The impact of cyber-attacks on publicly traded companies

Joseph DeCoste

A thesis in

The John Molson School of Business

Presented in Partial Fulfillment of the Requirements

For the Degree of Master of Science in Administration (Finance) at

Concordia University

Montreal, Quebec, Canada

June, 2017

CONCORDIA UNIVERSITY
School of Graduate Studies

This is to certify that the thesis prepared

By: **Joseph DeCoste**

Entitled: **The Impact of Cyber-Attacks on Publicly Traded Companies**

and submitted in partial fulfillment of the requirements for the degree of

Master of Science in Administration (Finance Option)

complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

_____ Chair
Mahesh Sharma

_____ Examiner
David Newton

_____ Examiner
Ian Rakita

_____ Supervisor
Lawrence Kryzanowski

Approved by _____
Thomas Walker, Graduate Program Director

_____
Anne-Marie Croteau, Dean of Faculty

Date: June 15, 2017

Abstract

The impact of cyber-attacks on publicly traded companies

Joseph DeCoste

This thesis explores the financial impact of cyber-attacks on publicly traded companies as determined by equity market investors, and attempts to identify the significant determinants of this impact. A hand collected sample of 313 events is analyzed using an event study methodology. The average (median) cumulative abnormal return when a company experiences a cyber-attack is -0.69% (-0.37%), which translates into an average (median) $134,604,868 ($30,506,757) destruction of firm value. Smaller firms are hit harder than larger firms, and the number of cyber-attacks in a trailing 30-day period is negatively related to average cumulative abnormal returns. Attacks on technology and telecom companies have become less frequent and less damaging, while attacks on Finance and Retail companies have become more frequent. Retail damages have become significantly worse, and Finance companies have experienced some of the most damaging attacks ever revealed. Hacktivism and State Sponsored attacks are relatively inexpensive to firm value over the studied period, as are breaches of proprietary and identity information.

Acknowledgements

The conclusion of this thesis marks the end of an exciting two years spent in Montreal, and there are many good friends and advisors I have to thank for that. First I would like to express gratitude to my supervisor, Dr. Lawrence Kryzanowski, for his calm and experienced guidance, responsiveness, and good example. Dr. David Newton I thank for his insightful advice on academic life, and Dr. Tingyu Zhou for setting a great example with her tireless work ethic, encouraging attitude, and commitment to her students. I am also grateful to my friends Huayi Tang, Younes El Gourari, and Yawen Mao for excellent conversations and brainstorming sessions which surely saved me countless hours of work and helped me improve my thesis. I was lucky to meet many amazing people and make many great friends, and I thank them all for the friendship and memories. Most of all I would like to thank my family and especially my fiancée and the love of my life, Stacey. Our time apart has been a sacrifice, but it is your unconditional love and support that gives me the courage to pursue my goals.

Table of Contents

List of Tables

Online Appendix

Introduction

The advent of the internet has led to a new and sophisticated channel for criminals to target organizations for nefarious purposes. Prior to the internet, theft of company business secrets, customer records, or the disruption of customer businesses generally required physical actions and considerable risk. Organizations could secure this limited avenue for access with proper physical security and information custody policies. Even now, a common way for businesses to protect their most treasured digital assets is by ensuring that they are not connected to the internet, limiting any risk to the physical realm which can more easily be protected. While keeping information disconnected is undeniably safer, it also robs an organization of the benefits that data connectivity provides. Therefore, businesses must expose potentially important and private information within the fast moving, constantly changing, and more sophisticated digital world, which is more difficult to safeguard.

With this in mind, it is not surprising that organizations are increasingly targeted in the digital environment, especially as digital usage has become more vital and integrated with organizational operations. Furthermore, security technology has often struggled to keep up with unauthorized intruders. For some perspective on the problem consider a survey on cyber-crime by CSI (2010) revealing that 41.1% of surveyed businesses experienced a cyber-attack in the year before the survey. Attacks such as the TJ MAXX data theft in 2007 resulting in 45 million stolen credit and debit card numbers, Heartland Payment Systems attack in 2009 compromising over 100 million credit card numbers, and the Sony PlayStation hack in 2011 that compromised the information of 102 million customers, illustrate the potential scale of damage that cyber-attacks pose. Further evidence of the increasing frequency of cyber-attacks over time is well documented

in Campbell et al (2003), Hovav and D'Arcy (2003, 2004), Yayla and Hu (2011), and Shackleford (2012).

Companies have begun to acknowledge cyber-attacks as a major threat to their businesses. Global surveys of CEO's conducted by PWC in 2015 and 2016 reported 61% consider cyber threats to be a key concern for their companies' growth, and lists cyber security technology as one of the top three most important technologies for companies. However, the dilemma for companies transcends a simple decision of whether or not to protect themselves. Cyber-security is costly, and protecting more information in more sophisticated ways, and doing so dynamically, takes significant initial and ongoing expense. Public companies in particular have to balance this cost with their fiduciary duty to investors to maximize shareholder wealth. From an investor wealth maximization perspective, such expenditures need to be at least value-neutral for the company. Compared to revenue generating and brand promoting investments, cyber-security is not flashy and its expected net benefits are difficult to calculate. A cyber-crime study conducted in 2010 by CSI found that only 52% of companies reported having intrusion detection capabilities, one of the most basic of protections, to inform them when they have been cyber-attacked. Clearly not all companies see even basic protections as a worthwhile investment.

Costs are also hard to determine for companies because the regulatory system in the US is a patchwork of laws covering specific data, industries, or geographical areas. Regulations deal primarily with notification requirements, leaving determination of actual legal liabilities to the courts. Some of these regulations include the HIPAA for health data, PCIDSS for the payment card industry, and US State notification laws (CSI, 2010). Some laws with the widest coverage are not specifically targeted towards cyber-security. For example, the 2002 Sarbanes-Oxley Act only

covers cyber-attacks indirectly, as part of more widespread requirements to report failures of internal controls, and items which will have a material effect on financial statements.

Direct data on the costs of cyber-attacks are unavailable, and are difficult to estimate when considering the potential effects on lost business and damaged reputations. A 2016 survey of managers by the Ponemon Institute estimated an average data breach cost of 4 million dollars, or approximately $221 per lost and stolen record in the US. A natural extension in the face of this paucity of direct data is to examine financial market reactions to determine the damage as perceived by investors. If investors punish the market values of firms' subject to cyber-attacks, then the extent of this punishment provides an estimate of cyber-attack costs when determining optimal investment in cyber-security. Previous literature has reported mixed or weak abnormal returns from cyber-attack announcements using event study methodologies for small samples of such breaches.

Unlike most previous research, this study examines the effects of only cyber-attacks as opposed to physical and cyber intrusions. It uses a much larger set of observations over a much longer time period. This allows for a deeper and more powerful analysis of the role that firm and attack characteristics play in the market's assessment of the costs of such attacks, and of these relationships over time.

The remainder of the thesis is organized as follows: Section I reviews the previous literature. Section II introduces variables and develops the hypotheses. Section III describes the data and methodology. Section IV presents and discusses the results. Section V addresses robustness. Section VI concludes.

I. Literature Review

For a sample of 43 data breaches, Campbell et al (2003) find a significant negative relationship between abnormal returns and privacy breaches only for the subset of breaches involving access to confidential information. Hovav and D'Arcy (2003) find no general market penalty for a sample of 23 denial of service (DoS)[1] attacks, and Hovav and D'Arcy (2004) find no general market penalty for a sample of 186 Virus[2] attacks.

In contrast, Cavusoglu et al (2004) find that breached firms experience heavy market capitalization losses, while information security companies gain significant market value when other firms are breached. Using a larger sample of 79 breaches, Acquisti, Friedman, and Telang (2006) find a moderate but significantly negative market response to data breaches that is higher for small firms, retail firms, greater perceived attack maliciousness and number of victims. They note that outliers seem to drive much of the negative performance, as the median negative response is lower than the mean response. While these determinants are not always significant, they indicate that the market may not treat all attacks the same. Goel and Shawky (2014) find that a sample of 168 data breaches between 2004 and 2008 has an average negative impact of 1% of firm market value. Yayla and Hu (2011) find a significant negative impact of information security events on firm value. Firms with DoS attacks are punished most, ecommerce firms experience more damaging breaches, and these market reactions have generally softened over time.

Using a sample of 121 data breaches from 1995-2007, Gordon, Loeb, and Zhou (2011) find that the impact of breaches was larger before 2001 than after. They also find that breaches affecting

[1] Denial of Service attacks involve a large number of requests to servers with the purpose of overwhelming and disrupting normal operations of the servers. This can prevent websites from working, and companies from accessing important information on servers.
[2] Virus attacks install rogue computer programs into a computer system, disrupting their operation.

the availability of a business's services are more damaging than those related to business integrity or data confidentiality.

Finally, Chai, Kim and Rao (2011) report a significantly positive abnormal return impact of security investment announcements. The abnormal returns became stronger after the passing of the Sarbanes-Oxley act in 2002, which introduced more stringent requirements on companies to keep private information safe.

Of these nine studies, only Cavusoglu et al (2004) focus on cyber-attacks. The others deal with very specific types of attacks (Hovav and D'Arcy, 2003, 2004) or more general data security breaches of which cyber-attacks are a specific subset. Other attacks in these studies include physical breaches such as lost laptops and hard drives with customer data, and employee data theft. While previous empirical results have been mixed, they do generally support the idea that cyber-attacks are damaging events to firms from the perspective of equity investors.

II. Hypotheses

A. Overall effect of cyber-attacks on publicly traded companies

Financial damage may be expected from cyber-attacks for many reasons, some of which have already been explained above. Valuable customer or proprietary information may be lost, legal liabilities may be incurred, a company's reputation may be damaged, and services may be disrupted. However, to the extent that a cyber-attack might motivate positive change within a company, there could be some positive effects which potentially outweigh the negative effects. An example might be a minor systems intrusion compromising a small amount of harmless information, motivating a complete upgrade of a company's information security system. The

market may decide that the reduced risk of a future catastrophic loss of valuable information outweighs the cost of the intrusion itself and react positively in such a case.

B. Effect of cyber-attacks by attack characteristics

It is interesting to test if subgroups of attacks with specific characteristics exhibit significantly different damage. The characteristics studied for each attack, the specific effect they could have on cyber-attack damage, and any potential differences between different subgroups is outlined below.

B.1. Attack Category

Attack categories are set as disrupt, information, or integrity. Disrupt attacks may cause direct losses, such as an online store unable to sell products because their website is offline, or indirect losses as frustrated customers seek other companies to do business with in the future. Disrupt attacks may also harm productivity by making important online resources unavailable to employees, or simply cause reputational harm by showing that a company is unable to protect itself.

Information attacks are those which seek to access private information. They may result in lost business as consumers no longer trust the company to keep their data safe and either seek competitor services, or reduce their use of the service in general; to the detriment of the industry as a whole. Legal liability is also likely from information attacks as most companies are subject to regulation and have a responsibility to protect customer data. If they fail to follow these regulations or fail to protect data, they are likely to face fines and lawsuits. Companies may also lose competitive advantages depending on what is lost. Proprietary information about products,

services, or business plans may end up in the hands of competitors. Lost customer information may also identify promising prospective clients for competitors to approach.

Integrity attacks primarily put reputation at risk, as they include website defacements and social media account hijackings. These defacements and hijackings are often used to spread controversial messages, which could be falsely attributed to the company by the public if they do not realize that an attack has taken place. Customers who realize that these are attacks may be forgiving. Consumer trust may also be damaged in certain integrity attacks. There have been cases where company websites have been attacked and subverted to infect the computers of those who visit with malicious viruses. This could make customers hesitant to use the company's online services in the future.

B.2. Attack type

Attack types are classified as either hacktivism, state sponsored, or cybercrime. Hacktivism attacks are simply a form of activism in the cyber realm. They often take the form of denial of service attacks on a company's website to punish them for a perceived wrong or to raise awareness about the social or political cause of the hacker.

Attacks which are speculated to be sponsored by a specific nation are classified as state sponsored. However, it is generally impossible to authenticate these claims as nations almost universally deny any involvement. Given the resources at the disposal of nations, such attacks may be particularly sophisticated and damaging. However, unlike basic criminal attacks motives may not be to seek financial gain or cause economic damage and some of these attacks may have unexpected positive effects for companies by galvanizing patriotic consumers behind them and generating public support and goodwill.

Those attacks which are not hacktivism or state sponsored are classified as cybercrime, and comprise the majority of attacks. There are many motivations for such attacks. Some are less malicious, and are simply undertaken to expose security weaknesses and force companies to respond with increased security. Some seem to be done simply to cause havoc, seeking no real gain other than notoriety. Others are quite clearly targeted for financial gain.

B.3. Responsibility

Attacks are further classified into two groups depending on who is actually hacked. Tasks such as website hosting and management, consumer data management, and payment processing are often outsourced to specialized services providers. Thus, a large share of the responsibility for stopping an attack on a corporate website, or protecting consumer data, often falls on a third-party. In such cases damages may be mitigated, as fault and legal liability is shared. Attacks with first party blame may therefore be more damaging than those with third or shared party blame.

B.4. Types of information lost

When a company discloses an information breach, it generally announces what information is lost which allows for a classification of the breach by account, identity, payment, and proprietary information.

Account information includes email addresses, log-in names, passwords, addresses, and phone numbers which are generally less sensitive or already semi-public. These types of attacks may have been more serious in the early years of email service. Lost email addresses are generally used to send unsolicited or malicious emails to unsuspecting recipients. These attacks are now familiar and easily avoided by those who use email services and many are identified and blocked by email filters. The danger of attacks involving login names and passwords may be

accentuated when those same credentials are used on many different accounts. These risks can be mitigated by following best practices and using different passwords and usernames for different accounts.

Identity information is considered to be more sensitive and private, and can lead to identity theft that can result in significant damage for the victim. This information includes social security numbers, and employment, health or tax records. Customer perceptions of the risk and cost of identity theft also impacts how they react, and thus the expected cost of these attacks to those responsible for ensuring the safety of the breached data.

Payment information consists of credit card, debit card, or bank account numbers and passwords. The loss of this information leads to a risk of fraud and direct financial loss by consumers. Trust and security is incredibly important in the payment system, and if consumers do not feel safe then damage may be felt as they seek alternate providers or transact less.

Proprietary information includes internal company communications, documents, business plans, product information, and source code. This has the potential to compromise products or decrease competitive advantage.

B.6. First or subsequent hack

If a company has never been hacked, they may be less likely to have proper protections in place to prevent or mitigate damages. Attacks should draw management attention to such deficiencies and motivate improvements to cyber security, mitigating the effects of subsequent attacks. Conversely, consumers may be more forgiving of a “first offense”, but grow increasingly frustrated by additional attacks.

B.7. Firm Industry

Industry classification begins by grouping each event by firm into a Fama-French 12 industry class by HSICCD number as reported in CRSP. Any classifications with less than 20 observations are condensed. Firms in class 12 (industry "other") are moved if they clearly fit better in another industry grouping. For example, Visa and MasterCard SIC codes place them in the "other" category at times, and are moved into the Finance industry grouping to best reflect the nature of the attack being on the financial system. The firms remaining in the "other" category include airlines, courier services, and hotels, amongst others.

We expect attacks on the Finance industry to be damaging if consumers value trust and security highly for these companies, and if the wealth of information held by such firms is vulnerable to unauthorized access. Technology companies might also be significantly affected since many rely on the internet as a core part of their business. Studies by Cavusoglu et al (2004) and Yayla and Hu (2011) indicate such for these two industries. Research by Acquisiti, Friedman, and Telang (2006) also finds that Retail companies are more negatively affected by attacks than other firms.

B.8. Time

To detect changes in cyber-attack damages over time, the sample is split into two sub-periods, 1997 to 2007 and 2008 to 2015, where the first sub period coincides with the last year examined by most previous studies and precedes the recent financial crisis. This allows for an examination of the changes in the category of attacks, motivations of attackers, and types of companies being targeted. Of specific interest is evaluating if the impact of attacks has weakened over time as noted by Gordon, Loeb, and Zhou (2011) and Yayla and Hu (2011). Time may also

reveal changes in the types of attacks and firms being targeted, and the success or failure of companies to respond to early threats.

C. Additional Contingencies

The effect of a cyber-attack may also be influenced by other circumstances. Media and investor attention may be heightened if many attacks have recently occurred, so the number of trailing events in the previous 30 days and the number of days passed since the last attack in the sample are used as a proxy for this effect. The damage associated with information attacks may depend on the number of records lost so this is also tested. The Ponemon (2016) survey of company managers reports that there is indeed a higher cost to a breach if more records are lost. If this increase in cost is significant, then we would expect to see those attacks with larger numbers of records compromised being punished more by investors.

Previous research by Cavusoglu et al (2004) and Acquisti, Friedman, and Telang (2006) find that smaller firms are impacted more by cyber-attacks than larger firms. Since legal costs have a fixed component, they have a disproportionate impact on smaller firms which may also lack the resources to identity and protect themselves as well as larger firms.

III. Data and Methodology

A. Data

A total of 350 events are collected over the 1997-2015 period from news articles obtained through both Factiva and Google News using a keyword search.[3] The event date is recorded as the date of the first media report announcing the attack, with either management confirmation or other credible evidence in support. Unsubstantiated rumours are excluded. The event is attributed

[3] Keywords included in the search: denial of service, ddos, dos, attack, cyber, hack, hacked, hacker, breach, virus, compromise, company, corporation.

to the next trading day if the report is released on a weekend or holiday or the time of publication is after the market close. Other information collected from the news articles includes attack category, attacker type, and whether a third party is at fault. For events involving information loss, the nature of that information and number of records compromised is also recorded when available.

Events are then excluded if they have another major confounding event within the event period [-1, 1] or if return data does not exist for the entire estimation period around the event. Some confounding events in the sample include earnings reports, earning guidance, and analyst ratings changes. A subsample excluding events during recessions is also analyzed given the finding by Kacperczyk, Van Nieuwerburgh and Veldkamp (2016) that investor attention may be focused on aggregate shocks as opposed to idiosyncratic shocks during recessions. The two recession periods as determined by the NBER are March 2001 to November 2001 and December 2007 to June 2009. As in Gordon, Loeb, and Zhou (2011), events are excluded not only if the event date falls in the recession period, but also if their estimation windows [-130, 130] overlap these recession periods, as estimates during high volatility recession periods may be unreliable. Table I provides details of sample size and attrition due to these exclusions.

This event data is merged with daily return and firm characteristic data available from CRSP. To conduct estimation and calculation of expected returns, returns on factor portfolios are used from WRDS and Ken French's data library (French, 2017).

Table 2 provides information on the number of attacks categorized by characteristic and industry for the entire sample, and the sub-periods of 1997 to 2007 and 2008 to 2015, and the recession period. Average and median firm size, number of unique firms targeted, and average number of attacks per firm are reported.

B. Methodology

The first step in determining how a cyber-attack affects stock returns on a given event day is to calculate the abnormal return (AR) due to the event. We do this by estimating the following regression for every event *i* using a 260 trading day window [-130, 130] centered on the event date 0:

$$R_{it} = \alpha_i + \sum \beta_{ij} F_{jt} + \sum_{T=-1}^{1} \gamma_{i\tau} D_\tau + \varepsilon_{it} \qquad (1)$$

Where R_{it} is the excess return over the daily return on the one month treasury bill on the security for event *i* on day *t*; F_{jt} are the excess returns on the market ($MKTRF$), and the raw returns on the size (SMB), value (HML), profitability(RMW), and investment (CMA) risk factors (Fama and French, 2015) for day t, D_T is a dummy variable equal to one on day τ in the event window [-1, 1], and zero otherwise; and ε_{it} is the error term. The estimated gamma represents the abnormal return on each event day τ as in Kryzanowski and Zhang (2013).

The 3-day event window centred on the event date 0 accounts for potential leakage of news before public announcements, for ambiguity in the time of day a news article is actually received by the public, and slight delay in the information release being reflected in market prices. We then sum the abnormal returns in the event window [-1, 1] to obtain a cumulative abnormal return (CAR) for that event. We test if the mean CAR is statistically different than zero using a t-test where the standard error of the cross section of CARs deals with event-induced variability (Campbell, Lo, and MacKinley, 1997). Medians are also examined using a sign test.

We use a simple two sample t-test for independent samples to examine if the mean CAR differ for various subsamples based on various attack characteristics. Inferences are made assuming equal or unequal variances based on the results of a folded F-test for equality of

variance. A Wilcoxon Rank Sum test is used to test median differences between the two samples. (Hollander, Wolfe, and Chicken, 2013). We also check normality of the subsamples using Shapiro-Wilks tests. When normality is rejected, t-tests of mean differences may not be reliable, and median differences should be given more importance.

To identify significant determinants of the CAR, we run a cross sectional regression to test the relationship between CAR and various potential determinants such as time passed since the last cyber-attack, firm size, number of records lost for information attacks, and number of trailing events. Parameter estimates are tested using heteroscedasticity consistent standard errors as recommended in Long and Ervin (2000), and using M-estimate robust regressions (Huber, 1973). We also conduct F-tests to determine equality of our regression coefficients as a further way to test for significant differences in CAR by attack characteristic and industry.

IV. Results and Discussion

A. Overall effect of cyber-attacks

Results in Table (3) show that cyber-attacks result in a small but significant negative mean and median CAR. The mean damage is -0.69% and the median damage is -0.37%. This effect is clearly concentrated on the event day. In terms of firm value, the mean (median) change in market capitalization in the face of a cyber-attack is $134,604,868 ($30,506,757). Clearly attacks are damaging events, and the worst attacks especially so.

Despite trends in earlier research by Gordon, Loeb, and Zhou (2011) and Yayla and Hu (2011) which showed the significance of cyber-attacks declining, results in Table (6) show no significant change in the mean or median CAR between the 1997-2007 and 2008-2015 sub-periods, and CARs in both periods are similar (Online appendix C.1 and C.2)

B. Effect of cyber-attacks by attack category

Results in Table (4) show that disrupt attacks result in a significant mean CAR and marginally insignificant median CAR. This indicates that most disrupt attacks are minor, but that they are capable of causing real damage. Information attacks on the other hand result in both significant mean and median CAR. This highlights the particular importance of data security for IT managers. Integrity attacks, primarily website defacements and social media account hacks, are highly insignificant. Perhaps unsurprisingly, these attacks are considered largely immaterial by investors.

While there are some clear mean and median differences between these attack categories, as shown in Table (5), there is little evidence of a statistical difference between them. Analysis in Table (6) also shows that mean and median CARs have not changed significantly over time for these attack categories.

While damage may not have changed, frequency has (Table 2). Disrupt attacks are much less frequent after 2007, likely due to a decrease in the use of widespread and disruptive virus attacks by hackers. Information and integrity attacks are much more frequent after 2007, and point to a change in motives amongst attackers. Information can be stolen for profit, while integrity attacks can be used to spread messages to wider audiences.

C. *Effect of cyber-attacks by attack type*

Table (4) reveals that damaging attacks are generally those that are criminally motivated. Hacktivism attacks are clearly not damaging based on investor perceptions. As with the case of integrity attacks, the purpose may be to raise awareness for a cause more than to cause damage. State Sponsored attacks also do not cause significant damage based on our sample. However, the

mean CAR is only marginally insignificant despite a relatively small sample, indicating that the threat should not be dismissed lightly.

Hacktivism attacks exhibit much less severe mean and median CARs than other attacks, but this difference is statistically weak (Table 5). While the difference in mean CARs is marginally significant, the test may be unreliable due to non-normality in the sample. The result is not robust to the exclusion of recession period events, and median differences are insignificant.

Hacktivism and State Sponsored attacks are almost non-existent before 2007 (Table 2). Their more recent introduction points to continual change in the challenges faced by companies to keep themselves safe in the cyber world.

D. Effect of cyber-attacks by responsibility

Attacks where the victim is solely responsible for security (first party) and those where responsibility is shared with a third party both exhibit significant negative mean CARs (Table 4). Median CAR is insignificant for third party attacks. The mean and median CAR are more negative and more significant for first party attacks than third party attacks, but these differences are not statistically significant (Table 5). There is also no material change in these differences over time (Table 6).

Despite the lack of a difference in the raw mean and median results between first and third party attacks, our cross sectional regression in Table (7) indicates a potential difference. When controlling for other attack factors, there is some evidence that attacks where the victim is solely to blame are more damaging than when a third party shares the reputational and legal burdens of the attack.

E. Effect of cyber-attacks by type of information lost

Mean and median CARs are significantly negative when account information is lost (Table 4). Payment information only yields a significantly negative mean CAR when recession events are excluded, even though the mean is smaller in magnitude. Payment attack CARs exhibit considerable volatility during the recessionary period. Median damage is insignificant, indicating that payment information is generally well protected, but the wide discrepancy in the mean and median for payment attacks points to the presence of some extremely damaging attacks. The most damaging attack in the sample was a payment attack on Heartland Payment Systems in 2009 in which over 100 million credit card numbers were stolen, causing a drop in firm value of 45.4%.

Mean and median CARs for both identity and proprietary information attacks are both insignificant, though their sample sizes are relatively small. The result is especially surprising for identity attacks, where sensitive information such as social security numbers could lead to identity theft. It may be that consumers are not aware of the risk of identity theft, or companies who store identity information may be in less competitive industries. For example, the largest theft of identity data was an attack in 2015 on California's largest for-profit health insurer, Anthem Health, where the personal information of up to 78.8 million people was compromised.[4] The greater difficulty involved in switching one's business to another provider and the multi-

[4] Initial media reports widely estimated the number of customers exposed to be approximately 80 million. Elizabeth Weise, Massive breach at health care company Anthem Inc., USAToday, Feb. 5, 2015. Available at: https://www.usatoday.com/story/tech/2015/02/04/health-care-anthem-hacked/22900925/ The full scale was confirmed by Anthem on Feb. 24, 2015 to be 78.8 million. Anna Wilde Mathews, Anthem: Hacked Database Included 78.8 Million People, WSJ, Feb. 24, 2015. Available at: https://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364

year delay in publicly revealing the existence of the breach most likely played a role in the market's reaction to the disclosure of this breach.

Again, statistically significant mean and median differences are elusive amongst the information types (Table 5). Identity attacks show signs of having a significantly less negative mean CAR than other attacks only when recession period events are excluded. There is also no evidence of a significant change in CARs for any particular type of information loss over time (Table 6).

F. Effect of cyber-attacks by first or subsequent attacks

Both mean and median CARs for first and subsequent attacks are significant (Table 4). There is some evidence that the mean CAR is significantly worse for first attacks than for new attacks on previously attacked firms (Table 5). Companies who have never been attacked before may be less protected and less prepared to mitigate damage than those who have previously been attacked. However, the medians are not significantly different, and the significance of the mean difference disappears when we control for other factors in our cross sectional regressions (Table 7). There is also no evidence of a change over time (Table 6).

G. Effect of cyber-attacks by industry

Consumer non-durables, technology, and finance companies show significant negative mean CARs, though only the technology industry exhibits a significant median CAR (Table 4). The mean for the Finance industry is only marginally significant, while medians are insignificant. This indicates that finance companies generally do an effective job of protecting themselves and mitigating damage, but when their security fails the damage is very large.

The only significant differences between industry CARs (Table 5) involve the "other" industry, which is significantly less affected by attacks than all other industries. This industry consists of companies such as airlines, courier services, and hotels. Cross sectional regression results (Table 7) also confirm pairwise that attacks are significantly more damaging for most industries relative to the "other" industry. F-tests for the equality of regression coefficients for each pairwise comparison of industries confirm that no other pair of industries exhibits a significant difference. These results are included in an online appendix C.3.

Time plays an interesting role in results by industry as shown in Table (6). Attacks on the technology industry became relatively less frequent and exhibited less significant damage after 2007. In fact, the mean and median CARs are insignificant for attacks on the technology industry after 2007. This is not unexpected as technology companies were early adopters of the internet and at the forefront of developing cyber networks. This provides evidence for the conjecture that technology companies were the best equipped in terms of resources and expertise to identify and respond to such threats.

Very similar results are found for the telecom industry. Companies within this sector generally developed and controlled the infrastructure of the internet and include major internet service providers. They seem to have done well in protecting themselves from cyber-attacks since 2007, experiencing a relatively lower frequency of attacks and significantly less negative mean and median CARs (see Table 2).

Both the number of attacks and the damage from attacks on retail companies have greatly increased. Often these attacks seek to steal customer payment information, with 58% of retail attacks targeting payment data. Ever since the TJ MAXX attack in 2007, large scale retail payment attacks have become more common. Unlike technology and telecom companies, retail

firms may lack the technology and in house expertise to identify and deal with cyber security issues.

Like the retail industry, financial companies have been targeted more frequently since 2007. While the mean and median CARs for cyber-attacks for financial companies are not significantly different over time, some extremely large and damaging attacks have occurred since 2007. One example is the Heartland Payment Systems cyber-attack in 2009.

These industry results combined with the decreased frequency of disrupt attacks and the increase in information attacks indicate that hacker motives appear to have changed over time. Attacks in the early period can be characterized as exploratory and disruptive that mainly targeted the technology of the internet and networks, while recent attacks are more sophisticated and profit driven.

H. Other contingencies

Additional cross sectional results in Table (7) show that smaller firms suffer more when experiencing a cyber-attack. This is consistent with previous research by Cavusoglu et al (2004) and Acquisti, Friedman, and Telang (2006). If much of the legal liability or recovery costs are fixed, then it follows that these costs are a relatively higher burden for smaller firms. This could also be an indication that smaller firms leave more valuable data or infrastructure vulnerable than do large firms, possibly due to a lack of the resources necessary to protect themselves.

Another interesting observation is the effect of trailing events on returns. There is a very small, but significant, negative impact on CARs when there has been an unrelated cyber-attack within the last 30 days. It appears that the number of days that have passed since the last attack is

irrelevant, so it is a clustering of multiple recent attacks which elicits this effect. This is consistent with heightened media and investor awareness during periods of high attack activity.

Somewhat surprising as it is inconsistent with industry research by Ponemon (2016), the number of records lost is not a reliable predictor of CAR. This may be explained by inconsistent reporting of such information across attacks. Often the scale is not evident or revealed at first announcement, or the company decides not to provide details to the public on the number of records lost. Only 35% of all information attacks report the number of records lost.

V. Robustness

The previous analysis was also conducted using a six factor asset pricing model from Fama and French (2016) which does not exclude the momentum factor. The results are included in online appendix A. Results were also evaluated including confounded events as outlined in online appendix B.

When a momentum factor is included, results are similar; with some minor changes in the significance of certain attacks. Mean CARs on payment attacks go from being marginally insignificant in the full sample including recession period events to being significant, mean CARs for companies who were previously hacked become insignificant, and mean CARs for attacks on finance companies become marginally insignificant. Differences in the mean CARs for attacks across characteristics and across time are not materially different. The decreased (increased) damage of attacks to technology (retail) firms becomes slightly less significant. Results of the cross sectional regressions are also very similar.

When confounded events are included, the mean and median CAR are still significantly negative. Results by characteristic and industry are generally similar. Mean CARs for attacks

where a third party shares blame, attacks where account information are lost, and attacks on consumer durable companies become insignificant; while the mean CARS for attacks targeting payment information become more significant. Significance of the medians is also reduced for attacks involving account information and for both the first hack and previously hacked categories. The only noticeable difference in regression results is the significance of the CAR due to disrupt attacks relative to integrity attacks. This is attributable more to the presence of confounding events with positive returns during some integrity attacks, as opposed to an increased severity of disrupt attacks

Robustness tests raise no concerns about our general results, which are generally robust to choice of asset pricing model, the exclusion or inclusion of confounded events or recession period events.

VI. Conclusion

Cyber-attacks continue to cause significant damage to companies. The average (median) cumulative abnormal return that a company experiences when attacked is -0.69% (-0.37%), which translates into an average (median) $134,604,868 ($30,506,757) destruction of firm value. The magnitude and significance of this damage has not declined, counter to the findings reported by Gordon, Loeb, and Zhou (2011) and Yayla and Hu (2011). We find that smaller firms are hit harder than larger firms which supports earlier findings by Cavusoglu et al (2004) and Acquisti, Friedman, and Telang (2006). Our finding that the number of cyber-attacks in a trailing 30-day period is negatively related to average cumulative abnormal returns implies that heightened awareness seems to lead to more concern amongst investors about cyber-attacks.

We have shown that either mean or median CARs are significantly negative for information attacks, disrupt attacks, theft of account data, theft of payment data, attacks on consumer non-durables companies, technology companies, and finance companies. The evidence for payment attacks and attacks on finance companies is mixed, as mean significance is due mainly to catastrophic outliers. We also reported some weak evidence of greater price effects for attacks where the attackee is solely to blame, and for first time attackees.

The cyber attackees and the number of attacks and their price effects have changed over time. While early attacks tended to target technology and telecom companies with the purpose of disrupting their activities, recent attacks appear to have become more sinister and sophisticated and targeted at Finance and Retail companies. Specifically, the damages are significantly lower (higher) for Technology and Telecom (Retail) since 2007. Finance companies have experienced some of the most damaging attacks based on public disclosures. The damage from integrity attacks (generally website defacements and social media account hacks) and state sponsored attacks have been small during the period studied herein.

We caution the reader that all of our conclusions are based on cyber attackees that are publicly traded, on the cyber attackees publicly acknowledging the cyber breach, and the specificity of the information made public about the cyber breach such as its breadth and severity. Furthermore, the power of our tests for some cyber categories is negatively affected by smaller sample sizes and how well the first disclosure of a cyber breach captures the severity of a breach when the full extent of its disclosure occurs over a period from a few days to several months and when the cyber attackees first disclosure of the cyber breach is such that it contains information that it has enacted remediation actions to eliminate its cyber vulnerability.

References

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 Proceedings*, 94.

Campbell, J. Y., Lo, A. W. C., & MacKinlay, A. C. (1997). *The econometrics of financial markets*. Princeton University press.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431-448.

Carhart, M. M. (1997). On persistence in mutual fund performance. *The Journal of Finance*, *52*(1), 57-82.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 70-104.

Chai, S., Kim, M., & Rao, H. R. (2011). Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems*, *50*(4), 651-661.

Computer crime and security survey. (2010). Computer Security Institute. Accessed February 22, 2017 from https://cours.etsmtl.ca/gti619/documents/divers/ CSIsurvey2010.pdf.

Eugene F. Fama, Kenneth R. French, (2015). A five-factor asset pricing model. *Journal of Financial Economics* 116, 1–22.

Fama, E. F., & French, K. R. (2016). Dissecting anomalies with a five-factor model. *Review of Financial Studies*, *29*(1), 69-103.

French, K. Data Library. Retrieved May 08, 2017, from http://mba.tuck.dartmouth.edu/pages/faculty/ken.french/data_library.html

Goel, S., & Shawky, H. A. (2014). The impact of federal and state notification laws on security breach announcements. *Communications of the Association for Information Systems*, *34*(1), 37-50.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs?. *Journal of Computer Security*, *19*(1), 33-56.

Hollander, M., Wolfe, D. A., & Chicken, E. (2013). *Nonparametric Statistical Methods*. John Wiley & Sons.

Hovav, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review*, *6*(2), 97-121.

Hovav, A., & D'Arcy, J. (2004). The Impact of Virus Attack Announcements on the Market Value of Firms. *Information Systems Security*, *13*(3), 32-40.

Huber, P. J. (1973). Robust regression: asymptotics, conjectures and Monte Carlo. *The Annals of Statistics*, 799-821.

Kacperczyk, M., Van Nieuwerburgh, S., & Veldkamp, L. (2016). A rational theory of mutual funds' attention allocation. *Econometrica*, *84*(2), 571-626.

Kryzanowski, L., & Zhang, Y. (2013). Financial restatements by Canadian firms cross-listed and not cross-listed in the US. *Journal of Multinational Financial Management*, *23*(1), 74-96.

Long, J. S., & Ervin, L. H. (2000). Using heteroscedasticity consistent standard errors in the linear regression model. *The American Statistician*, *54*(3), 217-224.

Ponemon Institute Cost of a Data Breach Study. (2016). Ponemon Institute. Retrieved February 22, 2017, from https://securityintelligence.com/media/2016-cost-data-breach-study/

18th Annual Global CEO Survey. (2015). PWC. Accessed May 15, 2017 from https://www.pwc.com/gx/en/ceo-survey/2015/assets/pwc-18th-annual-global-ceo-survey-jan-2015.pdf.

19th Annual Global CEO Survey. (2016). PWC. Accessed May 15, 2017 from https://www.pwc.com/gx/en/ceo-survey/2016/landing-page/pwc-19th-annual-global-ceo-survey.pdf.

Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance?. *Business Horizons*, *55*(4), 349-356.

Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology*, *26*(1), 60-77.

Appendix

Table 1: Sample attrition

Attrition of the sample due to insufficient return data in the [-130, 130] estimation window around the event date, confounding events within the [-1, 1] event window, and recession periods defined by the NBER are shown below. Confounding events in the sample include items such as earnings reports, earning guidance, and analyst ratings changes that are publicly announced during the event window.

Criteria	**Impact on Sample Size**		
	Overall	**1997-2007**	**2008-2015**
Initial Sample	350	144	206
Insufficient return data in estimation period	-8	-6	-2
Confounding events	-29	-12	-17
Full Sample	313	126	187
Recession period events	-36	-20	-16
Sample excluding recession period events	277	106	171

Table 2: Description of the sample

The number of cyberattack events collected between January 1, 1997 and December 31, 2015 is reported by attack characteristics and industry. These exclude events with insufficient return data and confounding events within a 3-day period centered on the event date (see Table 1 for sample attrition). The number of firms is presented for the full time period and the two sub periods. Recession events are events whose [-130, 130] estimation windows overlap an NBER defined recession period.

	Number of events				Avg. Market Capitalization ($Billion)		Number of firms	Avg. attacks per firm
	Full	1997-2007	2008-2015	Recession	Mean	Median		
Overall	313	126	187	36	61.5	23.2	170	1.84
Disrupt	110	83	27	15	84.3	33.9	65	1.69
Information	156	36	120	15	47.8	15.0	118	1.32
Integrity	47	7	40	6	53.8	26.4	31	1.52
Hacktivism	22	1	21	0	39.1	17.7	19	1.16
State Sponsored	25	0	25	0	57.5	34.1	21	1.19
Cybercrime	266	125	141	36	63.8	23.1	156	1.71
First Party at Fault	208	51	157	31	64.0	20.3	123	1.69
Third Party at Fault	105	75	30	5	56.8	32.5	79	1.33
Account	49	4	45	4	43.5	14.8	42	1.17
Identity	21	6	15	4	28.7	11.2	20	1.05
Payment	62	20	42	7	52.9	20.4	50	1.24
Proprietary	23	4	19	0	64.6	21.9	21	1.10
Previously Hacked	143	50	93	15	96.5	41.9	59	2.42
First Hack	170	76	94	21	32.1	10.4	170	1.00
Consumer Non Durables	21	10	11	3	7.6	5.4	8	2.63
Durables and Manuft.	28	12	16	1	42.0	5.3	12	2.33
Technology	97	48	49	16	107.7	38.4	43	2.26
Telecom and TV	31	18	13	4	61.2	45.1	15	2.07
Wholesale and Retail	31	4	27	2	30.7	10.6	26	1.19
Finance	68	24	44	4	57.0	36.4	38	1.79
Other	37	10	27	6	20.5	7.7	28	1.32

Table 3: Mean and median CAR by event day

The mean and median abnormal and cumulative abnormal returns are presented by time period for the event window [-1, 1]. Abnormal returns are estimated from regression model $R_{it} = \alpha_i + \sum \beta_{ij} F_{jt} + \sum_{T=-1}^{1} \gamma_{iT} D_T + \varepsilon_{it}$ where R_{it} is the excess return over the one month treasury bill rate on the security for event i on day t; F_{jt} are the excess returns on the market ($MKTRF$), size (SMB), value (HML), profitability(RMW), and investment (CMA) risk factors (Fama, 2015) for day t, D_T is a dummy variable equal to one on day τ in the event window [-1, 1], and zero otherwise; and ε_{it} is the error term. Abnormal returns are summed over the event window to compute cumulative abnormal returns. Significance of the means (medians) as determined by a two-tailed t-test (sign test) is highlighted with * for 10% level, ** for 5% level, and *** for 1% level.

	1997-2015 Overall					**1997-2015 Excluding Recession**			
	Mean	**p**	**Median**	**p**		**Mean**	**p**	**Median**	**p**
CAR	-0.0069***	0.0014	-0.0037***	0.0066		-0.0056***	0.0003	-0.0035**	0.0161
t-1	-0.0008	0.4093	-0.0004	0.572		-0.0001	0.8765	-0.0004	0.471
t=0	-0.0054***	<.0001	-0.0039***	<.0001		-0.0054***	<.0001	-0.0037***	<.0001
t+1	-0.0007	0.6337	0.0005	0.8212		-0.0001	0.9347	-0.0002	1.0000
	1997-2007								
	Mean	**p**	**Median**	**p**		**Mean**	**p**	**Median**	**p**
CAR	-0.0075***	0.0043	-0.0049*	0.0901		-0.0067**	0.0150	-0.0040	0.2065
t-1	-0.0020	0.2885	-0.0012	0.7894		-0.0010	0.5180	-0.0016	0.4968
t=0	-0.0058***	0.0005	-0.0041***	0.0031		-0.0053***	0.0029	-0.0037**	0.0148
t+1	0.0004	0.8072	-0.0006	0.6562		-0.0003	0.8565	-0.0013	0.3821
	2008-2015								
	Mean	**p**	**Median**	**p**		**Mean**	**p**	**Median**	**p**
CAR	-0.0065**	0.0392	-0.0034**	0.0403		-0.005***	0.0069	-0.0035**	0.0465
t-1	0.0001	0.9168	-0.0004	0.6609		0.0004	0.6118	-0.0004	0.7598
t=0	-0.0051***	0.0004	-0.0037***	0.0007		-0.0055***	<.0001	-0.0037***	0.0007
t+1	-0.0015	0.5240	0.0011	0.4647		0.0001	0.9404	0.0010	0.5408

Table 4: Mean and median CAR by characteristic and industry

The mean and median cumulative abnormal return is presented by attack characteristic and industry. Abnormal returns are estimated from regression model $R_{it} = \alpha_i + \sum \beta_{ij} F_{jt} + \sum_{T=-1}^{1} \gamma_{iT} D_T + \varepsilon_{it}$ where R_{it} is the excess return over the one month treasury bill rate on the security for event i on day t; F_{jt} are the excess returns on the market ($MKTRF$), size (SMB), value (HML), profitability(RMW), and investment (CMA) risk factors (Fama and French, 2015) for day t, D_T is a dummy variable equal to one on day τ in the event window [-1, 1], and zero otherwise; and ε_{it} is the error term. Abnormal returns are summed over the three-day event window [-1, 1] to compute cumulative abnormal returns. Significance of the means (medians) as determined by a two tailed t-test (sign test) is highlighted with * for 10% level, ** for 5% level, and *** for 1% level.

	Overall					Excluding Recession				
	N	Mean	p	Median	p	N	Mean	p	Median	p
Overall	313	-0.0069***	0.0014	-0.0037***	0.0066	277	-0.0056***	0.0003	-0.0035**	0.0161
Disrupt	110	-0.0054**	0.0270	-0.0031	0.1046	95	-0.0050**	0.0472	-0.0029	0.2181
Information	156	-0.0092**	0.0181	-0.0045**	0.0450	141	-0.0072***	0.0028	-0.0046**	0.0429
Integrity	47	-0.0026	0.3061	-0.0037	0.5601	41	-0.0017	0.5153	-0.0017	0.7552
Hacktivism	22	0.0010	0.8228	0.0016	0.8318	22	0.0010	0.8228	0.0016	0.8318
State Sponsored	25	-0.0059	0.1380	-0.0067	0.4244	25	-0.0059	0.1380	-0.0067	0.4244
Cybercrime	266	-0.0076***	0.0021	-0.0043***	0.0057	230	-0.0062***	0.0004	-0.0041**	0.0145
First Party at Fault	208	-0.0081***	0.0076	-0.0045**	0.0219	177	-0.0063***	0.0017	-0.0043*	0.0504
Third Party at Fault	105	-0.0045*	0.0509	-0.0028	0.1716	100	-0.0045*	0.0637	-0.0028	0.1933
Account	49	-0.0059*	0.0670	-0.0048**	0.0213	45	-0.0075**	0.0246	-0.0103**	0.0161
Identity	21	-0.0039	0.3971	0.0013	0.6636	17	0.0014	0.6786	0.0029	0.3323
Payment	62	-0.0138	0.1185	-0.0045	0.2529	55	-0.0089**	0.0304	-0.0047	0.1770
Proprietary	23	-0.0047	0.4224	-0.0044	1.0000	23	-0.0047	0.4224	-0.0044	1.0000
Previously Hacked	143	-0.0031*	0.0992	-0.0035*	0.0654	128	-0.0031*	0.0850	-0.0035*	0.0927
First Hack	170	-0.0101***	0.0056	-0.0047*	0.0549	149	-0.0078***	0.0013	-0.0046	0.1010
Consumer Non Durables	21	-0.0082*	0.0720	-0.0110	0.1892	18	-0.0091*	0.0861	-0.0116	0.2379
Durables and Manuft.	28	-0.0059	0.2420	-0.0045	0.3449	27	-0.0066	0.2054	-0.0051	0.2478
Technology	97	-0.0073***	0.0096	-0.0064**	0.0250	81	-0.0055**	0.0383	-0.0056	0.1193
Telecom and TV	31	-0.0054	0.2370	-0.0032	1.0000	27	-0.0063	0.2205	-0.0032	1.0000
Wholesale and Retail	31	-0.0063	0.2133	-0.0071	0.4731	29	-0.0085	0.1022	-0.0071	0.2649
Finance	68	-0.0128*	0.0943	-0.0023	0.3961	64	-0.0062	0.1071	-0.0017	0.5323
Other	37	0.0033	0.5464	0.0013	1.0000	31	0.0012	0.7090	0.0013	1.0000

Table 5: Mean and median differences in CAR across characteristic subgroups

Differences in the mean CAR between attacks with the noted characteristics and all others is shown along with the results of a two-tailed student t-test and a Wilcoxon Rank Sum Test. CARs are estimated using the Five Factor asset pricing model. Shapiro-Wilks tests (not shown) indicate non-normality for all difference tests, indicating that the Wilcoxon results may be more appropriate. Results for the full sample and excluding those events whose [-130,130] estimation window overlap a NBER defined recession are shown. Dif. refers to Difference.

	Overall						Excluding Recession					
	Mean Dif.	T	p-value	Median Dif.	W	p-value	Mean Dif.	T	p-value	Median Dif.	W	p-value
Disrupt	0.0022	0.58	0.5633	0.0013	17393	0.8728	0.0010	0.31	0.7604	0.0014	13494	0.6489
Information	-0.0046	-1.08	0.2820	-0.0013	23944	0.4945	-0.0032	-1.05	0.2951	-0.0023	19644	0.2682
Integrity	0.0050	1.42	0.1563	0.0001	7804	0.4585	0.0046	1.44	0.1542	0.0021	6150	0.3422
Hacktivism	0.0085*	1.73	0.0920	0.0060	3910	0.2666	0.0072	1.27	0.2034	0.0059	3454	0.2736
State Sponsored	0.0011	0.24	0.8120	-0.0031	3800	0.7744	-0.0003	-0.07	0.9427	-0.0032	3341	0.7270
Cybercrime	-0.0050	-1.31	0.1943	-0.0011	7710	0.5638	-0.0036	-1.05	0.2958	-0.0010	6795	0.6017
First Party at Fault	-0.0036	-0.94	0.3465	-0.0018	16853	0.6272	-0.0018	-0.58	0.5642	-0.0014	14172	0.6719
Account	0.0011	0.29	0.7760	-0.0013	7182	0.3809	-0.0023	-0.55	0.5856	-0.0072	5531	0.1424
Identity	0.0032	0.64	0.5294	0.0055	3511	0.5944	0.0075*	2.03	0.0535	0.0071	2772	0.2028
Payment	-0.0086	-0.97	0.3341	-0.0010	9361	0.5598	-0.0041	-0.95	0.3440	-0.0014	7123	0.3277
Proprietary	0.0024	0.39	0.6972	-0.0008	3784	0.6800	0.0011	0.19	0.8486	-0.0009	3340	0.6988
First Hack	-0.0070*	-1.74	0.0836	-0.0012	23210	0.3423	-0.0047	-1.58	0.1147	-0.0011	18328	0.4212
Consumer Non Durables	-0.0014	-0.29	0.7717	-0.0075	2877	0.2958	-0.0037	-0.59	0.5536	-0.0084	2103	0.2263
Durables and Manuft.	0.0010	0.19	0.8511	-0.0011	4292	0.8210	-0.0011	-0.22	0.8283	-0.0017	3559	0.6250
Technology	-0.0006	-0.14	0.8859	-0.0032	14650	0.4352	0.0002	0.07	0.9435	-0.0022	11155	0.8646
Telecom and TV	0.0017	0.34	0.7356	0.0009	5007	0.7707	-0.0007	-0.14	0.8866	0.0006	3771	0.9647
Wholesale and Retail	0.0006	0.11	0.9093	-0.0035	4791	0.8747	-0.0032	-0.61	0.5470	-0.0038	3720	0.4475
Finance	-0.0076	-0.98	0.3315	0.0021	10878	0.7604	-0.0007	-0.18	0.8586	0.0027	9195	0.5957
Other	0.0116*	1.76	0.0796	0.0062	6646	0.1058	0.0077*	2.09	0.0417	0.0062	5000	0.1006

Table 6: Mean and median differences by subgroup over time

Differences in mean CARs between the sub period 1997 to 2007 and sub period 2008 to 2015 are shown along with the results of a two tailed student t-test and a Wilcoxon Rank Sum Test. CARs are estimated using the Five Factor asset pricing model. Shapiro-Wilks tests are conducted on each subgroup by period and those groups which are not significantly non-normal are indicated with a *. Student t-test results are appropriate for these groups. Reported t-values assume either unequal or equal variance as appropriate based on an equality of variance (Folded F) test. For all others, Wilcoxon results may be more appropriate. Results for the full sample and excluding those events whose [-130,130] estimation window overlap a NBER defined recession are shown. Dif. refers to Difference.

	Overall						Excluding Recession					
	Mean Dif.	T	p-value	Median Dif.	W	p-value	Mean Dif.	T	p-value	Median Dif.	W	p-value
Overall	0.0010	0.24	0.8101	0.0014	19174	0.4397	0.0017	0.52	0.6069	0.0005	14707	0.9674
Disrupt	-0.0013	-0.23	0.8165	0.0005	1497	0.9945	0.0014	0.23	0.8219	0.0006	988	0.8023
Information	0.0050	0.65	0.5159	0.0011	2692	0.5752	0.0053	0.77	0.4487	0.0016	1908	0.6818
Integrity	0.0050	0.70	0.4898	0.0045	144	0.4861	-0.0057	-0.55	0.5844	-0.0075	70	0.7466
Hacktivism*	-0.0162	-0.77	0.4481	-0.0152	18	0.3550	-0.0162	-0.77	0.4481	-0.0152	18	0.3550
Cybercrime	0.0001	0.01	0.9906	0.0014	16448	0.7030	0.0012	0.34	0.7313	0.0003	12131	0.9952
Third Party at Fault	0.0048	0.81	0.4208	0.0028	4874	0.2245	0.0066	1.15	0.2552	0.0027	2840	0.3134
First Party at Fault	0.0002	0.05	0.9602	-0.0027	1527	0.6584	-0.0007	-0.16	0.8736	-0.0037	1375	0.5006
Account*	-0.0041	-0.35	0.7248	-0.0016	115	0.5989	0.0063	0.28	0.7787	0.0058	18	0.7306
Identity*	0.0100	1.00	0.3301	0.0154	56	0.4682	0.0063	0.71	0.4881	0.0142	23	0.6651
Payment	0.0067	-0.48	0.6345	-0.0061	646	0.8162	-0.0061	-0.90	0.3732	-0.0063	543	0.4928
Proprietary	0.0284	1.39	0.2483	0.0175	32	0.2219	0.0284	1.39	0.2483	0.0175	32	0.2219
Previously Hacked	-0.0008	-0.12	0.9049	0.0016	6496	0.9963	0.0005	0.11	0.9102	0.0006	4884	0.7493
First Hack	0.0017	0.43	0.6659	0.0008	3478	0.6078	0.0020	0.53	0.5969	-0.0015	2648	0.7593
Consumer Non Durables*	-0.0091	-1.05	0.3063	-0.0038	126	0.2880	-0.0101	-1.01	0.3278	-0.0103	89	0.2822
Durables and Manuft.*	-0.0055	-0.60	0.5563	-0.0052	183	0.6962	-0.0041	-0.44	0.6626	-0.0038	159	0.8260
Technology	0.0112*	2.05	0.0432	0.0054*	2116	0.0893	0.0118**	2.28	0.0259	0.0068	1394	0.1257
Telecom and TV*	0.0160*	2.11	0.0465	0.0155*	256	0.0564	0.0151*	1.78	0.0910	0.0141	184	0.1574
Wholesale and Retail	-0.0196	-1.34	0.1918	-0.0218*	95	0.0714	-0.0205	-1.25	0.2217	-0.0212	68	0.1183
Finance	-0.0156	-1.20	0.2361	-0.0045	927	0.2106	-0.0056	-0.71	0.4822	-0.0045	835	0.2280
Other*	0.0065	0.52	0.6072	0.0005	185	0.8786	-0.0063	-0.80	0.4312	-0.0027	125	0.5592

Table 7: Cross sectional regression of CAR

Results are reported for a cross sectional regression of determinants of cumulative abnormal returns. CARs used are calculated using a Five Factor asset pricing model. Firm size is the natural logarithm of firm size (in thousands) on the day of the attack. Days passed is the natural logarithm of the number of calendar days since the last attack. Trailing events count the number of cyber-attacks on publicly traded companies in the last 30 trading days. Number of records is the natural logarithm of the number of records lost in an attack. The remaining variables are dummies for the stated attack, industry, or time attribute. Results are shown for OLS estimates with ordinary and heteroscedasticity consistent standard errors. Robust regressions are conducted using the M-estimation method. Significance is highlighted with * for 10% level, ** for 5% level, and *** for 1% level. Std. Error refers to standard error.

				Heteroscedasticity Consistent			Robust Regression		
Variable	**Coefficient**	**Std. Error**	**p-value**	**Std. Error**	**p-value**		**Coefficient**	**Std. Error**	**p-value**
Intercept	-0.0818**	0.0371	0.0284	0.0364	0.0253		-0.0402	0.0207	0.0522
Firm Size	0.0044***	0.0014	0.0017	0.0017	0.0090		0.0021***	0.0008	0.0071
Disrupt	0.0018	0.0076	0.8086	0.0060	0.7601		-0.0005	0.0042	0.9138
Identity	0.0022	0.0112	0.8466	0.0081	0.7893		0.0010	0.0062	0.8729
Account	-0.0042	0.0086	0.6256	0.0059	0.4774		-0.0060	0.0048	0.2106
Payment	-0.0092	0.0089	0.2987	0.0115	0.4240		-0.0061	0.0049	0.2174
Proprietary	-0.0008	0.0099	0.9354	0.0070	0.9084		0.0013	0.0055	0.8180
Hacktivism	0.0064	0.0111	0.5651	0.0050	0.2047		0.0067	0.0062	0.2808
Crime	0.0011	0.0094	0.9107	0.0055	0.8496		0.0042	0.0052	0.4242
First Party	-0.0083*	0.0063	0.1904	0.0044	0.0600		-0.0042	0.0035	0.2391
First Hack	-0.0027	0.0050	0.5924	0.0036	0.4570		-0.0007	0.0028	0.8097
Consumer Non Durables	-0.0114	0.0107	0.2882	0.0075	0.1288		-0.0095	0.0059	0.1094
Durables and Manuft.	-0.0144*	0.0099	0.1457	0.0086	0.0937		-0.0081	0.0055	0.1425
Technology	-0.0173**	0.0079	0.0290	0.0074	0.0192		-0.0102**	0.0044	0.0209
Telecom and TV	-0.0183**	0.0095	0.0563	0.0086	0.0343		-0.0090*	0.0053	0.0906
Wholesale and Retail	-0.0087	0.0095	0.3634	0.0093	0.3503		-0.0054	0.0053	0.3112
Finance	-0.0225**	0.0081	0.0056	0.0113	0.0467		-0.0074*	0.0045	0.0986
Days Passed	-0.0009	0.0015	0.5619	0.0012	0.4554		-0.0006	0.0008	0.4606
Trailing Events	-0.0013**	0.0007	0.0764	0.0006	0.0451		-0.0009**	0.0004	0.0257
1997-2007	-0.0028	0.0063	0.6570	0.0068	0.6821		-0.0023	0.0035	0.5052
Recession Window	-0.0088	0.0073	0.2267	0.0148	0.5525		-0.0010	0.0040	0.8107
Number of Records	0.0003	0.0006	0.5343	0.0005	0.5117		0.0000	0.0003	0.9460

Online Appendix A: Results using a six factor asset pricing model to estimate abnormal returns

Table A.1: Mean and median CAR by event day, Six Factor Model

The mean and median abnormal and cumulative abnormal returns are presented by time period for the event window [-1, 1]. Abnormal returns are estimated from regression model $R_{it} = \alpha_i + \sum \beta_{ij} F_{jt} + \sum_{T=-1}^{1} \gamma_{iT} D_T + \varepsilon_{it}$ where R_{it} is the excess return over the one month treasury bill rate on the security for event i on day t; F_{jt} are the excess returns on the market ($MKTRF$), size (SMB), value (HML), momentum (UMD), profitability(RMW), and investment (CMA) risk factors (Fama, 2015) for day t, D_T is a dummy variable equal to one on day τ in the event window [-1, 1], and zero otherwise; and e_{it} is the error term. Abnormal returns are summed over the event window to compute cumulative abnormal returns. Significance of the means (medians) as determined by a two-tailed t-test (sign test) is highlighted with * for 10% level, ** for 5% level, and *** for 1% level.

	1997-2015 Overall				1997-2015 Excluding Recession			
	Mean	p	Median	p	Mean	p	Median	p
CAR	-0.0071***	0.0008	-0.0041***	0.0092	-0.0056***	0.0004	-0.0040**	0.0222
t-1	-0.0008	0.3669	-0.0005	0.4977	-0.0003	0.7205	-0.0006	0.4710
t=0	-0.0055**	<.0001	-0.0035***	<.0001	-0.0053***	<.0001	-0.0033***	<.0001
t+1	-0.0008	0.5956	0.0003	0.6512	0.0000	0.9748	0.0000	0.9044
	1997-2007							
	Mean	p	Median	p	Mean	p	Median	p
CAR	-0.0079***	0.0035	-0.0052*	0.0901	-0.0074**	0.0110	-0.0050	0.2065
t-1	-0.0025	0.1815	-0.0016	0.4228	-0.0016	0.3130	-0.0018	0.2853
t=0	-0.0057***	0.0007	-0.0039***	0.0031	-0.0052***	0.0037	-0.0033**	0.0148
t+1	0.0003	0.8535	-0.0003	0.9291	-0.0005	0.7698	-0.0015	0.6274
	2008-2015							
	Mean	p	Median	p	Mean	p	Median	p
CAR	-0.0066**	0.0308	-0.0032*	0.0570	-0.0046**	0.0139	-0.0032*	0.0661
t-1	0.0003	0.7363	-0.0001	0.8838	0.0005	0.5233	0.0000	1.0000
t=0	-0.0053***	<.0001	-0.0033***	0.0007	-0.0054***	<.0001	-0.0033***	0.0007
t+1	-0.0016	0.4984	0.0008	0.4647	0.0003	0.7855	0.0005	0.5408

Table A.2. Mean and median CAR by characteristic and industry, Six Factor Model

The mean and median cumulative abnormal return is presented by attack characteristic and industry. Abnormal returns are estimated from regression model $R_{it} = \alpha_i + \sum \beta_{ij} F_{jt} + \sum_{T=-1}^{1} \gamma_{iT} D_T + \varepsilon_{it}$ where R_{it} is the excess return over the one month treasury bill rate on the security for event *i* on day *t*; F_{jt} are the excess returns on the market ($MKTRF$), size (SMB), value (HML), momentum (UMD), profitability(RMW), and investment (CMA) risk factors (Fama and French, 2015) for day t, D_T is a dummy variable equal to one on day τ in the event window [-1, 1], and zero otherwise; and ε_{it} is the error term. Abnormal returns are summed over the three-day event window [-1, 1] to compute cumulative abnormal returns. Significance of the means (medians) as determined by a two tailed t-test (sign test) is highlighted with * for 10% level, ** for 5% level, and *** for 1% level.

	Overall						Excluding Recession				
	N	Mean	p	Median	p		N	Mean	p	Median	p
Overall	313	-0.0071***	0.0008	-0.0041***	0.0092		277	-0.0056***	0.0004	-0.0040**	0.0222
Disrupt	110	-0.0061**	0.0203	-0.0040	0.1046		95	-0.0058**	0.0334	-0.0040	0.2181
Information	156	-0.0093**	0.0135	-0.0037**	0.0450		141	-0.0068***	0.0052	-0.0042**	0.0429
Integrity	47	-0.0024	0.3580	-0.0042	0.7709		41	-0.0015	0.5829	-0.0020	1.0000
Hacktivism	22	0.0012	0.7744	0.0007	0.8318		22	0.0012	0.7744	0.0007	0.8318
State Sponsored	25	-0.0050	0.2050	-0.0058	0.4244		25	-0.0050	0.2050	-0.0058	0.4244
Cybercrime	266	-0.0080***	0.0011	-0.0042***	0.0083		230	-0.0064***	0.0005	-0.0042**	0.0208
First Party at Fault	208	-0.0082***	0.0052	-0.0042**	0.0441		177	-0.0059***	0.0034	-0.0042*	0.0979
Third Party at Fault	105	-0.0050**	0.0466	-0.0025	0.1180		100	-0.0052**	0.0468	-0.0029	0.1332
Account	49	-0.0058*	0.0722	-0.0046**	0.0444		45	-0.0075**	0.0236	-0.0090**	0.0357
Identity	21	-0.0035	0.4598	0.0014	0.6636		17	0.0021	0.5680	0.0030	0.3323
Payment	62	-0.0149*	0.0791	-0.0045	0.2529		55	-0.0087**	0.0376	-0.0048	0.1770
Proprietary	23	-0.0033	0.5684	-0.0033	0.6776		23	-0.0033	0.5684	-0.0033	0.6776
Previously Hacked	143	-0.0027	0.1520	-0.0041**	0.0444		128	-0.0029	0.1130	-0.0040*	0.0630
First Hack	170	-0.0108***	0.0024	-0.0040	0.1070		149	-0.0080***	0.0014	-0.0030	0.1898
Consumer Non Durables	21	-0.0090**	0.0478	-0.0118	0.1892		18	-0.0099*	0.0601	-0.0119	0.2379
Durables and Manuft.	28	-0.0053	0.2873	-0.0043	0.3449		27	-0.0058	0.2591	-0.0044	0.2478
Technology	97	-0.0076***	0.0075	-0.0056**	0.0417		81	-0.0062**	0.0263	-0.0055	0.1821
Telecom and TV	31	-0.0050	0.3054	-0.0020	1.0000		27	-0.0059	0.2878	-0.0020	1.0000
Wholesale and Retail	31	-0.0066	0.1816	-0.0030	0.4731		29	-0.0081	0.1191	-0.0049	0.2649
Finance	68	-0.0120	0.1198	-0.0028	0.3961		64	-0.0055	0.1558	-0.0014	0.5323
Other	37	0.0006	0.8868	0.0014	1.0000		31	0.0008	0.8254	0.0014	1.0000

A.3. Mean and median differences in CAR across characteristic subgroups, Six Factor Model

Differences in the mean CAR between attacks with the noted characteristics and all others is shown along with the results of a two-tailed student t-test and a Wilcoxon Rank Sum Test. CARs are estimated using the Five Factor asset pricing model. Shapiro-Wilks tests (not shown) indicate non-normality for all difference tests, indicating that the Wilcoxon results may be more appropriate. Results for the full sample and excluding those events whose [-130,130] estimation window overlap a NBER defined recession are shown. Dif. refers to Difference.

	Overall							Excluding Recession					
	Mean Dif.	T	p-value	Median Dif.	W	p-value		Mean Dif.	T	p-value	Median Dif.	W	p-value
Disrupt	0.0016	0.42	0.6769	0.0001	17097	0.8216		-0.0002	-0.06	0.9502	-0.0003	13223	0.9780
Information	-0.0043	-1.03	0.3033	0.0003	24239	0.7527		-0.0023	-0.72	0.4714	-0.0003	19387	0.4697
Integrity	0.0056	1.59	0.1138	-0.0001	7805	0.4575		0.0049	1.49	0.1396	0.0020	6164	0.3274
Hacktivism	0.0090	1.90	0.0653	0.0049	3931	0.2452		0.0074	1.66	0.1070	0.0049	3471	0.2535
State Sponsored	0.0023	0.51	0.6108	-0.0019	3857	0.8765		0.0007	0.16	0.8718	-0.0023	3391	0.8271
Cybercrime	-0.0059	-1.59	0.1149	-0.0022	7788	0.4756		-0.0043	-1.27	0.2075	-0.0022	6862	0.5121
First Party at Fault	-0.0032	0.83	0.4047	-0.0017	16592	0.8881		0.0007	-0.23	0.8210	-0.0013	13890	0.9882
Account	0.0016	0.39	0.6975	-0.0007	7221	0.4183		-0.0023	-0.62	0.5380	-0.0057	5545	0.1502
Identity	0.0039	0.76	0.4513	0.0056	3551	0.5273		0.0082	2.09	0.0473	0.0072	2825	0.1495
Payment	-0.0097	-1.14	0.2591	-0.0005	9445	0.6515		-0.0038	-0.86	0.3944	-0.0012	7195	0.3988
Proprietary	0.0042	0.69	0.4975	0.0008	3917	0.4652		0.0026	0.45	0.6502	0.0007	3458	0.4795
First Hack	-0.0081**	-2.04	0.0422	0.0000	23375	0.2478		-0.0051*	-1.67	0.0951	0.0010	18423	0.3437
Consumer Non Durables	-0.0021	-0.43	0.6729	-0.0083	2808	0.2236		-0.0046	-0.72	0.4714	-0.0087	2043	0.1641
Durables and Manuft.	0.0020	0.37	0.7142	-0.0006	4384	0.9799		-0.0002	-0.04	0.9684	-0.0011	3657	0.8093
Technology	-0.0008	-0.19	0.8492	-0.0029	14554	0.363		-0.0008	-0.23	0.8156	-0.0023	11057	0.7399
Telecom and TV	0.0024	0.45	0.6526	0.0022	5066	0.6784		-0.0002	-0.05	0.9631	0.0022	3829	0.8487
Wholesale and Retail	0.0006	0.11	0.9104	0.0011	4805	0.8978		-0.0027	-0.53	0.5961	-0.0011	3776	0.5335
Finance	-0.0062	-0.80	0.4289	0.0014	11021	0.6022		0.0001	0.03	0.9758	0.0028	9289	0.4855
Other	0.0088*	1.85	0.0687	0.0059	6503	0.1807		0.0072*	1.84	0.0729	0.0057	4852	0.1979

A.4. Mean and median differences by subgroup over time, Six Factor Model

Differences in mean CARs between the sub period 1997 to 2007 and sub period 2008 to 2015 are shown along with the results of a two tailed student t-test and a Wilcoxon Rank Sum Test. CARs are estimated using the Five Factor asset pricing model. Shapiro-Wilks tests are conducted on each subgroup by period and those groups which are not significantly non-normal are indicated with a *. Student t-test results are appropriate for these groups. Reported t-values assume either unequal or equal variance as appropriate based on an equality of variance (Folded F) test. For all others, Wilcoxon results may be more appropriate. Results for the full sample and excluding those events whose [-130,130] estimation window overlap a NBER defined recession are shown. Dif. refers to Difference.

	Overall						Excluding Recession					
	Mean Dif.	**T**	**p-value**	**Median Dif.**	**W**	**p-value**	**Mean Dif.**	**T**	**p-value**	**Median Dif.**	**W**	**p-value**
Overall	0.0013	0.33	0.7422	0.0019	19174	0.4397	0.0028	0.84	0.4030	0.0018	14454	0.6666
Disrupt	-0.0004	-0.06	0.9523	0.0017	1523	0.8679	0.0026	0.47	0.6426	0.0025	1007	0.6722
Information	0.0042	0.55	0.5812	0.0019	2680	0.5414	0.0056	0.79	0.4331	0.0024	1901	0.6555
Integrity	0.0059	0.82	0.4189	0.0029	142	0.4500	-0.0036	-0.34	0.7350	-0.0056	65	0.9405
Hacktivism*	-0.0135	-0.67	0.5113	-0.0138	18	0.3550	-0.0135	-0.67	0.5113	-0.0138	18	0.3550
Cybercrime	0.0002	0.03	0.9738	0.0020	16258	0.4939	0.0023	0.62	0.5352	0.0019	11950	0.7251
Third Party at Fault	0.0021	0.43	0.6693	0.0023	1580	0.9464	0.0006	0.13	0.8987	0.0021	1414	0.7049
First Party at Fault	0.0042	0.71	0.4793	-0.0003	4865	0.2155	0.0070	1.21	0.2335	-0.0007	2832	0.2996
Account*	-0.0061	-0.53	0.6007	-0.0011	116	0.5740	0.0059	0.27	0.7914	0.0065	18	0.7306
Identity*	0.0133	1.32	0.2009	0.0159	53	0.3421	0.0086	0.6	0.6027	0.0153	22	0.5786
Payment	-0.0098	-0.73	0.4678	-0.0079	650	0.7700	-0.0062	-0.89	0.3772	-0.0093	546	0.4599
Proprietary	0.0304	1.42	0.2413	0.0144	31	0.1884	0.0304	1.42	0.2413	0.0144	31	0.1884
Previously Hacked	0.0012	0.31	0.7551	0.0016	3504	0.6866	0.0014	0.35	0.7277	0.0007	2679	0.8812
First Hack	0.0000	-0.01	0.9950	0.0023	6334	0.6090	0.0031	0.6	0.5517	0.0026	4722	0.7667
Consumer Non Durables*	-0.0082	-0.95	0.3523	-0.0029	124	0.3531	-0.0093	-0.93	0.3653	-0.0097	88	0.3212
Durables and Manuft.*	-0.0028	-0.31	0.7620	-0.0030	176	0.9450	-0.0017	-0.18	0.8576	-0.0015	154	1.0000
Technology	0.0125**	2.26	0.0262	0.0039	2088	0.0570	0.0140**	2.56	0.0131	0.0065*	1363	0.0655
Telecom and TV*	0.0161*	1.98	0.0613	0.0136*	254	0.0681	0.0155	1.69	0.1082	0.0140	181	0.2024
Wholesale and Retail	-0.0191**	-2.42	0.0371	-0.0208*	95	0.0618	-0.0191**	-2.42	0.0371	-0.0207	68	0.1117
Finance	-0.0161	-1.22	0.2285	-0.0076	940	0.1535	-0.0064	-0.73	0.4691	-0.0102	846	0.1716
Other*	0.0050	0.54	0.5950	0.0007	182	0.7990	-0.0033	-0.38	0.7073	-0.0034	118	0.7968

A.5. Cross sectional regression of CAR, Six Factor Model

Results are reported for a cross sectional regression of determinants of cumulative abnormal returns. CARs used are calculated using a Five Factor asset pricing model. Firm size is the natural logarithm of firm size (in thousands) on the day of the attack. Days passed is the natural logarithm of the number of calendar days since the last attack. Trailing events count the number of cyber-attacks on publicly traded companies in the last 30 trading days. Number of records is the natural logarithm of the number of records lost in an attack. The remaining variables are dummies for the stated attack, industry, or time attribute. Results are shown for OLS estimates with ordinary and heteroscedasticity consistent standard errors. Robust regressions are conducted using the M-estimation method. Significance is highlighted with * for 10% level, ** for 5% level, and *** for 1% level. Std. Error refers to standard error.

				Heteroscedasticity Consistent			Robust Regression		
		Standard		Standard				Standard	
Variable	Coefficient	Error	p-value	Error	p-value		Coefficient	Error	p-value
Intercept	-0.0792	0.0363	0.0298	0.0365	0.0307		-0.0351	0.0216	0.1044
Firm Size	0.0043**	0.0014	0.0017	0.0017	0.0103		0.0019**	0.0008	0.0180
Disrupt	0.0012	0.0074	0.8688	0.0060	0.8395		-0.0005	0.0044	0.9080
Identity	0.0026	0.0109	0.8104	0.0081	0.7475		0.0015	0.0065	0.8197
Account	-0.0039	0.0084	0.6449	0.0060	0.5166		-0.0054	0.0050	0.2838
Payment	-0.0114	0.0087	0.1886	0.0108	0.2911		-0.0058	0.0052	0.2596
Proprietary	0.0002	0.0097	0.9818	0.0071	0.9751		0.0020	0.0058	0.7263
Hacktivism	0.0062	0.0109	0.5710	0.0050	0.2168		0.0064	0.0065	0.3222
Crime	0.0012	0.0092	0.8973	0.0055	0.8302		0.0045	0.0055	0.4126
First Party	-0.0091**	0.0062	0.1439	0.0046	0.0487		-0.0046	0.0037	0.2147
First Hack	-0.0037	0.0049	0.4504	0.0036	0.3019		-0.0012	0.0029	0.6844
Consumer Non Durables	-0.0098	0.0104	0.3484	0.0067	0.1442		-0.0099	0.0062	0.1121
Durables and Manuft.	-0.0124	0.0097	0.2013	0.0082	0.1339		-0.0071	0.0058	0.2154
Technology	-0.0154**	0.0077	0.0474	0.0064	0.0175		-0.0099**	0.0046	0.0307
Telecom and TV	-0.0155*	0.0093	0.0986	0.0080	0.0540		-0.0080	0.0056	0.1492
Wholesale and Retail	-0.0055	0.0093	0.5582	0.0077	0.4790		-0.0044	0.0055	0.4224
Finance	-0.0188*	0.0079	0.0174	0.0103	0.0695		-0.0062	0.0047	0.1866
Days Passed	-0.0011	0.0015	0.4554	0.0012	0.3440		-0.0007	0.0009	0.4174
Trailing Events	-0.0017***	0.0007	0.0146	0.0007	0.0091		-0.0013***	0.0004	0.0027
1997-2007	-0.0016	0.0061	0.7984	0.0067	0.8150		-0.0022	0.0036	0.5422
Recession Window	-0.0109	0.0071	0.1254	0.0141	0.4411		-0.0007	0.0042	0.8761
Number of Records	0.0003	0.0005	0.5771	0.0005	0.5459		-0.0001	0.0003	0.7902

Online Appendix B: Results using data set including confounded events

Table B.1: Mean and median CAR by event day, including confounded events

The mean and median abnormal and cumulative abnormal returns are presented by time period for the event window [-1, 1]. Abnormal returns are estimated from regression model $R_{it} = \alpha_i + \sum \beta_{ij} F_{jt} + \sum_{T=-1}^{1} \gamma_{iT} D_T + \varepsilon_{it}$ where R_{it} is the excess return over the one month treasury bill rate on the security for event i on day t; F_{jt} are the excess returns on the market ($MKTRF$), size (SMB), value (HML), profitability(RMW), and investment (CMA) risk factors (Fama, 2015) for day t, D_T is a dummy variable equal to one on day τ in the event window [-1, 1], and zero otherwise; and ε_{it} is the error term. Abnormal returns are summed over the event window to compute cumulative abnormal returns. Significance of the means (medians) as determined by a two-tailed t-test (sign test) is highlighted with * for 10% level, ** for 5% level, and *** for 1% level.

	1997-2015 Overall					1997-2015 Excluding Recession			
	Mean	p	Median	p		Mean	p	Median	p
CAR	-0.0057**	0.0109	-0.0030*	0.0583		-0.0042***	0.0094	-0.0029	0.1076
t-1	-0.0012	0.2699	-0.0004	0.6266		-0.0005	0.6618	-0.0004	0.5657
t=0	-0.0044***	0.0001	-0.0032***	<.0001		-0.0042***	<.0001	-0.0031***	<.0001
t+1	0.0000	0.9881	0.0007	0.7869		0.0005	0.6369	0.0000	1
	1997-2007								
	Mean	p	Median	p		Mean	p	Median	p
CAR	-0.0048*	0.099	-0.0027	0.2684		-0.0051*	0.0892	-0.0022	0.4035
t-1	-0.0029	0.2036	-0.0012	0.7985		-0.0022	0.3146	-0.0016	0.5159
t=0	-0.0037**	0.0407	-0.0033**	0.0329		-0.0036*	0.0691	-0.0031*	0.0507
t+1	0.0018	0.3062	-0.0005	0.7985		0.0007	0.7307	-0.0013	0.4035
	2008-2015								
	Mean	p	Median	p		Mean	p	Median	p
CAR	-0.0062**	0.0495	-0.0030	0.1413		-0.0036**	0.0492	-0.0030	0.1879
t-1	-0.0001	0.9074	-0.0004	0.7264		0.0006	0.5318	-0.0003	0.8838
t=0	-0.0049***	0.0012	-0.0032***	0.0006		-0.0046***	0.0002	-0.0032***	0.0007
t+1	-0.0012	0.5978	0.0011	0.5287		0.0003	0.7478	0.0010	0.5587

Table B.2: Mean and median CAR by characteristic and industry, including confounded events

The mean and median cumulative abnormal return is presented by attack characteristic and industry. Abnormal returns are estimated from regression model $R_{it} = \alpha_i + \sum \beta_{ij} F_{jt} + \sum_{T=-1}^{1} \gamma_{iT} D_T + \varepsilon_{it}$ where R_{it} is the excess return over the one month treasury bill rate on the security for event i on day t; F_{jt} are the excess returns on the market ($MKTRF$), size (SMB), value (HML), profitability(RMW), and investment (CMA) risk factors (Fama and French, 2015) for day t, D_T is a dummy variable equal to one on day τ in the event window [-1, 1], and zero otherwise; and e_{it} is the error term. Abnormal returns are summed over the three-day event window [-1, 1] to compute cumulative abnormal returns. Significance of the means (medians) as determined by a two tailed t-test (sign test) is highlighted with * for 10% level, ** for 5% level, and *** for 1% level.

	Overall					Excluding Recession				
	N	Mean	p	Median	p	N	Mean	p	Median	p
Overall	342	-0.0057**	0.0109	-0.0030*	0.0583	303	-0.0042***	0.0094	-0.0029	0.1076
Disrupt	120	-0.0057*	0.0893	-0.0028	0.2352	103	-0.0039	0.1900	-0.0015	0.4307
Information	168	-0.0088**	0.0171	-0.0041*	0.0757	153	-0.0069***	0.0032	-0.0044*	0.0750
Integrity	54	0.0042	0.2197	0.0021	0.8919	47	0.0037	0.2248	0.0021	0.7709
Hacktivism	24	0.0011	0.7788	0.0016	0.8388	24	0.0011	0.7788	0.0016	0.8388
State Sponsored	25	-0.0035	0.4319	-0.0032	0.6900	25	-0.0035	0.4319	-0.0032	0.6900
Cybercrime	293	-0.0064**	0.0120	-0.0030**	0.0468	254	-0.0048***	0.0096	-0.0030*	0.0900
First Party at Fault	225	-0.0079**	0.0111	-0.0037**	0.0453	192	-0.0056***	0.0060	-0.0036*	0.0967
Third Party at Fault	117	-0.0014	0.5853	-0.0009	0.7117	111	-0.0018	0.5016	-0.0009	0.7044
Account	56	-0.0026	0.4120	-0.0029	0.1409	52	-0.0038	0.2513	-0.0043	0.1263
Identity	23	-0.0065	0.1646	0.0012	1.0000	19	-0.0023	0.5671	0.0013	0.6476
Payment	66	-0.0146*	0.0804	-0.0045	0.2678	59	-0.0102**	0.0110	-0.0047	0.1925
Proprietary	23	-0.0047	0.4224	-0.0044	1.0000	23	-0.0047	0.4224	-0.0044	1.0000
Previously Hacked	159	-0.0028	0.1585	-0.0034	0.1124	143	-0.0027	0.1662	-0.0032	0.1807
First Hack	183	-0.0082**	0.0312	-0.0025	0.3007	160	-0.0056**	0.0281	-0.0021	0.3846
Consumer Non Durables	20	-0.0058	0.1859	-0.0086	0.2632	17	-0.0063	0.2200	-0.0092	0.3323
Durables and Manuft.	29	-0.0041	0.4385	-0.0040	0.4583	28	-0.0046	0.3888	-0.0045	0.3449
Technology	109	-0.0053*	0.0990	-0.0056*	0.0842	92	-0.0045	0.1504	-0.0048	0.2513
Telecom and TV	33	-0.0021	0.6641	0.0012	1.0000	28	-0.0048	0.3468	-0.0010	1.0000
Wholesale and Retail	34	-0.0068	0.1928	-0.0053	0.6076	32	-0.0088	0.1010	-0.0071	0.3771
Finance	70	-0.0144*	0.0769	-0.0012	0.7202	66	-0.0047	0.2164	-0.0007	0.9022
Other	47	0.0039	0.4108	0.0013	1.0000	40	0.0026	0.4695	0.0019	0.8746

Table B.3: Cross sectional regression of CAR, including confounded events

Results are reported for a cross sectional regression of determinants of cumulative abnormal returns. CARs used are calculated using a Five Factor asset pricing model. Firm size is the natural logarithm of firm size (in thousands) on the day of the attack. Days passed is the natural logarithm of the number of calendar days since the last attack. Trailing events count the number of cyber-attacks on publicly traded companies in the last 30 trading days. Number of records is the natural logarithm of the number of records lost in an attack. The remaining variables are dummies for the stated attack, industry, or time attribute. Results are shown for OLS estimates with ordinary and heteroscedasticity consistent standard errors. Robust regressions are conducted using the M-estimation method. Significance is highlighted with * for 10% level, ** for 5% level, and *** for 1% level. Std. Error refers to standard error.

					Heteroscedasticity Consistent			Robust Regression	
Variable		Coefficient	Standard Error	p-value	Standard Error	p-value	Coefficient	Standard Error	p-value
Intercept		-0.0486	0.0386	0.2087	0.0453	0.2840	-0.0259	0.0224	0.247
Firm Size		0.0035*	0.0014	0.0167	0.0019	0.0653	0.0018**	0.0008	0.0309
Disrupt		-0.0091	0.0079	0.2517	0.0080	0.2556	-0.0061	0.0046	0.1883
Identity		0.0051	0.0114	0.6515	0.0137	0.7076	-0.0061	0.0066	0.3584
Account		0.0015	0.0090	0.8681	0.0097	0.8783	-0.0075	0.0052	0.1529
Payment		-0.0069	0.0096	0.4695	0.0103	0.4999	-0.0111**	0.0056	0.0453
Proprietary		-0.0108	0.0107	0.3114	0.0079	0.1729	-0.0037	0.0062	0.5471
Hacktivism		0.0038	0.0119	0.7469	0.0064	0.5497	0.0037	0.0069	0.5916
Crime		-0.0046	0.0101	0.6509	0.0074	0.5326	0.0028	0.0059	0.6369
First Party		-0.0078	0.0067	0.2493	0.0053	0.1401	-0.0063	0.0039	0.107
First Hack		-0.0037	0.0052	0.4840	0.0042	0.3863	-0.0004	0.003	0.8891
Consumer Non Durables		-0.0124*	0.0117	0.2892	0.0073	0.0918	-0.0085	0.0068	0.2096
Durables and Manuft.		-0.0116	0.0106	0.2722	0.0075	0.1218	-0.009	0.0061	0.1415
Technology		-0.0166**	0.0082	0.0453	0.0075	0.0269	-0.011**	0.0048	0.0214
Telecom and TV		-0.0150*	0.0100	0.1345	0.0081	0.0642	-0.0083	0.0058	0.1513
Wholesale and Retail		-0.0120	0.0100	0.2315	0.0094	0.2009	-0.0071	0.0058	0.2196
Finance		-0.0277**	0.0085	0.0013	0.0129	0.0327	-0.0079	0.005	0.1131
Days Passed		-0.0011	0.0016	0.4784	0.0017	0.5023	-0.0003	0.0009	0.7663
Trailing Events		-0.0009	0.0007	0.2008	0.0006	0.1506	-0.0007*	0.0004	0.0838
1997-2007		0.0031	0.0067	0.6417	0.0081	0.7011	-0.0012	0.0039	0.7531
Recession Window		-0.0099	0.0076	0.1951	0.0144	0.4943	-0.0017	0.0044	0.6988
Number of Records		-0.0015	0.0006	0.0131	0.0014	0.2772	-0.0002	0.0003	0.6194

Online Appendix C: Miscellaneous

Table C.1: Mean and Median CAR by Characteristic and Industry, 1997-2007

The mean and median cumulative abnormal return is presented by attack characteristic and industry. Abnormal returns are estimated from regression model $R_{it} = \alpha_i + \sum \beta_{ij} F_{jt} + \sum_{T=-1}^{1} \gamma_{iT} D_T + \varepsilon_{it}$ where R_{it} is the excess return over the one month treasury bill rate on the security for event *i* on day *t*; F_{jt} are the excess returns on the market ($MKTRF$), size (SMB), value (HML), profitability(RMW), and investment (CMA) risk factors (Fama and French, 2015) for day t, D_T is a dummy variable equal to one on day τ in the event window [-1, 1], and zero otherwise; and ε_{it} is the error term. Abnormal returns are summed over the three-day event window [-1, 1] to compute cumulative abnormal returns. Significance of the means (medians) as determined by a two tailed t-test (sign test) is highlighted with * for 10% level, ** for 5% level, and *** for 1% level.

	Overall						Excluding Recession				
	N	Mean	p	Median	p		N	Mean	p	Median	p
Overall	126	-0.0075***	0.0043	-0.0049*	0.0901		106	-0.0067**	0.0150	-0.0040	0.2065
Disrupt	83	-0.0051*	0.0752	-0.0035	0.1875		75	-0.0053*	0.0744	-0.0029	0.2480
Information	36	-0.0130**	0.0375	-0.0053	0.4050		28	-0.0115*	0.0900	-0.0059	0.5716
Integrity	7	-0.0068	0.3649	-0.0072	1.0000		3	0.0035	0.6988	0.0048	1.0000
Hacktivism	1	0.0164	.	0.0164	1.0000		1	0.0164	.	0.0164	1.0000
State Sponsored	0	.	.	.	.		0	.	.	.	.
Cybercrime	125	-0.0077***	0.0036	-0.0049*	0.0732		105	-0.0069**	0.0126	-0.0044	0.1716
First Party at Fault	51	-0.0117**	0.0156	-0.0060*	0.0919		35	-0.0116**	0.0368	-0.0060	0.1755
Third Party at Fault	75	-0.0046	0.1185	-0.0013	0.4887		71	-0.0042	0.1667	-0.0009	0.6353
Account	4	-0.0021	0.7199	-0.0037	0.6250		1	-0.0136	.	-0.0136	1.0000
Identity	6	-0.0110	0.3586	-0.0125	0.6875		3	-0.0038	0.8009	-0.0110	1.0000
Payment	20	-0.0092	0.1671	0.0012	0.8238		18	-0.0048	0.2208	0.0012	0.8145
Proprietary	4	-0.0281	0.2503	-0.0105	0.1250		4	-0.0281	0.2503	-0.0105	0.1250
Previously Hacked	50	-0.0042	0.1868	-0.0048	0.1189		42	-0.0045	0.1511	-0.0040	0.1641
First Hack	76	-0.0096**	0.0118	-0.0049	0.4222		64	-0.0081**	0.0468	-0.0031	0.7080
Consumer Non Durables	10	-0.0035	0.5886	-0.0086	0.7539		8	-0.0034	0.6624	-0.0086	0.7266
Durables and Manuft.	12	-0.0028	0.5157	-0.0022	0.7744		11	-0.0042	0.3515	-0.0035	0.5488
Technology	48	-0.0129***	0.0063	-0.0085**	0.0293		38	-0.0117**	0.0112	-0.0085*	0.0730
Telecom and TV	18	-0.0120	0.1052	-0.0118	0.4807		16	-0.0124	0.1379	-0.0129	0.8036
Wholesale and Retail	4	0.0107	0.2087	0.0123	0.6250		3	0.0098	0.4055	0.0113	1.0000
Finance	24	-0.0027	0.7083	0.0012	0.8388		23	-0.0026	0.7294	0.0013	0.6776
Other	10	-0.0014	0.8456	0.0009	1.0000		7	0.0061	0.1949	0.0031	1.0000

Table C.2: Mean and Median CAR by Characteristic and Industry, 2008-2015

The mean and median cumulative abnormal return is presented by attack characteristic and industry. Abnormal returns are estimated from regression model $R_{it} = \alpha_i + \sum \beta_{ij} F_{jt} + \sum_{T=-1}^{1} \gamma_{iT} D_T + \varepsilon_{it}$ where R_{it} is the excess return over the one month treasury bill rate on the security for event i on day t; F_{jt} are the excess returns on the market ($MKTRF$), size (SMB), value (HML), profitability(RMW), and investment (CMA) risk factors (Fama and French, 2015) for day t, D_T is a dummy variable equal to one on day τ in the event window [-1, 1], and zero otherwise; and ε_{it} is the error term. Abnormal returns are summed over the three-day event window [-1, 1] to compute cumulative abnormal returns. Significance of the means (medians) as determined by a two tailed t-test (sign test) is highlighted with * for 10% level, ** for 5% level, and *** for 1% level.

	Overall						Excluding Recession				
	N	Mean	p	Median	p		N	Mean	p	Median	p
Overall	187	-0.0065**	0.0392	-0.0034	0.0403		171	-0.0050***	0.0069	-0.0035**	0.0465
Disrupt	27	-0.0064	0.1848	-0.0030	0.4421		20	-0.0039	0.3976	-0.0023	0.8238
Information	120	-0.0080*	0.0876	-0.0041	0.0824		113	-0.0061**	0.0147	-0.0043	0.5940
Integrity	40	-0.0019	0.4959	-0.0027	0.6358		38	-0.0022	0.4473	-0.0027	0.6271
Hacktivism	21	0.0002	0.9571	0.0012	1.0000		21	0.0002	0.9571	0.0012	1.0000
State Sponsored	25	-0.0059	0.1380	-0.0067	0.4244		25	-0.0059	0.1380	-0.0067	0.4244
Cybercrime	141	-0.0076*	0.0618	-0.0035	0.0429		125	-0.0057**	0.0130	-0.0040**	0.0487
First Party at Fault	157	-0.0069*	0.0618	-0.0032	0.1102		142	-0.0050**	0.0178	-0.0033	0.1534
Third Party at Fault	30	-0.0044	0.2184	-0.0040	0.2005		29	-0.0050	0.1695	-0.0046	0.1360
Account	45	-0.0063*	0.0735	-0.0053	0.0357		44	-0.0074**	0.0306	-0.0078**	0.0226
Identity	15	-0.0010	0.8243	0.0029	0.3018		14	0.0025	0.4468	0.0032	0.1796
Payment	42	-0.0160	0.2100	-0.0049	0.0884		37	-0.0109*	0.0625	-0.0050**	0.0470
Proprietary	19	0.0003	0.9563	0.0070	0.6476		19	0.0003	0.9563	0.0070	0.6476
Previously Hacked	93	-0.0025	0.2856	-0.0032	0.2997		86	-0.0024	0.2737	-0.0033	0.3318
First Hack	94	-0.0105*	0.0733	-0.0040	0.0790		85	-0.0076**	0.0106	-0.0046*	0.0821
Consumer Non Durables	11	-0.0125*	0.0643	-0.0124	0.2266		10	-0.0135*	0.0697	-0.0189	0.3438
Durables and Manuft.	16	-0.0083	0.3277	-0.0073	0.4545		16	-0.0083	0.3277	-0.0073	0.4545
Technology	49	-0.0017	0.5664	-0.0030	0.3916		43	0.0001	0.9752	-0.0017	0.7608
Telecom and TV	13	0.0039	0.1839	0.0036	0.5811		11	0.0027	0.3951	0.0012	1.0000
Wholesale and Retail	27	-0.0088	0.1188	-0.0095	0.2478		26	-0.0106*	0.0601	-0.0100	0.1686
Finance	44	-0.0183	0.1022	-0.0033	0.1742		41	-0.0082*	0.0600	-0.0032	0.2110
Other	27	0.0051	0.4805	0.0013	1.0000		24	-0.0002	0.9636	0.0003	1.0000

Table C.3: Pairwise F-Tests for Cross Sectional Regression Beta Coefficients

Results of a hypothesis test for the equality of the listed pairs of regression coefficients are shown. Main regression results are shown in Table (7). Regression coefficients represent the mean cumulative abnormal return when experiencing a cyber-attack for each subgroup. Results using the traditional OLS model are given with F-test, while the HEC model results are given with a Chi-Square test. Results indicate a failure to reject equality for all pairs.

Group 1	Group 2	F	p-value	Chi-Square	p-value
Hacktivism	Crime	0.30	0.5833	0.99	0.3200
Account	Identity	0.42	0.5153	0.95	0.3309
Account	Payment	1.02	0.3139	0.73	0.3933
Account	Proprietary	0.15	0.7020	0.31	0.5774
Identity	Payment	2.05	0.1531	1.90	0.1678
Identity	Proprietary	0.03	0.8527	0.07	0.7916
Payment	Proprietary	1.08	0.2989	1.23	0.2680
Consumer Non Durables	Durables and Manuft.	0.06	0.8130	0.12	0.7295
Consumer Non Durables	Technology	0.35	0.5567	0.88	0.3484
Consumer Non Durables	Telecom and TV	0.28	0.5981	0.59	0.4406
Consumer Non Durables	Wholesale and Retail	0.14	0.7074	0.23	0.6283
Consumer Non Durables	Finance	0.83	0.3627	0.88	0.3489
Durables and Manuft.	Technology	0.13	0.7214	0.22	0.6428
Durables and Manuft.	Telecom and TV	0.09	0.7582	0.19	0.6627
Durables and Manuft.	Wholesale and Retail	0.41	0.5218	0.44	0.5055
Durables and Manuft.	Finance	0.49	0.4864	0.59	0.4437
Technology	Telecom and TV	0.00	0.9915	0.00	0.9890
Technology	Wholesale and Retail	1.26	0.2627	1.41	0.2345
Technology	Finance	0.26	0.6099	0.19	0.6651
Telecom and TV	Wholesale and Retail	0.93	0.3364	1.01	0.3154
Telecom and TV	Finance	0.16	0.6900	0.20	0.6529
Retail	Finance	2.53	0.1125	1.25	0.2631