IT investment gave rise to the "productivity paradox" (Brynjolfsson 1993). More recent studies that detect such benefits are said to have taken us "beyond the productivity paradox" (Brynjolfsson and Hitt 1998). One can readily understand why academic researchers who teach information systems courses have sought evidence of IT success. What appears to be missing, however, is some balance in the literature. It is an economic truism that, in an uncertain world, rewards are earned by bearing risk. In this paper, we attempt to assess the risks borne by a set of firms highly reliant on information technology: the so-called Internet firms.

Knowledgeable observers allege that Internet firms typically experience operating risks that do not affect more traditional firms (Glover et al. 2001; Greenstein and Feinman 2000). A major source of such risk is the firms' complete reliance on IT when conducting such fundamental operations as buying and selling goods. When these firms experience interruptions of service, they literally cease to function for a period of time.[1] Glover et al. define and discuss other problems primarily affecting Internet firms such as data theft, unauthorized access to passwords, customer impersonation, false Web sites, e-mail or Web-visit hijacking, and compromised customer privacy. In addition to risks that arise from specific incidents, Internet firms allegedly are subject to risks that are more nebulous, but still very real, such as the unforeseen and sudden advent of competitors, and the risk that consumers will not accept the firms' new business models. In summary, firms that are heavily engaged in e-commerce are subject to a variety of "e-specific" risks, including unusually high reliance on IT.

This study investigates whether capital markets participants believe e-commerce activity subjects Internet companies to incremental firm-specific risk. We employ several variables that proxy for the extent of a firm's e-commerce risks. First, we employ a dichotomous variable to divide Internet firms into two sub-samples. The variable is coded "one" for Internet "e-tailers" (B2C firms). The business press has expressed the view that e-tailers are at increasing risk of failure compared to other firms. The variable is coded "zero" for Internet firms that are not e-tailers (B2B firms). We also derive a number of metrics from firms' descriptions of their business risks, made in filings to the Securities and Exchange Commission (SEC). We are particularly

[1]In June 1999, online auction company eBay experienced a 22-hour period in which its site was shut down due to operating system problems. Over a two-day period, eBay lost 25% of its stock value, or six billion dollars (Glover et al. 2001, pg. 76).

interested in several metrics that arguably capture self-assessed risks arising from reliance on IT: risk due to Internet technology change, risk due to inadequate infrastructure, and risk due to on-line security breach.

Numerous studies have computed abnormal common stock returns to investigate whether stockholders benefit when firms announce incremental resources devoted to IT (among others, Chatterjee et al. 2001; Dos Santos et al. 1993; Im et al. 2001; Subramani and Walden 2001). We examine investors' reactions to a major occurrence of e-commerce risk: distributed denial of service attacks launched by hackers against several of the best-known Internet firms in February 2000. We find that extent of negative abnormal returns are associated with most of the e-risk metrics employed. Investors appear to believe the likelihood an Internet firm will suffer harm in similar future attacks is positively related to its self-disclosed vulnerability to e-risks, including measures of reliance on IT. The negative abnormal returns observed are substantial in magnitude and do not reverse over time.

SETTING AND HYPOTHESES

Investor enthusiasm for technology firms, especially Internet firms, arguably reached its peak early in the year 2000. In February 2000, one observer characterized the situation as follows:

> A pack of investors these days is downright contemptuous of managers who look at fundamentals. To this hard-charging group, almost no price is to high to pay for a rapidly growing tech stock. If you don't believe in this new paradigm, you're a loser. (Dreman, 2000, pg. 172)

Another member of the business press, also writing in February, 2000, stated that hype surrounding the Internet had created a situation in which "Mere profits have no place in the land of infinite possibility" (Pfeiffer 2000a, pg. 70). However, this writer also quoted a veteran Silicon Valley venture capitalist, who earlier had warned:

> There is an Armageddon that's going to happen in the spring, after all those companies spend their huge advertising budgets in the fourth quarter—seeking brand recognition and identification—only to fail and come out broke on the other side. (Pfeiffer 2000b, pg. 68)

The writer concluded (pg. 68): "Soon, perhaps very soon, what we will be left with is cold, hard reality and a lot of dying dot-coms." Already, in February 2000, venture capital support for business-to-consumer (B2C or e-tailer) Internet startups was evaporating, although business-to-business (B2B) plans still were finding favor (Byron 2000).

On Sunday, February 6, through Tuesday, February 8, numerous well-known Internet firms' operations were brought to a standstill by attacks launched by hackers (Glover et al. 2001, p. 73). The victims of the attacks primarily were B2C firms, and included Yahoo!, Amazon.com, eBay, and Buy.com among others. A *BusinessWeek* commentary stated:

> Cyber crime is becoming one of the Net's growth businesses. The recent spate of attacks that gummed up Web sites for hours—known as "denial of service"—is only one type....Indeed, the tactic used to create mayhem in the past few days is actually one of the more innocuous ones. (Sager et al., February 21, 2000)

This study investigates stock market reaction to the February attacks. These occurrences are ideal for an event study of investors' reactions to e-risk because (1) the attacks were sudden and unexpected and (2) the attacks exposed the vulnerability of the best-known and largest Internet firms to risks that are highly specific to e-commerce.

The stock market's reaction to the widely publicized February hacker attacks can be conceptualized as follows. The market value of a firm's equity at time 1, MVE1, is equal to the present value of expected future cash flows, as of time 1, to equity investors:

$$MVE1 = PV(ECF1)$$

The expected future cash flows at time 1, ECF1, reflect all information publicly available to investors at that time. The hacker attacks likely provided investors with new information: that such attacks are more probable than previously thought and that their consequences are more adverse than previously estimated. The market was forcefully reminded that hacker attacks can "take down" even the best known Internet firms, and that such attacks deprive firms selling via the Internet of sales and cash flows. It is important to realize that investors do not simply reduce estimated cash flows for firms actually attacked to reflect those actual

attacks. Instead, investors anticipate *additional* attacks in future on firms that are *similar* to the ones attacked. Following the hacker attacks, the value of a firm's equity can be modeled as:

$$MVE2 = PV(ECF2)$$

The market value of equity at time 2 equals the present value of previously expected cash flows to investors, minus decreases due to anticipated future attacks. Thus ECF2 is less than or equal to ECF1. The size of each firm's decrease in expected future cash flows depends on (1) the probability the firm will be subject to future attacks, and (2) the cash flow consequences of future attacks. Both the expected probability and consequences should be greater for Internet firms and for firms that engage more heavily in e-business. Thus PV(ECF2) – PV(ECF1) is non-positive, and increasingly negative for firms having higher levels of e-activity and e-risk. The percentage change in investors' wealth due to the attacks is:

$$\text{Firm's Return} = \frac{PV(ECF2) - PV(ECF1)}{PV(ECF1)}$$

We adjust the Firm's Return to back out any market-wide movement in stock prices from time 1 to time 2. This yields the Firm's Abnormal Return:

$$\text{Firm's Abnormal Return} = \text{Firm's Return} - \text{Market's Return}$$

Our first alternative hypothesis, therefore, is:

> H1: Other things equal, there is a negative association between a firm's abnormal stock return and the extent of the firm's participation in Internet commerce.

This hypothesis is tested using samples of Internet and non-Internet firms. The hypothesis investigates whether investors' revised estimates of negative future risk outcomes depend on the extent of firms' Internet activity. We also test H1 individually for B2B and B2C firms. Our study, therefore, provides a counterpoint to Subramani and Walden (2001), who found *positive* abnormal stock returns to firms' announcements of e-commerce initiatives during the fourth quarter of 1998, and who examined differences in reaction between B2B versus B2C firms, among other partitions.

Our second hypothesis focuses on the effect of specific e-risks as opposed to general Internet activity level:

> H2: Other things equal, there is a negative association between a firm's abnormal stock return and the presence of specific e-risks.

In order to distinguish between risk adhering to Internet activity in general and risk generated by specific aspects of e-commerce, we test H2 separately for Internet firms and for control firms. That is, we investigate whether variance in extent of e-risks is associated with variance in abnormal returns *within* the Internet firms, and separately within the non-Internet firms.

Following the denial of service attacks, from March to May of 2000, the Nasdaq composite index (dominated by technology and Internet firms) dropped 37%. This drop likely was fueled in part by investors' decisions that even B2B Internet firms lacked clear "P2P" (i.e., path to profitability). In April, 2000, the largest shareholder in the Internet holding company Internet Capital Group announced that it would no longer invest directly in B2B companies (Kroll 2000). A portfolio of ten B2B stocks tracked by Merrill Lynch lost 38% of its value in March and April (Lyons 2000). By June, 2000, prominent analysts and investors were predicting that 75% to 80% of Internet firms will cease to exist (Clash 2000, pg. 314).

STUDY VARIABLES

Our first dependent variable, cumulative abnormal return (CAR) is computed over two different windows. The first window is a three-day period covering February 7 through one day following the hacker attacks, February 9, 2000. Abnormal returns are unavailable for the first day of attacks, February 6, because that was a Sunday. The second window is a six-day period that includes the three-day window and extends for an additional three trading days. We employ this longer window to determine whether any market reaction observed in the first three days subsequently reverses. In order to avoid confounding the general effect of the attacks with any additional effects arising from publicity in the business press, we delete three firms from our Internet sample when testing H1 and H2. These firms—Yahoo!, eBay, and Amazon.com—were specifically mentioned in press accounts

of the attacks. Based on our reading of the business press, we believe few, if any, of the remaining sample firms were subjected to attacks during the event windows.

To determine the cumulative abnormal return (CAR) during the event period (either the three-day or the six-day period), we follow the same market model procedures as Chatterjee et al. (2001).

Testing H1 requires a sample of Internet firms. These were obtained from the InternetStockList™ (available at www.wsrn.com). Parent company internet.com bills this as "A comprehensive list of the more than one hundred publicly-traded companies involved solely in Internet-related business" (www.internet.com as of July, 2000). We defined a dichotomous e-risk variable INET coded "one" for firms classified as Internet firms by this source, and zero otherwise. Internet.com dis-aggregates its InternetStockList into 13 categories based on the nature of a firm's business. Two other dichotomous variables were defined using this information. B2C was coded one for Internet firms identified as e-tailers by InternetStockList, and zero otherwise. B2B was coded one for non-e-tail Internet firms and zero otherwise.

To test H2 we derive e-risk metrics from managers' statements made in Forms 10-K, filed with the SEC. Item 1 of Form 10-K usually contains a discussion of the major risks and uncertainties facing the filing firm. Managers of firms that are heavily engaged in e-commerce typically disclose the resulting risks in item 1.[2] We expect that firms highly active in e-commerce will disclose more e-specific risks than do other firms. One test variable employed is the square root of the number of e-specific risks disclosed, SQNum. In addition, we divide the e-specific risks into two categories: those that we judge can be controlled by managers, and un-controllable (environment) risks. Variable CTRL is defined as one if a firm reports one or more controllable e-risks, and zero otherwise. Variable UTRL is defined as one if a firm discloses one or more un-controllable e-risks. The distinction between controllable and un-controllable e-risks is useful for managers. If results indicate that specific e-risks generate more negative CARs and lowerDun & Bradstreet financial ratings, controllable e-risks can be mitigated.

Table 1. Definitions of Study Variables

Models:		
	CAR = f(Test variables, LnMVE)	(1)
Panel A: Dependent Variables		
CAR3	= cumulative abnormal stock return over a 3-day event window.	
CAR6	= cumulative abnormal stock return over a 6-day event window.	
Panel B: Test Variables		
B2B	= one if a firm is classified by the InternetStockList as an Internet non-e-tailer as of June, 2000, and equals zero otherwise.	
B2C	= one if a firm is an e-tailer, and equals zero otherwise. E-tailer status was based on classification by the InternetStockList as of June, 2000,supplemented by firms' Form 10-K, Item 1 disclosures.	
INET	= one if a firm is classified as an Internet firm by InternetStockList as of June, 2000, and equals zero otherwise. Equals B2B + B2C.	
SQNum	= the square root of the total number of e-specific risks disclosed by a firm in Item 1 of Form 10-K.	
CTRL	= one if a firm discloses one or more controllable e-specific risks in Item 1 of Form 10-K. (See Table 3.)	
UTRL	= one if a firm discloses one or more un-controllable e-specific risks in Item 1 of Form 10-K. (See Table 3.)	

[2]For example, Autobytel.com's December 31, 1999, Form 10-K discusses specific e-business risks in Item 1, including a paragraph with the following heading (emphasis in original): "IF ANY OF OUR RELATIONSHIPS WITH INTERNET SEARCH ENGINES OR ONLINE AUTOMOTIVE INFORMATION PROVIDERS TERMINATES, OUR PURCHASE REQUEST VOLUME COULD DECLINE."

As a proxy for e-commerce risks, the metrics mentioned above have several favorable features. First, managers presumably know their firms' activities better than do outside observers. Second, managers have incentives to disclose relevant risks as a means of averting liability arising from forward-looking statements. Most importantly, from our perspective, the Form 10-K contents provide e-metrics for all filing firms, not just Internet firms. This allows us to distinguish between higher "e" and lower "e" firms among the non-Internet firms.

For all sample firms, we obtained the most recent available Form 10-K as of June, 2000. We examined the business risks disclosed in Item 1 and developed a taxonomy of e-risks, described below. Risks were designated as e-specific if they arise from "buying and selling over digital media" (Kalakota and Robinson 1999, pg. 4), or from internal activities that directly support such purchases or sales. We do not specify that the digital media employed must be the Internet because much e-commerce is conducted otherwise (e.g., electronic data interchange via telecommunications). Subsequently, two research assistants employed the taxonomy to determine how many e-risks each sample firm disclosed. The research assistants made independent judgments and reconciled differences. The e-risk variables described above (SQNum, CTRL, UTRL) were derived from the 10-K disclosures.

SAMPLES AND DESCRIPTIVE STATISTICS

Sample

Four samples, designated (i) through (iv) below, are employed to investigate the association between e-risk metrics and perceived business risks. Most Internet firms have been publicly listed for only a few years. In order to capture incremental e-risk experienced by Internet firms, we contrast (i) a sample of Internet B2B firms with (ii) a sample of non-Internet firms that made their initial public offerings (IPOs) at about the same times. In testing H1, these two samples share the business risk inherent in a short public history of operations, while the Internet firms experience additional e-commerce risks. To test H1 we also contrast a sample of Internet B2C e-tailers (iii) with a sample of non-Internet retail firms (iv) to control for industry characteristics while allowing e-risk to vary. Specific e-risk variables are employed to test H2 using samples (i) and (iii) pooled, and separately using samples (ii) and (iv) pooled.

Taxonomy of Form 10-K Item 1 E-Risks

For all sample firms, we obtained the most recent available Form 10-K as of June, 2000, so long as the statements were issued in calendar year 1999 or 2000. We examined the business risks disclosed in Item 1 and developed the taxonomy of e-risks. Research assistants employed the taxonomy to determine how many e-risks each sample firm disclosed. The taxonomy of e-risks that evolved from inspection of the Item 1 disclosures is shown in Table 2, together with information about the frequency of e-risk disclosures by sample.

Table 2 indicates that the two samples of Internet firms, (i) and (iii), disclose substantially more e-risks of every type than do the samples of non-Internet firms, (ii) and (iv). In general, the B2C e-tailers, sample (iii), disclose more e-risks than do the B2B non-e-tailers, sample (i). They also disclose different types of e-risks. Several of the e-risk categories exhibit differences of 20% or more between samples (i) and (iii). E-tailers are more likely to disclose risk of public non-acceptance, risk of inadequate e-commerce infrastructure, risk of on-line security breach, risk of government intervention (such as imposition of Internet sales taxes), risk due to Internet technology change, and risk due to unavailability of domain names. The e-risk disclosures do not appear to be uniform "boiler-plating" or random noise. Instead, they vary systematically between the various samples in believable ways. In particular, the firms designated by InternetStockList as Internet firms disclose more e-risks.

Descriptive Statistics

Table 3 presents descriptive statistics for the dependent variables by sample. The statistics in panels A and B strongly support H1. Panel A indicates that the median abnormal stock return cumulated over the three-day window, CAR3, is –4.5% for Internet B2B firms versus 2.3% for the IPO sample. The median CAR3 for Internet B2C firms is –7.9% versus –2.2% for the retail sample. These differences in central tendency are both economically and statistically significant. Furthermore, the differences do not disappear over time. Panel B indicates that median abnormal stock return cumulated over a six-day window, CAR6, is –8.1% and –13.6% for the Internet samples versus 2.6% and –3.7% for the control samples. The differences in central tendency are even more pronounced after six days.

Table 2. Disclosure of E-specific Risks in Item 1 of Form 10-K

	% of sample firms disclosing a risk			
	Sample (i) Internet B2B	Sample (ii) Non-Internet IPO	Sample (iii) Internet B2C	Sample (iv) Non-Internet Retail
Uncontrollable e-risks				
A. Risk of public non-acceptance of e-commerce	42.1%	8.8%	73.1%	5.9%
B. Risk of non-acceptance of e-advertising	23.1%	0.0%	19.2%	0.0%
C. Risk of non-acceptance of e-products	31.4%	12.3%	19.2%	0.0%
D. Risk of government Internet intervention	51.2%	3.5%	80.8%	2.9%
E. Risk due to Internet technology change	33.9%	7.0%	53.8%	2.9%
F. Risk due to unavailable domain names	4.1%	0.0%	34.6%	2.9%
Controllable e-risks				
G. Risk of inadequate e-commerce infrastructure	42.1%	1.8%	76.9%	4.4%
H. Risk of inadequate content/service provider	19.8%	3.5%	34.6%	0.0%
I. Risk of on-line security breach	37.2%	3.5%	61.5%	1.5%
J. Risk of off-line customer privacy breach	14.9%	0.0%	11.5%	0.0%
K. Risk due to relations with other Web sites	17.4%	3.5%	23.1%	0.0%
Number of sample firms	121	57	26	68

Table 3. Descriptive Statistics for Dependent Variables

Panel A: CAR3				Quartlies		
	N	Mean	S. Dev.	1st	Median	3rd
Sub-sample						
(i) Internet B2B Firms	115	-0.030	0.115	-0.098	-0.045	0.025
(ii) Non-Internet IPO Firms	51	0.029	0.103	-0.044	0.023	0.092
Test of Mean (i) = Mean (ii):		t-statistic = 3.134				
		Wilcoxon Z = 3.593				
				Quartlies		
	N	Mean	S. Dev.	1st	Median	3rd
(iii) Internet B2C Firms	26	-0.086	0.058	-0.115	-0.079	0.041
(iv) Non-Internet Retailer Firms	56	-0.010	0.078	-0.063	0.022	0.018
Test of Mean (iii) = Mean (iv)		t-statistic = 4.455				
		Wilcoxon Z = 4.404				
Panel B: CAR6				Quartlies		
	N	Mean	S. Dev.	1st	Median	3rd
Sub-sample						
(i) Internet B2B Firms	115	-0.074	0.153	-0.177	-0.081	0.023
(ii) Non-Internet IPO Firms	51	0.025	0.200	-0.080	0.026	0.108
Test of Mean (i) = Mean (ii):		t-statistic = 3.503				
		Wilcoxon Z = 3.166				
				Quartlies		
	N	Mean	S. Dev.	1st	Median	3rd
(iii) Internet B2C Firms	26	-0.152	0.112	-0.220	-0.136	-0.089
(iv) Non-Internet Retailer Firms	56	-0.019	0.106	-0.087	-0.037	0.022
Test of Mean (iii) = Mean (iv)		t-statistic = 3.134				
		Wilcoxon Z = 3.593				

Table 4. Model (1) Between-Sample

Panel A: Dependent Variable = CAR3

Variable	Exp. Sign	Samples (i) and (ii)	Samples (iii) and (iv)	Samples (i), (ii), (iii), (iv)	Samples (i), (ii), (iii), (iv)
Intercept		0.101 (2.43)*	-0.018 (-0.66)	0.015 (0.56)	0.018 (0.67)
B2B	–	-0.060 (-2.87)*	—	—	—
B2C	–	—	-0.078 (-4.42)*	—	—
INET	–	—	—	-0.050 (-3.41)*	-0.031 (-1.70)*
SQNum	–	—	—	—	-0.014 (-1.69)*
LnMVE		-0.011 (-1.76)*	0.0005 (0.10)	-0.001 (-0.29)	-0.001 (-0.25)
Number of Observations		141	74	215	209
F-statistic		6.55*	9.94*	6.66*	5.26*
Adjusted R-squared		7.3%	19.7%	5.0%	5.8%

Panel B: Dependent Variable = CAR6

Variable	Exp. Sign	Samples (i) and (ii)	Samples (iii) and (iv)	Samples (i), (ii), (iii), (iv)	Samples (i), (ii), (iii), (iv)
Intercept		0.183 (3.00)*	-0.003 (-0.06)	0.054 (1.37)*	0.058 (1.49)*
B2B	–	-0.111 (-3.61)*	—	—	—
B2C	–	—	-0.133 (-4.71)*	—	—
INET	–	—	—	-0.094 (-4.22)*	-0.067 (-2.43)*
SQNum	–	—	—	—	-0.019 (-1.61)*
LnMVE		-0.022 (-2.51)*	0.005 (0.62)	-0.001 (-1.31)*	-0.001 (-1.26)
Number of Observations		141	74	215	209
F-statistic		11.23	9.94	12.35	9.07
Adjusted R-squared		12.8%	19.7%	9.6%	10.4%

Estimated coefficients are presented above (t-statistics).
P-values less than or equal to 0.10 are highlighted by an asterisk: "*."
P-values are one-tailed except for the intercept and for LnMVE.

RESULTS

Model (1) Results

Model (1) investigates stock market reaction to the hacker attacks of February 6–7–8, 2000. Model (1) estimation results that contrast the Internet samples with the control samples are presented in Table 4. Panel A of Table 4 employs CAR3 as the dependent variable. All models are significant based on F-statistics. Adjusted R-square values are similar to those observed in other studies employing short window CARs as dependent variables. Panel A indicates that, controlling for residual differences in market capitalization, Internet B2B firms' CARs are 6.0% less than the IPO control sample CARs. Similarly, Internet B2C firms' CARs are 7.8% less than the retail control sample. When all four samples are combined, the Internet firms' CARs are 5.0% less than control sample CARs. The final result column indicates that number of self-disclosed e-risks, SQNum, has additional explanatory power beyond Internet status, INET. Firms disclosing more e-risks have lower CARs.

Results presented in Panel B using six-day CARs are similar to those in Panel A but are generally somewhat stronger. Both F-statistics and Adjusted R-squares are greater in Panel B, and t-statistics for the e-risk variables are more negative, compared to Panel A.

In summary, Table 4 indicates that all measures of e-risk employed are associated with more negative stock reactions using pooled samples of Internet and non-Internet firms. Table 5 investigates whether e-risk metrics can explain variance in market reaction *within* the Internet firms. Models estimated with only non-Internet firms had insignificant F-statistics and are not presented.

Panel A of Table 5 employs three-day CARs as the dependent variable. All models are significant based on F-statistics. Adjusted R-square values are similar to those observed in other studies employing short window CARs as dependent variables. The first results column shows that, controlling for residual differences in firm market cap, Internet B2C firms (e-tailers) experienced CARs that are 7.9% lower than for the B2B Internet firms. This is reasonable given that, according to the business press, the firms subjected to hacker attacks predominantly were B2C firms. The second result column indicates that Internet firms disclosing one or more controllable e-risks experienced more negative abnormal returns. The third result column demonstrates the same is true for Internet firms that disclosed one or more uncontrollable e-risks.

When both controllable and uncontrollable e-risk variables are entered into the same model, both are insignificant (not tabulated). The final result column shows that, among Internet firms, those disclosing more e-risks in Item 1 of Form 10-K experienced more negative abnormal returns. The results when six-day CARs are employed, shown in Panel B, are similar to those in Panel A although generally weaker.

In summary, the Table 5 results indicate that investors make more sophisticated distinctions than that between Internet and non-Internet firms. In particular, *within* the samples of Internet firms, differences in type and numbers of e-risks are significantly associated with differences in market reaction to the February 2000 hacker attacks. Stock price decreases associated with greater e-risk appear to persist over time, suggesting a permanent increase in cost of equity for affected firms.

SUMMARY AND CONCLUSIONS

This study investigates whether capital markets participants believe e-commerce activity subjects companies to incremental firm-specific risk. We employ several variables that proxy for the extent of a firm's e-commerce risks. First, we employ a dichotomous variable capturing observers' judgments whether a firm sells primarily via the Internet. Additional dichotomous variables are used to divide Internet firms into two sub-samples. One dichotomous variable represents Internet "e-tailers" (B2C firms). A second dichotomous variable represents Internet firms that are not e-tailers (B2B firms). We also obtain e-risk metrics from firms' self-disclosed business risks.

We investigate investors' reactions to "hacker" attacks launched against several of the best-known Internet firms in February 2000. These occurrences are ideal for an event study of investors' reactions to e-risk because (1) the attacks were sudden and unexpected and (2) the attacks exposed the vulnerability of the best-known and largest Internet firms to risks that are highly specific to e-commerce. After excluding three firms in our sample that are known subjects of the attacks, we investigate whether the remaining sample firms experienced "contagious" negative abnormal stock returns following the attacks.

Table 5. Model (1) Within-Sample Results

Panel A: Dependent Variable = CAR3

Variable	Exp. Sign	Samples (i) and (iii)	Samples (i) and (iii)	Samples (i) and (iii)	Samples (i) and (iii)
Intercept		0.067 (1.43)	0.051 (1.10)	0.045 (0.97)	0.048 (1.01)
B2C	–	-0.079 (-2.95)*	—	—	—
CTRL	–	—	-0.049 (-2.27)*	—	—
UTRL	–	—	—	-0.048 (-2.06)*	—
SQNum	–	—	—	—	-0.019 (-2.01)*
LnMVE		-0.014 (-2.15)*	-0.010 (-1.45)*	-0.008 (-1.21)	-0.009 (-1.32)*
Number of Observations		118	113	113	113
F-statistic		5.25*	3.56*	3.10*	3.00*
Adjusted R-squared		6.8%	4.4%	3.6%	5.2%

Panel B: Dependent Variable = CAR6

Variable	Exp. Sign	Samples (i) and (iii)	Samples (i) and (iii)	Samples (i) and (iii)	Samples (i) and (iii)
Intercept		0.023 (0.35)	-0.001 (-0.02)	-0.001 (-0.15)	0.009 (-0.13)
B2C	–	-0.098 (-2.68)*	—	—	—
CTRL	–	—	-0.053 (-1.83)*	—	—
UTRL	–	—	—	-0.050 (-1.61)*	—
SQNum	–	—	—	—	-0.019 (-1.46)*
LnMVE		-0.015 (-1.62)*	-0.009 (-0.99)	-0.007 (-0.80)	-0.008 (-0.89)
Number of Observations		118	113	113	113
F-statistic		3.96*	2.12	1.74	1.52
Adjusted R-squared		4.8*	2.0%	1.3%	0.9%

Estimated coefficients are presented above (t-statistics).
P-values less than or equal to 0.10 are highlighted by an asterisk: "*."
P-values are one-tailed except for the intercept and for LnMVE.

Overall, the findings suggest that managers of firms disclosing controllable e-risks potentially can reduce their costs of equity if they ameliorate the controllable risks. We do not have sufficient data to determine whether the benefits of reduced cost of capital would exceed the costs of addressing the controllable risks, and so this issue is left for possible future study.

References

Brynjolfsson, E. "The Productivity Paradox of Information Technology: Review and Assessment," *Communications of the ACM* (36:12, 1993, pp. 67-77

BrynolfssonE., and Hitt, L. M. "Beyond the Productivity Paradox," *Communications of the ACM* (41:8), August 1998, pp. 49-56.

Byron, C. "Balance Due," *Forbes ASAP*, February 21, 2000, pp. 104-107.

Chatterjee, D., Richardson, V. J., and Zmud, R. W. "Examining the Shareholder Wealth Effects of New CIO Position Announcements," *MIS Quarterly* (25:1), March 2001, pp. 43-70.

Clash, J. "Henry Blodget Debates Jeremy Grantham," *Forbes*, June 12, 2000, pp. 312-20.

Dehning, B., and Richardson, V. "Returns to Information System Investments: A Review of the Literature," Working Paper, University of Kansas, 2001.

Dos Santos, B. L., Peffers, K., and Mauer, D. "The Impact of Information Technology Investment Announcements on the Market Value of the Firm," *Information Systems Research* (4), March 1993, pp. 1-23.

Dreman, D. "Jim Cramer: Wrong!," *Forbes*, February 21, 2000, p. 172.

Glover, S., Liddle, S., Prawitt, D. *Ebusiness: Principles and Strategies for Accountants*, Prentice Hall, Upper Saddle River, NJ., 2001.

Greenstein, M., and Feinman, T. *Electronic Commerce: Security, Risk Management and Control*, Irwin McGraw-Hill, New York, 2000.

Im, K. S., Dow, K. E., and Grover, V. "A Reexamination of IT Investment and the Market Value of the Firm – An Event Study Methodology," *Information Systems Research* (12:1), March 2001, pp. 103-117.

Kalakota, R., and Robinson, M. *E-Business: Roadmap for Success*, Addison Wesley, Reading, MA, 1999

Kroll, L. "P2P or Bust," *Forbes Best of the Web*, July 17, 2000, pp. 94-96.

Lyons, D. "B2Bluster," *Forbes*, May 1, 2000, pp. 122-126.

Pfeiffer, E. "Don't Call It "Tulip Mania," It's Just Plain Old Hype," *Forbes ASAP*, February 21, 2000a, pg. 70.

Pfeiffer, E. "Where Are We in the Revolution?," *Forbes ASAP*, February 21, 2000b, pp. 68-70.

Sager, I., Hamm, S., Gross, N., Carey, J., and Hof, R. "Cyber Crime," *Business Week*, February 21, 2000.

Sircar, S., Turnbow, J. L., and Bordoloi, B. "The Impact of Information Technology Investments on Firm Performance: A Review of the Literature," *Engineering Valuation and Cost Analysis* (1), 1998, pp. 171-181.

Subramani, M., and Walden, E. "The Impact of E-commerce Announcements on the Market Value of the Firm," *Information Systems Research* (12:2), June 2001, pp. 135-154.