Cyber terrorism cases and stock market valuation effects

Katherine Taken Smith
Department of Management and Marketing, Texas A&M University – Corpus Christi, Corpus Christi, Texas, USA

Lawrence Murphy Smith
Department of Accounting, Texas A&M University – Corpus Christi, Corpus Christi, Texas, USA

Marcus Burger
Department of Accounting, The University of North Carolina at Pembroke, Pembroke, North Carolina, USA, and

Erik S. Boyle
Department of Accounting, Idaho State University, Pocatello, Idaho, USA

Received 3 September 2022
Revised 16 November 2022
5 January 2023
Accepted 6 January 2023

Abstract

Purpose – Cyber terrorism poses a serious technology risk to businesses and the economies they operate in. Cyber terrorism is a digital attack on computers, networks or digital information systems, carried out to coerce people or governments to further the social or political objectives of the attacker. Cyber terrorism is costly in terms of impaired operations and damaged assets. Cyber terrorism harms a firm's reputation, thereby negatively affecting a firm's stock market valuation. This poses grave worries to company management, financial analysts, creditors and investors. This study aims to evaluate the effect of cyber terrorism on the market value of publicly traded firms.

Design/methodology/approach – Financial information was obtained on business firms that were featured in news stories as targets of cyber terrorism. The firm's stock price was recorded for 1, 3 and 7 days before and after the news article. Percentage changes in the firm's stock price were compared to percentage changes in the Dow Jones Index to ascertain whether the firm's stock price went up or down matching the market overall.

Findings – Results indicate that stock prices are significantly negatively affected by news of cyber terrorist attacks on companies. In all three time periods after the cyber terrorist attack, there was a significant negative decline in the stock value relative to the Dow Jones Index. Thus, the market valuation of the firm is damaged. As a result, the shareholders and institutions are financially damaged. Furthermore, exposed system vulnerability may lead to loss of business from consumers who have reduced confidence in the firm's operations.

Practical implications – This paper examines the risks posed by cyber terrorism, including its impact on individual business firms, which in turn affect entire national economic systems. This makes clear the high value of cybersecurity in safeguarding computer systems. Taking steps to avoid being a victim of cyber terrorism is an important aspect of cybersecurity. Preventative steps are normally far less costly than rebuilding an information system after a cyber terrorist attack.

Originality/value – This study is original in examining the effect of cyber terrorism on the stock value of a company.

Keywords Cyber terrorism, Cybersecurity, Electronic markets, Information technology, Market value

Paper type Research paper

Statements and declarations: The authors have no relevant financial or non-financial interests to disclose. The authors have no competing or conflict of interest to declare that is relevant to the content of this article.

Information & Computer Security
Vol. 31 No. 4, 2023
pp. 385-403

2056-4961
DOI 10.1108/ICS-09-2022-0147

Highlights

- Cyber terrorism is a potential threat to all online organizations, including publicly traded firms.
- Cyber terrorism has notable negative effects on firms, such as shut down of online operations.
- Findings indicate that market valuation (stock price) is significantly negatively affected by cyber terrorist attacks.
- Firm managers can learn from the experiences of previous victims of cyber terrorism and bolster their cybersecurity.

Introduction

Cyber terrorism has become one of the world's major concerns, posing a serious, potentially devastating, information technology risk to publicly traded business firms and the economies in which they carry out operations. An act of cyber terrorism involves a digital attack on computers, networks or digital information systems, carried out to intimidate or coerce individuals, businesses or governments to further the social or political objectives of the attacker. Protecting business information systems from internal and external threats, including cyber terrorism, is a vital component of information technology management. Cyber terrorism is costly in terms of impaired business and damaged virtual and physical assets. In addition, cyber terrorism harms a firm's reputation, thereby negatively affecting a firm's stock market valuation. This poses grave worries to a company's customers, company management, financial analysts, creditors and investors.

This study evaluates to what extent cyber terrorism affects the market value of publicly traded firms. While a negative impact might be anticipated, this study quantifies the significance and extent of that impact. This is a unique contribution to research regarding cyber terrorism. Findings indicate that a firm's market valuation (stock price) is significantly negatively affected by news of a cyber terrorist attack. In all three time periods examined following a cyber terrorist attack, there was a significant negative decline in the stock value relative to the Dow Jones Index.

A decline in market valuation shows diminished public confidence in the firm's future business viability. When a firm becomes a victim of cyber terrorism, this reveals that a firm's information system is vulnerable and lacks adequate cybersecurity. For shareholders, individuals, institutions and other stakeholders, a cyber terrorist attack is financially detrimental. Furthermore, exposed system vulnerability may lead to loss of business from consumers who have reduced confidence in the firm being able to carry on its operations, providing products or services.

We structure the remainder of our paper as follows. First, we discuss relevant background literature. Second, we detail our research methodology. Third, we present several case studies. Fourth, we provide our analysis and results. Fifth, we provide some recommendations that companies can use to protect themselves from cyber terrorism attacks. Finally, we offer a conclusion, including limitations of the paper and opportunities for future research.

Literature review

Although cyber terrorism does not have a universally accepted definition in the prior literature (Broeders *et al.*, 2021; Shandler *et al.*, 2022), there are elements that are consistently included. Researchers generally agree that it is a subset of cybercrime (Burger *et al.*, 2020; Beveren, 2001), but they disagree over its exact scope. Collin (1997) is generally credited with

creating the term cyber terrorism, which he used to describe the use of the "virtual world" to attack, threaten or disrupt a government. Gordon and Ford (2006) broadly define cybercrime as any crime facilitated or committed using a computer or other hardware device. Denning (2000, para. 1) provides the first widely accepted definition for cyber terrorism, which she describes as any unlawful attack or threat of attack "against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives."

Denning (2000) further states that only acts that result in physical harm to people or property, or sufficient harm to generate fear, should be considered acts of cyber terrorism. She specifically excludes attacks that are "mainly a costly nuisance" (para. 1). Prior research refers to this as the "pure" definition of cyber terrorism. However, it is difficult to argue that terrorists do not target economies or that economic harm or threat of economic harm are not a source of anxiety or concern for governments or their people, which may warrant an expanded definition of cyber terrorism.

Backhaus *et al.* (2020) investigate the differences in individuals' emotional responses to violent and nonviolent cyber terrorism attacks by running an experiment that evaluates participants' cortisol levels and self-reported anger and anxiety in response to specially designed news report videos demonstrating a terrorist attack. They find that participants' emotional responses and cortisol levels are significantly higher after observing reports of a cyber terrorist attack, but they do not find any significant differences between emotional responses based on whether participants observed a traditional terrorist attack, lethal cyber terrorism attack or nonlethal cyber terrorist attack. In their treatment for a nonlethal cyber terrorist attack, they used a scenario where the attack had only financial repercussions. Backhaus *et al.*'s (2020) findings suggest that cyber terrorism may have broader impacts, including financial market impacts, and that the definition should be expanded to provide for greater consideration and analysis.

Indeed, the National Security Agency's (NSA) definition includes actions taken to "exploit information to gain an advantage" over a government, including to gain "an economic advantage, or to gain insight into [their] military or foreign policy" (NSA, 2021, para. 6). The NSA also includes in its definition actors' actions to "spread their messages of hate and intolerance, and to recruit new members" (para. 7).

Macdonald *et al.* (2019) provide support for the NSA's definition of cyber terrorism. They survey cyber terrorism researchers and find that researchers' definitions for cyber terrorism tend to converge around three core attributes:

(1) a political ideological motive;

(2) a digital means or target; and

(3) fear as an intended outcome.

The target and methods chosen are similar. Some cyber criminals attack their targets for financial gain, although they are also motivated by ego, entertainment and vengeance. While many cyber criminals wish to remain anonymous, cyber terrorists often wish to associate their actions with their ideology to spread their message and recruit new members. Cyber terrorists may be attracted to cybercrime because the internet may allow them to better craft their desired identity, avoid detection and achieve criminal goals over a broader outlet. Furthermore, it may allow for alternative forms of criminal organization and collaboration that provides a wider variation in strategical tactics (Lee *et al.*, 2021). Table 1 summarizes the sources of cybersecurity threats and some common tools used by cyber criminals and hackers.

Threat	Description
Bot-network operators	A hacker methodology where the hacker hijacks computers to form a network focused on attacking other systems to spread malware, hijack additional computers, or bring down another network or server via a distributed denial-of-service (DDoS) attack
Cyber criminals	Black hat hackers that range in sophistication from script kiddies to more sophisticated hacktivists and malicious insiders. Script kiddies are curious novices that pose less threat because of their lack of creativity and knowledge about system vulnerabilities. Hacktivists tend to be more sophisticated users that apply their increased knowledge to their cause. Edward Snowden is among the most well-known hacktivists. Malicious insiders, because of their inside knowledge and access to a system, pose the greatest threat. With little sophistication, a knowledgeable insider with legitimate system access can pose a serious system threat
Cyber terrorists	Cyber criminals that seek to enforce their ideology by destroying, incapacitating, or exploiting critical infrastructure to threaten national security, cause mass casualties, weaken the economy and cause public fear. They may use malware, phishing and other hacking techniques to obtain financial gain and support their efforts. However, they primarily seek to communicate their message and recruit others to their ideology through online acts of terror
Foreign intelligence	Foreign governments use sophisticated hacking techniques to conduct espionage activities. They infiltrate other governments' systems obtain strategic and classified government secrets, including technology. Well-funded and supported, secret agents are among the most sophisticated cyber criminals. They often exploit zero-day system vulnerabilities where the target is unaware of the vulnerability giving it "zero days" to fix the problem and granting the cyber criminals the greatest chance of success
Organized crime	Organized criminals attack systems for financial gain. They use phishing schemes, spam and malware attacks to obtain unauthorized systems access and commit identity theft or online fraud. The attacks are often anonymous and sophisticated to allow the perpetrators to remain hidden and extract greater financial gains
Phishing	A hacker methodology where the hacker sends an electronic message or constructs a website pretending to be a legitimate company or person. The message or website attempts to lure the user to download malware or provide information that the hacker can use for financial gain or to obtain unauthorized access to a system
Spam	A hacker methodology where the hacker sends unsolicited electronic messages to a large number of users. The message may be used to facilitate a phishing scheme but also to sell products or services
Spyware/ malware	Malware is any software intended to do harm. Spyware is specialized form of malware used to monitor the infected hardware's usage and to collect other sensitive information without authorization. The software often contains virus code intended to infect and replicate itself on other hardware

Table 1.
Sources of cybersecurity threats

For purposes of this study, we define cyber terrorism as follows: a digital attack on computers, networks or digital information systems, carried out to intimidate or coerce individuals, businesses or governments to further the social or political objectives of the attacker. Thus, cyber terrorism can be aimed at specific government digital systems, private sector infrastructure systems (e.g. utilities, pipelines, etc.) or private businesses (the focus of this study). Disrupting the operations of private businesses, especially large publicly traded corporations, can not only be very detrimental to specific businesses but also to the economy overall as the ripple of effect of the disruption spreads, affecting other businesses. Many citizens may wish their government leaders would accommodate the political demands of the cyber terrorists. Yet, the literature shows that acceding to terrorist demands is problematic, often leading to other problems (cf., Mendelsohn *et al.*, 2018; Schneider, 2017; Clutterbuck, 1993).

In this study, we build upon prior literature that often focuses on the economic impact of corporate security breaches (Spanos and Angelis, 2016, for a literature review) to include cybercrimes that may have had a more political or ideological purpose than just the theft of private data. Although prior research has found that data security breaches may have limited long-term stock price impact for an individual company (Richardson *et al.*, 2019), investors may view an ideological attack as more personal and long-lasting against a company and/or country. This may lead them to respond more negatively in the short-term, and those responses may be more persistent over the long term.

Cohen (2014) categorizes cyber terrorist attacks according to three levels of increasing sophistication:

(1) gateway attacks;

(2) information system attacks; and

(3) operational system attacks.

Gateway attacks require the least sophistication and are generally the least damaging to the target. However, they are potentially the most publicly prominent. Gateways are the organization's interface with the internet and are most prone to external attacks. Two common types of gateway attacks are website defacing and denial of service (DoS) attacks. Website defacing refers to cybercrimes where the hacker alters the organization's public website to display different content. For cyber terrorists, this may come in the form of displaying messages consistent with their ideological viewpoints. DoS attacks are designed to make an intended resource, such as a web or email server, unavailable to its users. Cyber criminals perpetrate DoS attacks by overwhelming the target computer or network with repeated communication requests so that it is unable to respond to normal requests, effectively rendering the website or other service inoperable. DoS attacks perpetrated from a single machine are easier to identify and contain. As a result, cyber criminals often turn to malware that infects and takes control of multiple computers to perform a distributed DoS (DDoS) attack that is much more difficult to predict and contain.

Information system attacks require access to an organization's internal systems through employees or some other means. For example, the cyber terrorist might use a phishing attack to entice an unknowing employee to download malware that grants the terrorist access to the employee's computer and network. With this access, the terrorist can perpetrate more significant attacks on the organization's internal servers, databases, networks and other systems that would normally sit behind the organization's firewalls.

The third type of attack, operational system attacks, requires that the cyber terrorist not only obtain access to the organization's internal systems but also that the terrorist have a sophisticated familiarity with the vulnerabilities of the systems used by the organization. Attacks on an organization's core operational systems are most likely to result in physical damage to the company. For example, such attacks may target critical infrastructure systems such as water, gas, public transportation systems or even industrial control systems such as those found in chemical plants.

Arquilla and Ronfeldt (2001) provide an alternative classification of cyber terrorist activities that emphasizes one additional aspect of cyber terrorist behavior. Cyber terrorist operations are classified into three types:

(1) perception management and propaganda;

(2) disruptive attacks; and

(3) destructive attacks.

While the latter two dimensions intersect with Cohen's (2014) framework for classifying cyber terrorism attacks, they omit the importance of recruiting and propaganda activities to the terrorist operation. Terrorists leverage technology not only to commit cyberattacks but also to communicate their message and recruit new members. Terrorists use online chat rooms, bulletin boards and other web sites to market their ideologies and find sympathizers to their cause. Cyber terrorists also use their own sites to communicate and advertise their activities.

Nickolov (2005) describes how the rapid advancement of technology has improved business practices, increasing productivity and competition. It has also increased globalization and the importance of technology in supporting the economic infrastructure of most developed countries. Dependence on these new economic infrastructures has also increased countries' economic vulnerabilities to the threats of cyber terrorism. As these infrastructures continue to expand – especially online in the era of cloud computing – the potential for serious impact on the well-being of citizens, proper functioning governments and industries continues to grow. Nickolov (2005, p. 106) describes:

> [t]his symbiosis [as] a national security priority, since the information infrastructure is crucial to economic progress [. . .] The greater role of information and the availability of electronic means to collect, analyze and modify it, have transformed information and information systems into an invaluable asset and lucrative target.

Former FBI director, Robert Mueller, warned that the threats of cyber terrorism are "real [. . .] and rapidly expanding" (Nakashima, 2010, para. 1). He indicated that terrorists are very interested in developing hacking skills or recruiting outsiders already possessing such skills. He also acknowledged that cyber terrorism is likely underreported among companies and requested companies to end their silence when they are the victims of such attacks.

Companies may hesitate to reveal that they have been the targets of cyber terrorist attacks. Reporting such attacks may promote further attacks. It may also promote the cyber terrorist's agenda. However, companies may also be concerned about public perceptions regarding the vulnerability of their operations. In this paper, we investigate this hypothesis by examining stock market reactions to media announcements about companies that are victims of cyber terrorist attacks.

Our study is unique in that it expands the focus of cyber terrorism events to include those with political or ideological motivations, rather than focusing almost solely on theft of private data. Using an event study methodology, we identify occurrences of cyber terrorism and analyze the market impact of those events. We know of no other studies that investigate cyber terrorism in this manner. A number of prior studies use an event study methodology on issues other than cyber terrorism. For example, a study by Im *et al.* (2001) uses an event study methodology and finds that market prices increase following the announcement of a company's investment in information technology.

A recent event study by Choi *et al.* (2020) finds that health technology spending at hospitals increases in the year after a data breach, and Tweneboah-Koduah *et al.* (2020) use an event study to investigate corporate data breaches. They find mixed results across industries; however, the financial sector exhibited significant increases in market volatility following a data breach. As there is limited academic research on cyber terrorism events, this research is valuable in increasing our understanding of the economic impact of cyber terrorism.

We seek to understand the association between firms affected by cyber terrorism and market responses because prior literature suggests the association may be unclear. In addition to the previous mixed evidence regarding data breaches, past research also indicates that victims of cyber terrorist attacks may perceive cyberterrorism as less

threatening or more distant because it occurs in cyberspace and is more anonymous and virtual and thus perceived as less of a threat relative to a more traditional terrorist attack having potentially more direct effects (Tomz and Weeks, 2020; Kreps and Schneider, 2019). A traditional terrorist attack generally includes direct physical effects such as people being personally harmed by guns and explosives, which seems more hurtful than the nonphysical effects occurring in the cyber world. Shandler *et al.* (2022) suggest that cyber terrorist attacks must surpass a threshold before they are acted upon. As a result, it is unclear whether the market would respond significantly to a cyber terrorist attack. This study addresses specific cyber terrorist attacks and measures if the impact passes the threshold of significance from a stock market valuation standpoint.

Methodology

This study uses an event study methodology, which is defined as an "empirical analysis that examines the impact of a significant catalyst occurrence or contingent event on the value of a security, such as company stock" (Hayes, 2020, para. 1). The specific methodology of this study has been implemented in prior studies (cf., Smith *et al.*, 2019; Smith *et al.*, 2011). Event studies are predicated on the theory of efficient capital markets for a theoretical framework, whose chief architect is Nobel Laureate Eugene Fama:

> In the strong form of the theory, all information – both public and private – are already factored into the stock prices. So it assumes no one has an advantage to the information available, whether that's someone on the inside or out. (Dhir, 2019, para. 6)

To determine whether news stories regarding cyber terrorist attacks significantly impact stock prices, the stock prices of publicly traded companies are examined before and after the story becomes public. The change in stock price is then compared to the change in the Dow Jones Industrial (DJI) Index for the same time period.

The day the news story becomes public is the "event day" and labeled as "Day 0." Stock prices of companies that were victims of cyber terrorism are documented the day before and after Day 0, three days before/after Day 0 and a week before/after Day 0. Using dates within a week of the event day is customary for event studies to reduce the potential occurrence of other confounding effects.

Company stock prices were obtained from Yahoo Finance. The Yahoo Finance website (finance.yahoo.com) provides extensive information about company stocks, such as market (NYSE, NASDAQ, etc.), ticker symbol, annual high/lows and EPS. For each of the documented days, the average percentage change in stock price of victimized companies was compared to the DJI Index to ascertain whether the change in stock price was different than the fluctuations in the market overall. To determine whether there was a significant difference in the comparison of stock prices, a matched-pair *t*-test was used.

Data was assembled concerning news stories of cyber terrorist attacks on publicly traded companies. This follows the collection method of prior research (cf., Smith *et al.*, 2019; Smith *et al.*, 2011). The specific data collected on each news story and company are: perpetrator and victims of cyber terrorist attack, date of news story, details of the cyber terrorism event, ticker symbol of the company attacked and the company's stock price before and after the attack.

Case studies

Described below are case studies of 14 cyber terrorist attacks on publicly traded business firms. Specific details about each firm and the cyber terrorist attack will be described below. Table 2 lists the business firms and people affected by the cyber terrorist attack. Table 3 lists the cyber terrorist attack perpetrators and a brief description of the events in the attack.

Table 2.
Business firms and people affected by cyber terrorist attack

Firm name	Ticker symbol	Date of news story	Impact of attack
Amazon	AMZN	10/22/2019	More than 4,600 companies using Amazon Web Services
Amazon	AMZN	10/4/2018	Estimated 30 US companies, including Amazon and Apple Inc.
Apple	AAPL	10/4/2018	Estimated 30 US companies, including Amazon and Apple Inc.
Merck	MRK	6/27/2017	30,000 computers and 7,500 servers
FedEx	FDX	6/27/2017	490,000 employees, 65 million customers, 15 million average daily shipments
Equifax	EFX	9/7/2017	143 million customers
American Express	AXP	3/28/2013	53.1 million American cardholders and 54.1 million international cardholders
Bank of the West (BNP Paribas S.A.)	BNP	2/13/2013	1 company, Ascent Builders, 62 BNP customers used as money mules and over 20 million customers using Bank of the West's website
Capital One	COF	10/9/2012	Between 60 million and 62.5 million cardholders
Wells Fargo	WFC	9/26/2012	Hundreds of customer complaints
Citigroup	C	9/21/2012	Hundreds of customer complaints
JP Morgan Chase	JPM	9/19/2012	Over 1,000 confirmed customer complaints
Bank of America	BAC	9/19/2012	53 million users and small businesses
Google	GOOG	1/12/2010	At least 2 Gmail accounts, as well as at least 20 other large companies

Amazon, 2019

In 2019, Amazon experienced a DDoS attack that lasted approximately 8 h and targeted its Route 53. Route 53 is a cloud domain name system service that enables businesses to route users to internet applications (Amazon, 2021a, para. 1). Furthermore, Route 53 allows users to connect to infrastructure that runs in Amazon Web Services (AWS). Route 53 is also responsible for Amazon's Simple Storage Services, which businesses use to store and protect data for a range of uses, such as mobile applications, backup and restore and big data analytics (Amazon, 2021b, para. 1). Although the primary attack was on the Route 53 DNS servers, there was a trickle-down impact on other AWS, such as Google Cloud Storage (Muncaster, 2019). This third-party cyber terrorist attack incapacitated critical US digital infrastructure.

Catchpoint, a digital monitoring firm, claimed that Amazon was slow to react to the attack, likely because they were monitoring their own systems instead of monitoring end-user impacts (McCarthy, 2019). This incident reveals the vulnerability of individual companies such as Amazon to cyber terrorist attacks but also to the ripple effect to connected companies. The incident also shows how rapid changes in technology create difficulties for any company trying to monitor potential weak points in their operations.

Amazon and Apple, 2018

While reported in 2018, the beginning of this event is traced back to 2015 when Amazon hired a third-party security services company to evaluate a startup company, Elemental Technologies, as part of due diligence for a potential acquisition. Elemental produced software for video file compression and formatting; their primary products were servers that customers could use to run the software. During the course of this evaluation, the testers discovered a tiny microchip, about the size of a grain of rice, included as part of the

Table 3.
Cyber terrorist attack perpetrators and events

Firm name	Perpetrator	Cyber terrorism event
Amazon	Third party	Amazon Web Services experienced a DDoS attack for 8 h that crashed sites of many customers using Amazon Web Services to help host their site. AWS experienced over 4,600 issue reports
Amazon	Chinese spies	Chinese spies embedded a microchip on server motherboards and gained access to supply chains, including company trade secrets and government communication networks
Apple	Chinese spies	Chinese spies embedded a microchip on server motherboards and gained access to supply chains, including company trade secrets and government communication networks
Merck	NotPetya	Ransomware/wiper software hit Merck's computers, crippling its sales, manufacturing, research units and production facilities, preventing Merck meeting demand for Gardasil 9, a vaccine against HPV. Estimated $870m in damages
FedEx	NotPetya	Ransomware/wiper software infected TNT Express, a Ukrainian delivery and logistics company owned by FedEx. Reported $400m recovery cost and $600m estimated increase in cost of integrating TNT Express into FedEx
Equifax	Chinese People's Liberation Army	Hackers gained access to company data that potentially compromised sensitive information for 143 million American consumers, including Social Security numbers and driver's license numbers
American Express	Izz ad-Din al-Qassam; Operation Ababil	DDoS attack disrupted online account access for American Express both in the US and abroad for about 2 h. Backend systems that handle bill pay, statements and account summary were all targeted in the DDoS
Bank of the West (BNP Paribas S.A.)	Attack matches the profile of cybercrime gangs using the Gameover Trojan	DDoS attack on Bank of the West's website caused customers to be unable to access their accounts. This was used as a distraction for a hacker group to steal $900,000 from corporate accounts belonging to California construction firm Ascent Builders using money mules
Capital One	Izz ad-Din al-Qassam; Operation Ababil	DDoS attack overloaded Capital One's website, causing a day-long slowdown and was sporadically unreachable for many customers
Wells Fargo	Izz ad-Din al-Qassam; Operation Ababil	DDoS attack overloaded Wells Fargo's website, causing day-long slowdowns and was sporadically unreachable for many customers
Citigroup	Izz ad-Din al-Qassam; Operation Ababil	DDoS attack overloaded Citigroup's website, causing day-long slowdowns and was sporadically unreachable for many customers
JP Morgan Chase	Izz ad-Din al-Qassam; Operation Ababil	DDoS attack disrupted the bank's website and corporate networks resulting in a day-long slowdown that made the website unreachable for many customers
Bank of America	Izz ad-Din al-Qassam; Operation Ababil	DDoS attack overloaded Bank of America's website, causing day-long slowdowns and was sporadically unreachable for many customers
Google	China; Operation Aurora	Chinese Government deployed malware to target Gmail web service and obtain access to messages of Chinese dissidents. Two of Ai Weiwei's Google email accounts were hacked and his emails were read and copied

motherboard of Elemental's servers. Further investigation revealed that the microchips had been inserted during the servers' production stage (Robertson and Riley, 2018).

As documented in Robertson and Riley (2018), the servers in question had been manufactured in China and sold by San Jose-based Super Micro Computer Inc. The insertion of the microchips had been performed by individuals with connections to the People's Liberation Army. Approximately 30 additional US companies were also found to have similar microchips installed on company servers. Victims included "a major bank, government contractors, and the world's most valuable company, Apple Inc." (pp. 52–53).

Although no consumer data appeared to be compromised in the attack, US government officials believe "China's goal was long-term access to high-value corporate secrets and sensitive government networks" (Robertson and Riley, 2018, p. 53). These chips were designed to hold small amounts of code that would ultimately connect victim networks to a larger superchip, which could then be used to remotely access servers and discreetly alter machine code. The chips could override password requirements for servers, effectively turning a secure machine into one that is open for all users (Robertson and Riley, 2018).

Merck and FedEx, 2017

On June 27, 2017, the GRU, Russia's military intelligence agency, unleashed a cyberattack against Ukraine named NotPetya that spread globally and caused more than $10bn in global damages (Blosfield, 2020; Voreacos *et al.*, 2019). The infected software was initially spread in the days before the attack using accounting software and malicious emails that embedded malware on unsuspecting servers and computers. After being installed, the malware had the ability to continue spreading within corporate networks (McMillan *et al.*, 2017). Once the software was triggered externally, infected computers were locked down and users received a ransom demand for $300 per infected machine, payable in bitcoin. Despite the ransom demand, the primary purpose of the malware was deemed political in nature (Voreacos *et al.*, 2019). The White House labeled the attack as the "most destructive and costly cyberattack in history" (Voreacos *et al.*, 2019).

Merck was among the companies infected by the NotPetya malware through a server in their Ukraine office. Overall, the company had 30,000 computers and 7,500 servers infected and locked down for over two weeks. The attack also caused problems with their production facility and prevented the company from creating enough Gardasil 9, their HPV vaccine, to meet annual supply. Merck was forced to borrow the entirety of the US emergency supply of that vaccine, and it took Merck 18 months to restock that supply. Merck's year-end regulatory filing indicated the attack caused $870m of damages (Voreacos *et al.*, 2019).

FedEx was also damaged by the NotPetya malware when it was exposed through its European subsidiary, TNT Express (Dignan, 2017). Although there was no data breach or data loss, the company experienced significant operational issues that forced the company to shift some services to manual operations for a period of time. FedEx did not have insurance coverage for this type of event, thus the financial impact was significant.

Equifax, 2017

Equifax is a major credit reporting agency in the USA that stores sensitive personal information on a multitude of people. Hackers breached their security systems and accessed information for 143 million Americans in May 2017. Fruhlinger (2012) describes key events that led to the breach's success. The hackers initially breached the company using a known vulnerability in Equifax's consumer complaint web portal that had not been patched. From there, the hackers were able to move to different servers within the company because Equifax had failed to segment their different systems. Within these systems, the hackers

accessed usernames and passwords that gave them increased access to Equifax's systems. Once sensitive information had been compromised, the hackers removed the data undetected over a period of months because Equifax had overlooked the renewal on an encryption certificate. Equifax then waited more than a month after discovering the breach to alert the public.

These hackers accessed the names, addresses, Social Security numbers and drivers' licenses of the 143 million Americans (Bernard *et al.*, 2017; Fruhlinger, 2012). Authorities monitored the dark web in the months after the breach under an assumption that the hackers would attempt to sell the information for a profit. When none of the data appeared online, authorities began to suspect state-sponsored Chinese hackers, who would be motivated by espionage rather than theft (Fruhlinger, 2012). The U.S. Department of Justice eventually charged four Chinese military members in February 2020 for their connection to the attack (Fruhlinger, 2012).

After this breach, much of Equifax's corporate management team was replaced and the company offered all individuals, not just those impacted by the breach, a free one-year subscription to their credit protection services (Bernard *et al.*, 2017). In addition, Equifax spent $1.4bn on cleanup costs (Fruhlinger, 2012).

American Express, 2013

A DDoS attack was launched against American Express on March 28, 2013, and impacted online-access for approximately 2 h (Kitten, 2013). The attack hit bill-pay, statements and account summary systems. It also took down some online ad and content platforms, as well as tablet and mobile apps, though American Express declared that no customer information had been compromised (Estes, 2013).

Bank of the West, 2013

According to the news story published by Krebs (2013), Bank of the West experienced a DDoS attack in December 2012 that was implemented as a means to hide the theft of funds from the account of Ascent Builders. The theft was engineered by fraudsters who used money mules, individuals who knowingly or unknowingly assist fraudsters, to receive funds that were illegally transferred from Ascent's corporate account. As soon as the illegal transfers were completed, the DDoS attack was initiated and bank operations were disrupted (Krebs, 2013).

In addition to the DDoS attack, the fraudsters took advantage of malware that had been inserted on Ascent's computer systems to gain additional time to transfer stolen funds. When Ascent's management attempted to access their online bank account on the morning of the theft, the malware directed them to a site with a message indicating the bank website was down for a 24-h period. Fortunately for Ascent, the money mule realized what had occurred and contacted KrebsOnSecurity, who in turn alerted Ascent of the scheme (Krebs, 2013). The combination of theft followed by a DDoS attack is a similar profile to hackers that have previously used the Gameover Trojan (Krebs, 2013). The Gameover Trojan, which sets up a massive botnet, was designed by Russian hacker Evgeniy Mikhailovich Bogachev (Wei, 2015).

The individual who confessed to KrebsOnSecurity was 1 of the 62 such money mules that the fraudsters had used to steal over $900,000 from Ascent's corporate account. Ascent was eventually able to retrieve half of the stolen funds. The FBI was alerted to the scheme and shared that other companies were also targeted on that same day (Krebs, 2013).

The remaining cyber terrorist attacks in this paper were allegedly committed by the same group, Izz ad-Din al-Qassam Cyber Fighters. This group claimed credit for multiple large-scale

DDoS attacks against major US financial corporations under the codename Operation Ababil (Infosecurity, 2013; Kitten, 2013; Rushe, 2012). These attacks were purportedly initiated as a protest against an offensive video appearing on YouTube (Infosecurity, 2013). However, Dmitri Alperovitch, CEO of the private security firm CrowdStrike, believed this explanation was a ruse because the group had begun claiming credit for attacks prior to the video being posted (Rushe, 2012). The group successfully overloaded computing systems at several large-scale financial organizations (Goldman, 2021; Infosecurity, 2013; Wagenseil, 2012). Some attacks overwhelmed "bank websites with information at up to 100 gigabits a second; the usual DDoS attack is in the order of 5–10 gigabits a second" (Rushe, 2012, para. 7). Each attack disabled user access to online accounts for at least several hours during the day of the attack, though fortunately there was no apparent long-term impact. Below are brief descriptions of specific attacks for which this group claimed credit.

Capital One, 2012

Capital One was attacked on October 9, 2012. Users who tried to log in to their accounts were met with the following message: "Our site is currently unavailable. We apologize for the inconvenience and suggest that you check back later today to view your account information" (Kovacs, 2013, para. 5). Interruptions to their service occurred intermittently over the space of approximately 3 h (Arsene, 2012; Kitten, 2012).

Wells Fargo, 2012

Wells Fargo was attacked on September 26, 2012. Although no customer information was compromised, there were hundreds of complaints registered throughout the day on https://sitedown.co/wells-fargo that referenced the inaccessibility of the website (Rushe, 2012).

Citigroup, 2012

Citigroup was attacked in September 2012. Although there were no official reports released of the full impact of this specific attack, it was similar to other attacks in that it prevented users from accessing their online accounts and using bill pay and other online features (Perlroth, 2012).

JP Morgan Chase, 2012

JP Morgan Chase was attacked on September 19, 2012 (Egan and Samson, 2012). The attack began in the morning and created intermittent issues for users attempting to log in to their account during the day. Despite the attack, JP Morgan shares increased by 0.19% by the end of the trading day (Egan and Samson, 2012).

Bank of America, 2012

Bank of America was attacked on September 18, 2012, which impacted the ability of some of their approximately 53 million customers to access their accounts online (Bank of America, 2013). There were reports throughout the day of intermittent outages and customers' inability to access their accounts because of the slowness of the network. The outages began at 10 a.m. ET, and their website performance was not stabilized until mid-morning of the following day (Pepitone, 2012). There were no reports of customer information being compromised in the attack.

Google, 2010

In January 2010, Google's Gmail web service was part of a targeted cyberattack that hit at least 30 companies (Paul, 2010). Although Google only identified China as the origin of the attackers, VeriSign's iDefense security lab published a report implicating the Chinese Government as the instigators. The goal of the attack was to gather information on Chinese dissidents (Google, 2010; Paul, 2010). Although Google reported the theft of intellectual property, they claimed the hack was limited to two Gmail accounts, and the hackers were only able to see high-level account information and the subject line of emails (Google, 2010). Besides the two accounts that were compromised, dozens of additional accounts belonging to people pressing for human rights in China had also been hacked (Branigan, 2010; Wong, 2010).

Analysis and results

Findings show that news stories about cyber terrorism have a significant negative affect on company stock prices. On average, companies that were the victim of cyber terrorism had lower stock prices after the terrorist attack was publicized. The per cent change in stock prices of victimized companies were compared to the DJI Index before and after the news story occurred. Table 4 reveals that the average stock price of victimized companies changed significantly more than the DJI Index after the news story. For each of the designated days following the news story, the average stock price of victimized companies fell at a significantly higher rate than the DJI Index.

The day after the cyber terrorist attack was publicized (Day +1), the average change in stock price of the victimized company was −1.55%, compared to a −0.07% change in the DJI ($p < 0.1$). On the third day after the news story (Day +3), the average change in company stock price was −2.89%, compared to a −0.24% change in DJI ($p < 0.1$). On the seventh day after the news story (Day +7), the average change in company stock price was −5.08%, compared to a −0.76% change in DJI ($p < 0.1$).

		Percent change in company stock price around event day						
Ticker symbol		Day	Day	Day	Day	Day	Day	Day
#	Company	−7	−3	−1	0	+1	+3	+7
1	AMZN (2019)	(2.53)	0.47	(1.03)	0	(1.50)	(5.07)	(0.68)
2	AMZN (2018)	3.41	4.97	2.27	0	(1.04)	(2.05)	(7.78)
3	AAPL	(2.54)	(0.32)	1.79	0	(1.62)	(0.49)	(4.66)
4	MRK	(3.92)	0.73	0.58	0	(0.58)	(2.21)	(3.63)
5	FDX	(1.79)	(1.26)	0.48	0	1.32	1.40	1.95
6	EFX	(1.47)	(0.79)	(0.93)	0	(13.66)	(18.75)	(33.87)
7	AXP	(1.96)	(1.07)	(1.05)	0	0.16	0.52	(2.48)
8	BNP	(2.22)	(3.27)	(0.68)	0	2.79	(1.02)	(5.03)
9	COF	(3.84)	0.17	(0.20)	0	(0.19)	(0.32)	(1.88)
10	WFC	2.53	1.81	1.24	0	(0.80)	(0.03)	3.77
11	C	(3.87)	(1.75)	(2.27)	0	(3.12)	(5.24)	(3.12)
12	JPM	(5.08)	1.52	(0.68)	0	(0.90)	(1.74)	(2.20)
13	BAC	(5.25)	2.89	(1.82)	0	(2.04)	(3.64)	(4.72)
14	GOOG	4.99	0.61	1.80	0	(0.57)	(1.77)	(6.85)
Avg % change stock price		(1.68)	0.34	(0.04)	0	(1.55)	(2.89)	(5.08)
Avg % change DJI index		(0.57)	0.08	0.22	0	(0.07)	(0.24)	(0.76)
Significance (prob>)		0.09	0.39	0.16		0.08	0.05	0.07

Notes: On all three post-event dates, +1, +3 and +7, the sample firms experience price changes significantly more negative than the market overall

Table 4.
Effect of cyber terrorism news on stock price

Stock prices were also documented for the week preceding the news story regarding a cyber terrorist attack. There was no significant difference when comparing the stock price change of the DJI Index and the average stock price of victimized companies for the day before the news story (Day −1), nor three days before (Day −3). Seven days before the news story (Day −7), the company stock price and the DJI had a slightly significant difference.

As can be seen in Table 4, Equifax incurred the greatest negative impact on their stock price after a cyber terrorist attack. This could be because of the enormity of the attack. Hackers accessed sensitive information on 143 million customers, including Social Security and driver's license numbers. Equifax stock price fell at an increasing rate during the week after the news story was publicized.

Slightly over half of the companies that suffered a cyber terrorist attack experienced an increasing rate of stock price decline during the week after the news story. Other company stock prices continued to decline, but at a lower rate. One company, Wells Fargo, managed to recover by the end of the week with an increase in stock price on Day +7. FedEx was the only company whose stock price never fell, but actually increased during the week after a cyber terrorist attack. This may be because the attack affected a Ukrainian delivery company owned by FedEx, rather than the parent company.

While other issues can influence stock prices, such as inflation, the economy, interest rates and political changes, the impact of these issues is reduced by using dates close to the cyber terrorism event. The effect of these other issues is further minimized by comparing the change in company stock price with the change in the market overall. Finding that the average stock price of companies experiencing a cyber terrorist attack decline significantly more than the DJI Index reveals the extensive damage that cyber terrorism can inflict on a company. Half of the cyber terrorist attacks cited in this study involved a bank or credit card company. Because these companies obtain sensitive financial information from their customers, they could be a prime target for cyber terrorism.

Cyber terrorism prevention

Companies should be active in developing methods to prevent cyber terrorist attacks. One common strategy is to adopt defense-in-depth strategies appropriate to their organizations. Defense-in-depth is a layered architecture approach to cybersecurity that provides a tiered defense to cyberattacks [U.S. Department of Homeland Security (DHS), 2016]. In addition to granting companies the flexibility to choose a cybersecurity posture that weighs companies' cyber risk preferences against their need to provide relevant system performance, a tiered approach provides redundancies such that if one security mechanism fails, another may yet thwart an in-progress attack. For example, a company may place their ecommerce website under a shallow perimeter tier that has relatively few security layers while placing sensitive customer or employee data in a deeper tier with greater security. The deeper tier can still interact with the shallower tier, but it would be protected by multiple firewalls and access controls such as multifactor authentication. It would also be subject to other measures such as encryption and stricter change controls. In general, defense-in-depth provides greater flexibility for effectively catering to system user needs while also providing a holistic approach to system security as it incorporates security from multiple aspects (e.g. software controls, HR and business policy controls and physical controls).

Current cyber risk management strategies also realize that passive prevention tactics are generally insufficient to guard against cyber terrorist attacks. An effective security model recognizes that when proficient threat actors are determined to penetrate a system, time is the key limiting factor. Preventing a breach is thus de-emphasized; rather, the focus is on system penetration discovery and response tactics so as to quickly limit a breach's impact

(Schwartau, 1998). Detection strategies involve active tactics such as network monitoring for unusual traffic patterns or events, and strategic responses may activate back-up sites and divert network traffic, in addition to blocking the intruder. If done quickly enough, detection and response may be sufficient to prevent the threat actors from obtaining critical or sensitive information. It may also allow the company to strengthen their defenses by identifying and correcting weaknesses in their system.

Once an organization has a good understanding of its time to detect and respond to a cyber terrorist attack, it can also better estimate how much it should invest in prevention strategies to reduce the risk of a successful attack. Such decisions will depend on a company's chosen cybersecurity posture, which is the company's position on how much risk it is willing to accept related to the potential impact of a successful cybersecurity threat. When the company understands its detection and response times, it can better determine whether additional detection or prevention measures should be adopted. Penetration tests, or tests that mimic real-world attacks, can be invaluable for assessing an organization's weak points and susceptibility to attacks, as well as identifying where additional training, detection or prevention measures may be needed.

Conclusions

Cyber terrorism is a growing world problem and a serious technology risk to publicly traded business firms and the economies in which they operate. Guarding business information systems from cyber terrorism is an essential component of technology management. Cyber terrorism is costly in terms of impaired business and damaged virtual and physical assets. Furthermore, cyber terrorism harms a firm's reputation, thereby negatively affecting a firm's stock market valuation. This paper examines the risks posed by cyber terrorism, specifically its impact on market valuation (stock prices) of publicly traded firms.

Findings of the analysis indicate that market valuation (stock price) is significantly negatively affected by news of a cyber terrorist attack on business firms. For all three time periods after the cyber terrorist attack, there occurred a significant negative decline in the stock value relative to the Dow Jones Index. A firm's valuation is damaged by cyber terrorism. A successful cyber terrorism attack exposes the vulnerability of a firm's information system. Taking steps to avoid being a victim of cyber terrorism is vital to cybersecurity. Preventative steps are normally far less costly than rebuilding an information system after a cyber terrorist attack. Firm managers would do well to learn from past cyber terrorism cases and bolster their cybersecurity to prevent or minimize risks of cyber terrorist attacks against their firms.

Limitations and future research

This study was limited by firms in its sample of cyber terrorist attacks and the time periods in which the attacks occurred. Future studies could include additional firms, other cyber terrorist attacks and other time periods, both before and after time period of this study. Another possible future study could investigate the economic and business costs associated with the different types of cyberattacks. With regard to defending against cyber terrorism on business firms, future research could consider developing high to low sensitivity ratings of specific defense approaches according to their practical use by firms and society. Data for this study was limited to publicly available information. Future studies might be able to work with firms to share privately held information.

References

Amazon (2021a), "Amazon Route 53", AWS, available at: aws.amazon.com/route53/ (accessed 25 February 2021).

Amazon (2021b), "Amazon S3", AWS, available at: https://aws.amazon.com/s3/ (accessed 24 February 2021).

Arquilla, J. and Ronfeldt, D. (2001), *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Rand Corporation, Santa Monica, CA.

Arsene, L. (2012), "Cyber attack on capital one places US banks on alert", Bitdefender, available at: https://hotforsecurity.bitdefender.com/blog/cyber-attack-on-capital-one-places-u-s-banks-on-alert-3889.html (accessed 25 February 2021).

Backhaus, S., Gross, M.L., Waismel-Manor, I., Cohen, H. and Canetti, D. (2020), "A cyberterrorism effect? Emotional reactions to lethal attacks on critical infrastructure", *Cyberpsychology, Behavior and Social Networking*, Vol. 23 No. 9, pp. 595-603.

Bank of America (2013), "Bank of America 2012 annual report", available at: http://investor.bankofamerica.com/static-files/12926fa6-1976-4d30-9e7f-f73ba515309b (accessed 27 February 2021).

Bernard, T., Hsu, T., Perlroth, N. and Lieber, R. (2017), "Equifax says cyberattack may have affected 143 million in the U.S", The New York Times, p. A1.

Beveren, J.V. (2001), "A conceptual model of hacker development and motivations", *Journal of E-Business*, Vol. 1 No. 2, pp. 1-9.

Blosfield, E. (2020), "Cyber lessons for the insurance industry continue three years after NotPetya", Insurance Journal, available at: www.insurancejournal.com/news/national/2020/08/12/578788.htm (accessed 24 February 2021).

Branigan, T. (2010), "Accounts invaded, computers infected – human rights activists tell of cyber attacks", The Guardian, available at: www.theguardian.com/world/2010/jan/14/china-human-rights-activists-cyber-attack (accessed 27 February 2021).

Broeders, D., Cristiano, F. and Weggemans, D. (2021), "Too close for comfort: cyber terrorism and information security across national policies and international diplomacy", *Studies in Conflict and Terrorism*, pp. 1-28, doi: 10.1080/1057610X.2021.1928887.

Burger, M., Smith, L.M. and Wood, J. (2020), "Recent cybercrimes and cybersecurity strategies", *Internal Auditing, January-February*, Vol. 35 No. 1, pp. 12-19.

Choi, S.J., Johnson, M.E. and Lee, J. (2020), "An event study of data breaches and hospital IT spending", *Health Policy and Technology*, Vol. 9 No. 3, pp. 372-378, doi: 10.1016/j.hlpt.2020.04.008.

Clutterbuck, R. (1993), "Negotiating with terrorists", In R.D. Crelinsten and A.P. Schmid (Eds), *Western Responses to Terrorism*, Routledge, London.

Cohen, D. (2014), "Chapter 13 - cyber terrorism: case studies", in Akhgar, B. Staniforth, A. and Bosco, F. (Eds), *Cyber Crime and Cyber Terrorism Investigator's Handbook*, Syngress, pp. 165-174, 10.1016/B978-0-12-800743-3.00013-X

Collin, B. (1997), "Future of cyberterrorism: the physical and virtual worlds converge", *Crime and Justice International*, Vol. 13 No. 2, pp. 15-18.

Denning, D. (2000), "Cyberterrorism", FAS, available at: https://fas.org/irp/congress/2000_hr/00-05-23denning.htm#:~:text= (accessed 20 September 2021).

Dhir, R. (2019), "Efficient market hypothesis: is the stock market efficient?", Investopedia, available at: www.investopedia.com/articles/basics/04/022004.asp (accessed 19 February 2021).

Dignan, L. (2017), "FedEx said TNT Petya attack financial hit will be material, some systems won't come back", ZDNet, available at: www.zdnet.com/article/fedex-said-tnt-petya-attack-financial-hit-will-be-material-some-systems-wont-come-back/ (accessed 26 February 2021).

Egan, M. and Samson, A. (2012), "Chase, NYSE websites targeted in cyber attacks", Fox Business, available at: https://web.archive.org/web/20121019181832/http:/www.foxbusiness.com/industries/2012/09/19/chase-website-experiences-intermittent-troubles/ (accessed 25 February 2021).

Estes, A.C. (2013), "A DDoS attack just took down AmEx.com", Vice. available at: www.vice.com/en/article/xyy3bz/a-ddos-attack-just-took-down-amexcom (accessed 24 February 2021).

Fruhlinger, J. (2012), "Equifax data breach FAQ: what happened, who was affected, what was the impact?", CSO Online, available at: www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html (accessed 20 September 2021).

Goldman, D. (2021), "Major banks hit with biggest cyberattacks in history", CNN Business., from https://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html (accessed 25 February 2021).

Google (2010), "Official Google blog: a new approach to China", Google, available at: https://googleblog.blogspot.com/2010/01/new-approach-to-china.html (accessed 24 February 2021).

Gordon, S. and Ford, R. (2006), "On the definition and classification of cybercrime", *Journal in Computer Virology*, Vol. 2 No. 1, pp. 13-20, doi: 10.1007/s11416-006-0015-z.

Hayes, A. (2020), "Event study", Investopedia, available at: www.investopedia.com/terms/e/eventstudy.asp (accessed 19 February 2021).

Im, K.S., Dow, K.E. and Grover, V. (2001), "Research report: a reexamination of IT investment and the market value of the firm–an event study methodology", *Information Systems Research*, Vol. 12 No. 1, pp. 103-117, doi: 10.1287/isre.12.1.103.9718.

Infosecurity (2013), "American Express joins the ranks of US banks attacked by al-Qassam group", Infosecurity Group, available at: www.infosecurity-magazine.com/news/american-express-joins-the-ranks-of-us-banks/ (accessed 24 February 2021).

Kitten, T. (2012), "CapOne site takes DDoS hit", Bank Info Security, available at: www.bankinfosecurity.com/capone-site-takes-ddos-hit-a-5181 (accessed 24 February 2021).

Kitten, T. (2013), "DDoS strikes American Express", Bank Info Security, available at: www.bankinfosecurity.com/american-express-a-564 (accessed 24 February 2021).

Kovacs, E. (2013), "Sites of Capital One, HSBC, Fifth Third Bank, Ally Financial disrupted by DDoS attack", Softpedia News, available at: https://news.softpedia.com/news/Sites-of-Capital-One-HSBC-Fifth-Third-Bank-Ally-Financial-Disrupted-by-DDOS-Attacks-318407.shtml (accessed 25 February 2021).

Krebs, B. (2013), "DDoS attack on bank hid $900,000 cyberheist", KrebsOnSecurity, from https://krebsonsecurity.com/2013/02/ddos-attack-on-bank-hid-900000-cyberheist/ (accessed 20 September 2021).

Kreps, S. and Schneider, J. (2019), "Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics", *Journal of Cybersecurity*, Vol. 5 No. 1, pp. 1-11.

Lee, C.S., Choi, K., Shandler, R. and Kayser, C. (2021), "Mapping global cyberterror networks: an empirical study of Al-Qaeda and ISIS cyberterrorism events", *Journal of Contemporary Criminal Justice*, Vol. 37 No. 3, pp. 333-355.

Macdonald, S., Jarvis, L. and Lavis, S.M. (2019), "Cyberterrorism Today? Findings from a follow-on survey of researchers", *Studies in Conflict and Terrorism*, Vol. 45 No. 8, doi: 10.1080/1057610X.2019.1696444, (accessed 24 February 2021).

McCarthy, K. (2019), "Amazon is saying nothing about the DDoS attack that took down AWS, but others are", The Register, available at: www.theregister.com/2019/10/28/amazon_ddos_attack/ (accessed 20 September 2021).

McMillan, R., Gauthier-Villars, D. and Marson, J. (2017), "Cyberattacks hit major companies across globe", *The Wall Street Journal*, available at: www.wsj.com/articles/cyberattacks-hit-global-companies-in-europe-1498575793 (accessed 25 February 2021).

Mendelsohn, B., Katzenstein, P.J. and Seybert, L.A. (2018), "Terrorism and protean power: how terrorists navigate uncertainty", In Katzenstein, P.J. and Seybert, L.A. (Eds), *Protean Power: Exploring the Uncertain and Unexpected in World Politics*, Cambridge University Press, Cambridge.

Muncaster, P. (2019), "AWS left reeling after eight-hour DDoS", Infosecurity Magazine, available at: www.infosecurity-magazine.com/news/aws-customers-hit-by-eighthour-ddos/ (accessed 24 February 2021).

Nakashima, E. (2010), "FBI director warns of "rapidly expanding" cyberterrorism threat", Washington Post, available at: www.washingtonpost.com/wp-dyn/content/article/2010/03/04/AR2010030405066.html (accessed 20 September 2021).

National Security Agency (NSA) (2021), "Understanding the threat", NSA/CSS, available at: www.nsa.gov/what-we-do/understanding-the-threat/ (accessed 20 September 2021).

Nickolov, E. (2005), "Critical information infrastructure protection: analysis, evaluation and expectations", *Information and Security*, Vol. 17, pp. 105-119.

Paul, R. (2010), "Researchers identify command servers behind Google attack", Ars Technica, available at: https://arstechnica.com/information-technology/2010/01/researchers-identify-command-servers-behind-google-attack/ (accessed 24 February 2021).

Pepitone, J. (2012), "Bank of America's site stuck in prolonged slowdown", CNN Business, available at: https://money.cnn.com/2012/09/18/technology/bank-of-america-site-down/index.html?iid=EL (accessed 25 February 2021).

Perlroth, N. (2012), "Attacks on 6 banks frustrate customers", The New York Times, p. B1.

Richardson, V.J., Smith, R.E. and Watson, M.W. (2019), "Much ado about nothing: the (lack of) economic impact of data privacy breaches", *Journal of Information Systems*, Vol. 33 No. 3, pp. 227-265.

Robertson, J. and Riley, M. (2018), "The Big Hack: an investigative report", *Bloomberg Businessweek*, pp. 52-59.

Rushe, D. (2012), "Wells Fargo believed to be victim of cyber-attack over innocence of Muslims", The Guardian, available at: www.theguardian.com/technology/2012/sep/26/wells-fargo-cyber-attack-innocence-of-muslims (accessed 24 February 2021).

Schneider, F. (2017), "Macroeconomics: the financial flows of Islamic terrorism", In *Global Financial Crime*, pp. 97-123, Routledge, London.

Schwartau, W. (1998), "Time-based security explained: provable security models and formulas for the practitioner and vendor", *Computers and Security*, Vol. 17 No. 8, pp. 693-714, doi: 10.13052/jcsm2245-1439.931.

Shandler, R.M., Gross, M.L., Backhaus, S. and Canetti, D. (2022), "Cyber terrorism and public support for retaliation – a multi-country survey experiment", *British Journal of Political Science*, Vol. 52 No. 2, pp. 850-868.

Smith, K.T., Jones, A., Johnson, L. and Smith, L.M. (2019), "Examination of cybercrime and its effects on corporate stock value", *Journal of Information, Communication and Ethics in Society*, Vol. 17 No. 1, pp. 42-60.

Smith, K.T., Smith, L.M. and Smith, J.L. (2011), "Case studies of cybercrime and its impact on marketing activity and shareholder value", *Academy of Marketing Studies Journal*, Vol. 15 No. 2, pp. 67-81.

Spanos, G. and Angelis, L. (2016), "The impact of information security events to the stock market: a systematic review", *Computers and Security*, Vol. 58, pp. 216-229.

Tomz, M. and Weeks, J.L.P. (2020), "Public opinion and foreign electoral intervention", *American Political Science Review*, Vol. 114 No. 3, pp. 856-873.

Tweneboah-Koduah, S., Atsu, F. and Prasad, F. (2020), "Reaction of stock volatility to data breach: an event study", *Journal of Cybersecurity and Mobility*, Vol. 9 No. 3, pp. 355-384.

U.S. Department of Homeland Security (DHS) (2016), "Recommended practice: improving industrial control system cybersecurity with defense-in-depth strategies", cisa.gov, available at: www.cisa.gov/uscert/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf (accessed 23 May 2022).

Voreacos, D., Chiglinksky, K. and Griffin, R. (2019), "Merck cyberattack's $1.3 billion question: was it an act of war?", Bloomberg, Bloomberg.com, available at: www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war (accessed 20 September 2021).

Wagenseil, P. (2012), "Capital One hit as bank cyberattacks resume", NBC News, available at: www.nbcnews.com/id/wbna49351177 (accessed 24 February 2021).

Wei, W. (2015), "FBI offers $3 million reward for arrest of Russian hacker", The Hacker News, available at: https://thehackernews.com/2015/02/fbi-wanted-russian-hacker.html (accessed 20 September 2021).

Wong, E. (2010), "Hackers said to breach Gmail accounts in China", *The New York Times*, p. B4.

Further reading

Gordon, S. and Ford, R. (2002), "Sarah Gordon", *Computers and Security*, Vol. 21 No. 7, pp. 636-647.

Jarvis, L., Macdonald, S. and Nouri, L. (2014), "The cyberterrorism threat: findings from a survey of researchers", *Studies in Conflict and Terrorism*, Vol. 37 No. 1, pp. 68-90, doi: 10.1080/1057610X.2014.853603 (accessed 24 February 2021).

About the authors

Katherine Taken Smith is an Associate Professor of Marketing at Texas A&M University – Corpus Christi. She specializes in digital marketing, emerging technologies, social media marketing and information technology. Her academic record includes numerous journal articles, books, academic conference presentations and awards for teaching and research. Her work is highly referenced, with over 3,700 citations per Google Scholar. Katherine Taken Smith is the corresponding author and can be contacted at: Katherine.Smith@tamucc.edu

Lawrence Murphy Smith, CPA, is a Professor of Accounting at Texas A&M University – Corpus Christi. He specializes in ethics, information technology and international accounting. His academic record includes numerous research articles, books and monographs, academic conference presentations, research grants and awards for teaching and research. His work has been reported in various news media, including National Public Radio, Fortune, USA Today and The Wall Street Journal. His work is highly referenced, with over 4,200 citation per Google Scholar.

Marcus Burger is an Assistant Professor of accounting at the University of North Carolina at Pembroke. He specializes in financial accounting and accounting information systems. His research focuses on financial reporting, accounting standards and cybersecurity issues.

Erik S. Boyle, CPA, is an Assistant Professor of accounting at Idaho State University. He specializes in auditing and forensic accounting. His research focuses on determinants of audit quality and the impact of auditor decisions on non-auditor evaluators of audit quality, such as client management or investors.